



Educational Handouts/Resources

KMK Law Annual Legal Update Seminar
Thursday, December 5, 2024

Keating Muething & Klekamp PLL
Attorneys at Law

One East Fourth Street | Suite 1400 | Cincinnati, Ohio 45202
P: 513.579.6400 | F: 513.579.6457 | kmklaw.com

Table of Contents

I.	Labor & Employment Law Update	PAGE
	<u>Summary of Key Provisions - PWFA</u>	1
II.	Ethics Odds and Ends	PAGE
	<u>Ethics Odds and Ends Resources</u>	13
III.	I Thought the Future Would Be Cooler	PAGE
	<u>Protecting the Privacy of Health Information</u>	32
	<u>Operation AI Comply Continuing the Crackdown on Overpromises and AI-Related Lies</u>	37
	<u>Anonymous Messaging App Targeting Teens</u>	41
	<u>Petition for Approval of AVC Pieces File Stamped</u>	45
	<u>Attorney General James and DFS Superintendent Harris</u>	58
	<u>QANDA 21 1683</u>	62
	<u>Policy Brief The Colorado AI Act</u>	71



Summary of Key Provisions of EEOC's Final Rule to Implement the Pregnant Workers Fairness Act (PWFA)

The U.S. Equal Employment Opportunity Commission issued a final rule to implement the Pregnant Workers Fairness Act (PWFA). The final rule was issued on April 15, 2024, and published in the Federal Register on April 19, 2024. The rule is available at <https://www.federalregister.gov/d/2024-07527> (<https://www.federalregister.gov/d/2024-07527>). The regulation went into effect June 18, 2024. Prior to the issuance of the final rule, the EEOC issued a Notice of Proposed Rulemaking (NPRM), published in the Federal Register on August 11, 2023, and available here <https://www.federalregister.gov/d/2023-17041> (<https://www.federalregister.gov/d/2023-17041>).

This document provides a summary of key portions of the final rule. This document is provided for informational purposes only. It is not a substitute for the full text of the final rule. It does not discuss all of the provisions in the final rule and does not contain details, examples, or explanations that are provided in the final rule. This document indicates the notable differences between the proposed and final rule. In addition to the differences noted in this document, the final rule has numerous minor language changes and several additional examples.

The PWFA requires a covered entity to make reasonable accommodations to a qualified employee's or applicant's known limitations related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions, absent undue hardship on the operation of the business of the covered entity. The PWFA directs

the Equal Employment Opportunity Commission to promulgate regulations to implement the PWFA. As required by the PWFA, the final rule also provides examples of reasonable accommodations.

1. Who is Covered:

The PWFA covers employers (as well as unions and employment agencies), employees, applicants, and former employees who are currently covered by: (1) Title VII of the Civil Rights Act of 1964 (Title VII); (2) the Congressional Accountability Act of 1995 and 3 U.S.C. § 411(c);^[1] (3) the Government Employee Rights Act of 1991 (GERA); or (4) section 717(a) of Title VII, which covers federal employees. Whoever satisfies the definition of an “employer” or “employee” under any of these laws is an employer or employee for purposes of the PWFA.^[2]

2. Remedies and Enforcement:

- a. The procedures for filing a charge or claim under the PWFA, as well as the available remedies, including the ability to obtain damages, are the same as under (1) Title VII; (2) Congressional Accountability Act of 1995 and 3 U.S.C § 411(c); (3) GERA; and (4) section 717 of Title VII, for the employees covered by the respective statutes. Limitations regarding available remedies under these statutes likewise apply under the PWFA. As with the Americans with Disabilities Act, as amended (ADA), damages are limited if the claim involves the provision of a reasonable accommodation, and the employer makes a good faith effort to meet the need for a reasonable accommodation.
- b. In the preamble to the final regulation, the Commission also previews enhancements to its administrative charge processing procedures to facilitate the submission of information about potential defenses, including religious defenses. The Commission is revising numerous documents, including its Notice of Charge of Discrimination letter and webpages, to identify how employers can raise defenses, including religious defenses, in response to a charge of discrimination. Additionally, as appropriate, the Commission will resolve charges based on the information submitted in support of the asserted defenses, including religious defenses, in order to minimize the burden on the employer and the charging party.

3. Definitions:

- a. "Known limitation" is defined in the PWFA as a "physical or mental condition related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions that the employee or the employee's representative has communicated to the covered entity, whether or not such condition meets the definition of disability" under the ADA.
 - i. In the final rule, as in the proposed rule, "known" means "the employee or the employee's representative has communicated the limitation to the employer."
 - ii. In the final rule, as in the proposed rule, "limitation" means a physical or mental condition related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions. The physical or mental condition that is the limitation is:
 - 1. an impediment or problem that may be modest, minor and/or episodic;
 - 2. a need or problem related to maintaining the employee's health or the health of the pregnancy; or
 - 3. seeking health care related to pregnancy, childbirth, or a related medical condition itself.

The physical or mental condition can be a PWFA limitation whether or not it meets the definition of "disability" under the ADA. The physical or mental condition must be a condition of the employee (or applicant) themselves.

- iii. "Pregnancy, childbirth, or related medical conditions" is a phrase used in Title VII (42 U.S.C. 2000e(k)) and in the final rule, as in the proposed rule, it has the same meaning under the PWFA as under Title VII. The final rule clarifies that the pregnancy, childbirth, or related medical conditions refer to the pregnancy, childbirth, or related medical conditions of the specific employee in question. Like the proposed rule, the final rule provides examples of "pregnancy, childbirth, or related medical conditions."

iv. The physical or mental condition must be “related to, affected by, or arising out of” pregnancy, childbirth, or related medical conditions. The final rule explains that “related to, affected by, or arising out of” is an inclusive term. Under the final rule, pregnancy, childbirth, or related medical conditions do not need to be the sole, the original, or a substantial cause of the physical or mental condition at issue in order for the physical or mental condition to be “related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions.”

b. The PWFA has two definitions of “qualified.”

i. First, the PWFA uses language from the ADA: “an employee or applicant who, with or without reasonable accommodation, can perform the essential functions of the employment position” is qualified.

ii. Second, the PWFA allows an employee or applicant to be qualified even if they cannot perform one or more essential functions of the job if the inability to perform the essential function(s) is “temporary,” the employee could perform the essential function(s) “in the near future,” and the inability to perform the essential function(s) can be reasonably accommodated. The terms “temporary,” “in the near future,” and “can be reasonably accommodated” are not defined in the statute.

1. The final rule, like the proposed rule, defines the term “temporary” as lasting for a limited time, not permanent, and may extend beyond “in the near future.”

2. In the final rule, as in the proposed rule, if the employee is pregnant, it is assumed that the employee could perform the essential function(s) “in the near future” because they could perform the essential functions within generally 40 weeks of the temporary suspension of the essential function. The final rule’s definition in this section does not mean that the essential function(s) of a pregnant employee must always be suspended for 40 weeks, or that if a pregnant employee seeks the temporary suspension of an essential function(s) for 40 weeks it must be automatically granted.

3. In the final rule, unlike in the proposed rule, whether the employee could perform the essential function(s) “in the near future” in situations other than when the employee is pregnant is determined on a case-by-case basis.
 4. The final rule, like the proposed rule, also discusses the meaning of the PWFA’s requirement that the inability to perform the essential function(s) can be reasonably accommodated. For some positions, this may mean that one or more essential functions are temporarily suspended (with or without reassignment to someone else) and the employee continues to perform the remaining functions of the job. For other positions, some of the essential functions may be temporarily suspended (with or without reassignment to someone else) and the employee may be assigned other tasks to replace them. In yet other situations, one or more essential functions may be temporarily suspended (with or without reassignment to someone else) and the employee may perform the functions of a different job to which the employer temporarily transfers or assigns them, or the employee may participate in the employer’s light or modified duty program. Throughout this process, as with other reasonable accommodation requests, an employer may need to consider more than one alternative to identify a reasonable accommodation that does not pose an undue hardship.
- c. “Essential function” is a term from the ADA, and the final rule, like the proposed rule, uses the same definition as in the ADA. In general terms, it means the fundamental duties of the job.
 - d. “Reasonable accommodation” is a term from the ADA, and the PWFA uses a similar definition as in the ADA. Generally, it means a change in the work environment or how things are usually done. The final rule, like the proposed rule, provides specific examples of possible reasonable accommodations under the PWFA, including:
 - i. Frequent breaks;
 - ii. Sitting/Standing;

- iii. Schedule changes, part-time work, and paid and unpaid leave;
 - iv. Telework;
 - v. Parking;
 - vi. Light duty;
 - vii. Making existing facilities accessible or modifying the work environment;
 - viii. Job restructuring;
 - ix. Temporarily suspending one or more essential functions;
 - x. Acquiring or modifying equipment, uniforms, or devices; and
 - xi. Adjusting or modifying examinations or policies.
- e. “Undue hardship” is a term from the ADA, and the PWFA follows the definition in the ADA. Generally, it means significant difficulty or expense for the operation of the employer. The final rule, like the proposed rule, outlines some factors to be considered when determining if undue hardship exists. These are the same factors as under the ADA.
- i. Additionally, to address that under the PWFA an employer may have to accommodate an employee’s temporary inability to perform an essential function(s), the final rule, like the proposed rule, adds additional factors that may be considered when determining if the temporary suspension of an essential function(s) causes an undue hardship. These additional factors include: consideration of the length of time that the employee will be unable to perform the essential function(s); whether there is work for the employee to accomplish; the nature of the essential function, including its frequency; whether the employer has provided other employees in similar positions who are unable to perform the essential function(s) of their positions with temporary suspensions of those functions and other duties; if necessary, whether there are other employees, temporary employees, or third parties who can perform or be temporarily hired to perform the essential function(s) in question; and whether the essential

function(s) can be postponed or remain unperformed for any length of time and, if so, for how long.

ii. The final rule, like the proposed rule, identifies a limited number of simple modifications that will, in virtually all cases, be found to be reasonable accommodations that do not impose an undue hardship when requested by a pregnant employee. These “predictable assessments” in the final rule are the same ones as in the proposed rule: (1) allowing an employee to carry or keep water near and drink, as needed; (2) allowing an employee to take additional restroom breaks, as needed; (3) allowing an employee whose work requires standing to sit and whose work requires sitting to stand, as needed; and (4) allowing an employee to take breaks to eat and drink, as needed. As in the proposed rule, the predictable assessments provision in the final rule does not alter the meaning of the terms “reasonable accommodation” or “undue hardship.” The individualized assessment of whether these modifications are reasonable accommodations that would cause undue hardship will, in virtually all cases, result in a determination that the modifications are reasonable accommodations that will not impose an undue hardship under the PWFA when they are requested as workplace accommodations by an employee who is pregnant. Therefore, with respect to these modifications, the individualized assessment should be particularly simple and straightforward.

f. “Interactive process” is a term from the ADA, and the final rule, like the proposed rule, explains that the “interactive process” is a method to help the employer and the employee (or applicant) identify the limitation and the adjustment or change at work needed due to the limitation and potential reasonable accommodations. Generally, it means a discussion or two-way communication between an employer and an employee.

g. Limitations on Supporting Documentation: Under the final rule, as under the proposed rule, an employer is not required to seek supporting documentation from an employee or applicant who requests an accommodation under the PWFA. If an employer decides to seek supporting documentation, it is only permitted to do so under the final

rule if it is reasonable to require documentation under the circumstances for the employer to determine whether the employee (or applicant) has a physical or mental condition related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions (a limitation) and needs a change or adjustment at work due the limitation. The final rule, like the proposed rule, sets out examples of when it would not be reasonable for the employer to require documentation.

Under the final rule, as with the proposed rule, when requiring documentation is reasonable, the employer is limited to requiring documentation that itself is reasonable. The final rule has modified the definition of “reasonable documentation” so that it now means the minimum documentation that is sufficient to: (1) confirm the physical or mental condition; (2) confirm the physical or mental condition is related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions (together with (1) “a limitation”); and (3) describe the change or adjustment at work needed due to the limitation.

The final Interpretive Guidance explains how the provisions of the ADA that require a covered entity to keep medical information confidential apply to employees and information under the PWFA.

4. Requesting an Accommodation:

The final rule, like the proposed rule, explains how an employee may request a reasonable accommodation, which has two parts. The employee must identify the limitation (the physical or mental condition related to, affected by, or arising out of pregnancy, childbirth, or related medical conditions) and that the employee needs an adjustment or change at work due to the limitation.

5. Nondiscrimination With Regard To Reasonable Accommodations

- a. The PWFA prohibits an employer from failing to make reasonable accommodation to the known limitations of qualified employees or applicants, absent undue hardship. The final rule, like the proposed rule, sets out additional considerations for covered entities and employees in complying with this provision. Under the final rule, as under the proposed rule:

- i. An unnecessary delay in making a reasonable accommodation may result in a violation of the PWFA. This can be true even if the reasonable accommodation is eventually provided, when the delay was unnecessary.
 - ii. An employee is not required to accept an accommodation. However, if an employee rejects a reasonable accommodation that they need in order to be “qualified” under the PWFA (either because they need it to perform an essential function, to apply for the job, or to obtain a temporary suspension of an essential function), then that employee or applicant will not be considered qualified.
 - iii. An employer cannot justify failing to make a reasonable accommodation or the unnecessary delay in providing a reasonable accommodation based on the employee (or applicant) failing to provide supporting documentation unless: (1) the employer seeks the supporting documentation; (2) seeking supporting documentation is reasonable under the circumstances as set out under the final rule; (3) the supporting documentation is reasonable documentation as defined in the final rule; and (4) the employer provides the employee with sufficient time to obtain and provide the documentation.
 - iv. When choosing among effective accommodations, the employer must choose an accommodation that provides the qualified employee (or applicant) equal employment opportunity to attain the same level of performance, or to enjoy the same level of benefits and privileges as are available to the average employee without a known limitation who is similarly situated. The similarly situated average employee without a known limitation may include the employee requesting accommodation at a time prior to communicating the limitation.
- b. The PWFA prohibits an employer from requiring a qualified employee or applicant to accept an accommodation other than one arrived at through the interactive process.
 - c. The PWFA prohibits an employer from denying employment opportunities to a qualified employee or applicant if the denial is based

on the employer's need to make a reasonable accommodation for the known limitation of the employee or applicant.

- d. The PWFA prohibits an employer from requiring a qualified employee with a known limitation to take leave, either paid or unpaid, if another effective reasonable accommodation exists, absent undue hardship.
- e. The PWFA prohibits an employer from taking adverse action in terms, conditions, or privileges of employment against a qualified employee or applicant on account of the employee requesting or using a reasonable accommodation for a known limitation.

6. Prohibition on Retaliation and Coercion:

- a. The PWFA prohibits retaliation against any employee, applicant, or former employee because that person has opposed acts or practices made unlawful by the PWFA or has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under the PWFA.
- b. The PWFA prohibits coercion, intimidation, threats, or interference with any individual in the exercise or enjoyment of rights under the PWFA or with any individual aiding or encouraging any other individual in the exercise or enjoyment of rights under the PWFA. The final rule, like the proposed rule, adds "harass" to the list of prohibited activities.
- c. The final rule explains how, depending on the facts, certain actions can violate the prohibitions on retaliation and coercion, such as not providing an interim reasonable accommodation, seeking supporting medical documentation or information when it is not permitted under the PWFA or the final rule, or disclosing confidential medical information.

7. Relationship to Other Laws:

- a. The PWFA does not limit the rights of individuals affected by pregnancy, childbirth, or related medical conditions under any Federal, State, or local law that provides greater or equal protection.
- b. The final rule provides more information about the interactions between the PWFA and Title VII and between the PWFA and the ADA.

c. The PWFA provides a “[r]ule of construction” stating that the law is “subject to the applicability to religious employment” set forth in section 702(a) of the Civil Rights Act of 1964, 42 U.S.C. 2000e-1(a). The relevant portion of section 702(a) provides that “[Title VII] shall not apply . . . to a religious corporation, association, educational institution, or society with respect to the employment of individuals of a particular religion to perform work connected with the carrying on by such corporation, association, educational institution, or society of its activities.” The final rule, like the proposed rule, provides that when this PWFA provision is asserted by a respondent employer, the Commission will consider the application of the provision on a case-by-case basis.

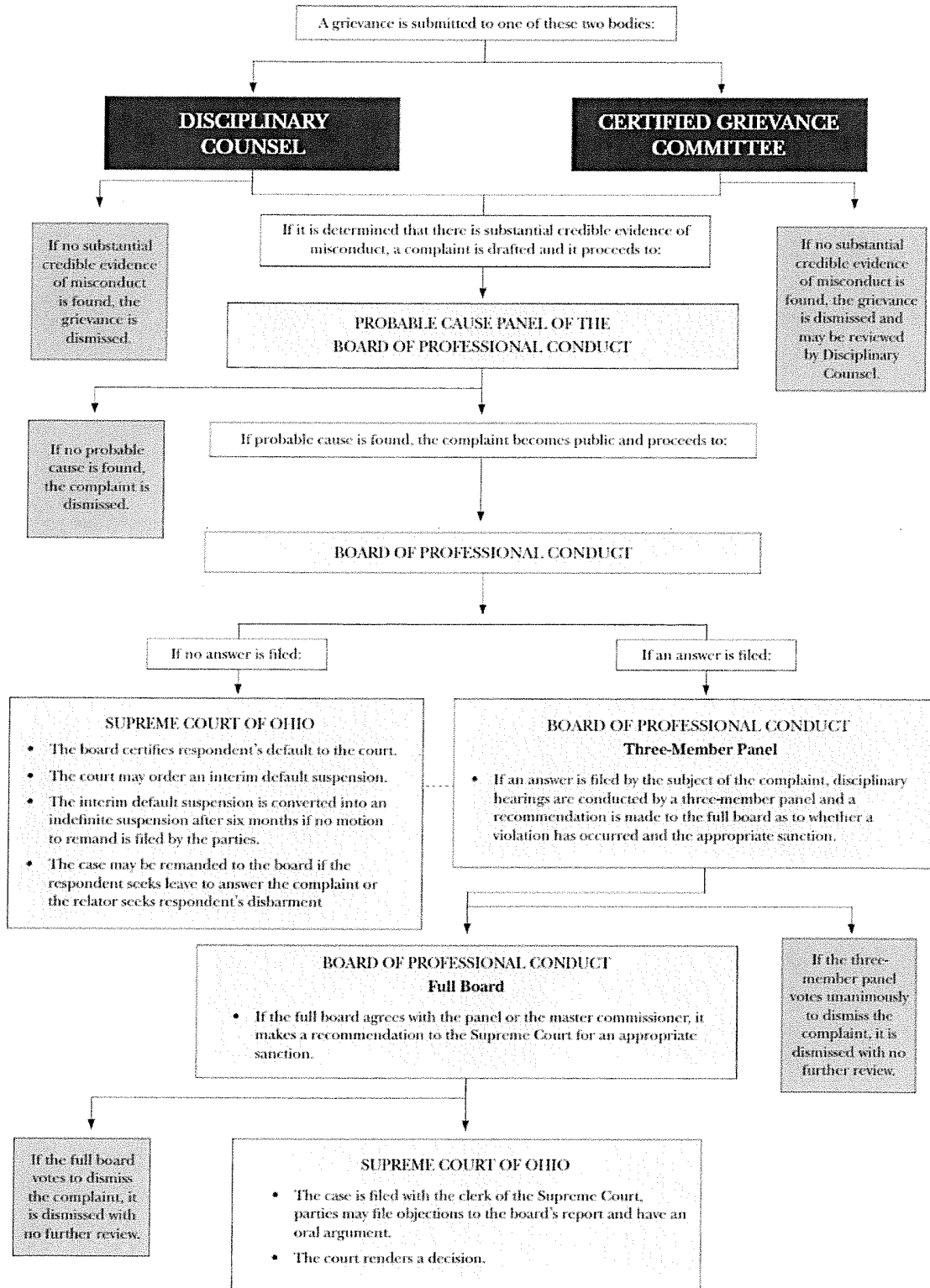
[1] The EEOC does not have enforcement authority for the Congressional Accountability Act (CAA). Thus, the final regulations do not apply to employees or employers covered by this law.

[2] This document uses the term “employer,” but the requirements apply to all covered entities. On February 27, 2024, a federal district court in Texas issued **a permanent injunction** (<https://casetext.com/case/texas-v-garland?q=5:23-CV-034-H&sort=relevance&p=1&type=case>) prohibiting the EEOC from accepting PWFA charges against agencies or divisions of the State of Texas. On June 17, 2024, a federal district court in Louisiana issued **a preliminary injunction** (<https://casetext.com/case/state-v-equal-empt-opportunity-commn>) prohibiting the EEOC from initiating any investigation or issuing notices of right to sue for PWFA charges involving accommodations for abortions “that are not necessary to treat a medical condition related to pregnancy” for employees (a) “whose primary duty station is located in Louisiana or Mississippi,” or (b) who work for the following entities: the State of Louisiana, or any agency thereof; the State of Mississippi, or any agency thereof; the United States Conference of Catholic Bishops; Catholic University of America; the Society of the Roman Catholic Church of the Diocese of Lake Charles; or the Society of the Roman Catholic Church of the Diocese of Lafayette. On September 23, 2024, a federal district court in North Dakota issued a **preliminary injunction** (https://www.eeoc.gov/sites/default/files/2024-10/31%20-%20PI%20Order_508FINAL.pdf) that, in relevant part, prohibits the EEOC from “interpreting or enforcing,” initiating any investigation, or issuing any notice of right to sue for PWFA charges against the Catholic Benefits Association (CBA), the Diocese of Bismarck, CBA members, and those acting in concert with or participating with CBA or a member of CBA, with regard to charges alleging certain

claims related to “abortion or infertility treatments that are contrary to the Catholic faith.”

DISCIPLINARY PROCESS

A grievance against a judge or attorney may be submitted to the Disciplinary Counsel or a certified grievance committee of a local bar association. If either of those bodies determines that substantial credible evidence of professional misconduct exists, a formal complaint is drafted. It then moves to a probable cause panel of the Board of Professional Conduct, which determines if there is probable cause. If the panel determines that there is probable cause, the formal complaint becomes public and is filed with the Board of Professional Conduct. Hearings are then conducted by the board and if it finds a violation, a recommendation is made to the Supreme Court of Ohio. The Supreme Court of Ohio makes the final decision as to findings of misconduct, and issues an appropriate sanction.





Ohio Board of Professional Conduct

[Lawyers](#)

[Judges and Magistrates](#)

[Judicial Candidates](#)

[File a Grievance](#)

[More](#)



[Board Case Docket](#)

[Advisory Opinions](#)

[New Reports Filed
With Supreme Court](#)

[Board Hearing Schedule](#)

[© 2021 Ohio Board of Professional Conduct
Commissioner and Staff Login](#)

[Contact Webmaster](#)



Ohio Board of Professional Conduct

[Lawyers](#)[Judges and Magistrates](#)[Judicial Candidates](#)[File a Grievance](#)[More](#)

Advisory Opinions

Advisory Opinion Process

The Ohio Board of Professional Conduct may issue nonbinding advisory opinions in response to prospective or hypothetical questions from members of the bar and judiciary. Written requests to the Director are reviewed by a committee under the **Standards for Issuing Advisory Opinions**.

The Board is solely responsible for the content of the advisory opinions, and the advice contained in the opinions do not reflect and should not be construed as reflecting the opinion of the Supreme Court of Ohio.

[Search Advisory Opinions](#)

Pending Advisory Opinions

No advisory opinions are pending at this time.

Advisory Opinion Status List

The Advisory Opinion Status List identifies the opinions as "Withdrawn," "Modified," or "Not Current," "CPR Opinion" or other designations as decided upon by the Board.

Advisory Opinion Master Index

The Advisory Opinion Master Index enables opinions to be researched by subject area.

Advisory Opinion Subscription Service

Subscribers receive electronic copies of Advisory Opinions when released by the Board of Professional Conduct.

[Subscribe](#)

Advisory Opinion Inquiries

- **Telephone Inquiries:**
A legal staff member is usually available to discuss ethics questions with judges, lawyers, and judicial candidates.
Call 614.387.9370
- **Written Inquiries:**
Richard A. Dove, Esq., Director
Board of Professional Conduct
65 South Front Street, 5th Floor
Columbus, Ohio 43215-3431



Ohio Board of Professional Conduct

[Lawyers](#)[Judges and Magistrates](#)[Judicial Candidates](#)[File a Grievance](#)[More](#)

Ethics Guides

Ethics Guides address subjects on which the staff of the Ohio Board of Professional Conduct receives frequent inquiries from the Ohio bench and bar. Ethics Guides provide nonbinding advice from the staff of the Board of Professional Conduct and do not reflect the views or opinions of the Ohio Board of Professional Conduct, commissioners of the Board, or the Supreme Court of Ohio.

[Corporate Ethics \(2022\)](#)

[Extrajudicial Activities \(2022\)](#)

[Limited Scope Representation \(2020\)](#)

[Transition from the Practice of Law to the Bench Guide \(2017\)](#)

[Switching Firms Guide \(2017\)](#)

[Succession Planning Guide \(2017\)](#)

[Client File Retention Guide \(2016\)](#)



ETHICS GUIDES

Ethics Guides are copyrighted, but may be used or cited without prior permission for non-commercial purposes, if the Board of Professional Conduct is properly acknowledged as the source of the guide.

For questions about an Ethics Guide, please contact:

D. Allan Asbury, Senior Counsel

Kristi McAnaul, Counsel

[© 2021 Ohio Board of Professional Conduct](#)
[Commissioner and Staff Login](#)

[Contact Webmaster](#)



Ohio Board of Professional Conduct

[Lawyers](#)[Judges and Magistrates](#)[Judicial Candidates](#)[File a Grievance](#)[More](#)

Ohio Disciplinary Decisions

Disciplinary Handbooks contain case summaries of disciplinary decisions issued by the Supreme Court of Ohio.

Annual Handbooks

- Disciplinary Handbook XVIII, Cases 1/2/2024 through 6/30/2024
- Disciplinary Handbook XVII, Cases 1/1/2023 through 12/31/2023
- Disciplinary Handbook XVI, Cases 1/1/2022 through 12/31/2022
- Disciplinary Handbook XV, Cases 1/1/2021 through 12/31/2021
- Disciplinary Handbook XIV, Cases 1/1/2020 through 12/31/2020
- Disciplinary Handbook XIII, Cases 1/1/2019 through 12/31/2019
- Disciplinary Handbook XII, Cases 1/1/2018 through 12/31/2018
- Disciplinary Handbook XI, Cases 1/1/2017 through 12/31/2017
- Disciplinary Handbook X, Cases 1/1/2016 through 12/31/2016
- Disciplinary Handbook IX, Cases 1/1/2015 through 12/31/2015
- Disciplinary Handbook VIII, Cases 1/1/2014 through 12/31/2014
- Disciplinary Handbook Vol. VII, Cases from 1/1/2013 through 12/31/2013
- Disciplinary Handbook Vol. VI, Cases from 1/1/2012 through 12/31/2012

Multi-Year Compilations

- Disciplinary Handbook Compilation, Cases 1/1/2017 through 12/31/2022
- Disciplinary Handbook Vol. V, Cases 2008-2011

[© 2024 Ohio Board of Professional Conduct](#)
[Commissioner and Staff Login](#)

[Contact Webmaster](#)

TABLE OF CONTENTS

[Link is to the beginning of the section]

I. TABLE OF CASES

II. CASE SUMMARIES

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

III. INDEX

AGGRAVATING & MITIGATING FACTORS

CODE OF JUDICIAL CONDUCT VIOLATIONS

CRIMINAL CONDUCT (Felony, Misdemeanor, Treatment in Lieu of Conviction)

DISCIPLINARY PROCEDURAL ISSUES (Aggravation/ Mitigation, Cause
remanded by Court, Consent-to-Discipline, Default, Sanction Increase/ Decrease, Other)

DISCIPLINARY RULE VIOLATIONS

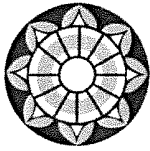
VIOLATIONS OF THE RULES FOR THE GOVERNMENT OF THE BAR

PRIOR DISCIPLINARY RECORD (Attorney Registration, Board Discipline, Other)

PUBLIC EMPLOYEE MISCONDUCT (Judge/ Magistrate/ Clerk, Public Official)

RULES OF PROFESSIONAL CONDUCT VIOLATIONS

SANCTION (Disbarment, Dismissal, Indefinite Suspension, Public Reprimand, Term Suspension)



Ohio Board of Professional Conduct

Disciplinary Case Statistics 2021-2023

Supreme Court Decisions

(excluding defaults and reinstatements)

2021	2022	2023
47	31	22

Sanction Imposed

(excluding defaults)

Public reprimand
Term suspension
Indefinite suspension
Disbarment
Dismissal

2021	2022	2023
10	2	3
29	21	16
5	6	3
3	0	0
0	2	0

Court Action on Board-Recommended Sanction

Imposed recommended sanction

Modified recommended sanction

- Increased
- Decreased

2021	2022	2023
46 (98%)	26 (84%)	18 (82%)
1 (2%)	5 (16%)	4 (18%)
1	2	2
0	3	2

Court Action on Consent to Discipline Cases

(cases in which the Board recommended acceptance)

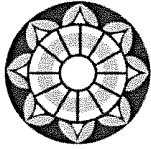
Accept with public reprimand
Accept with term suspension
Rejected and remanded

2021	2022	2023
7	0	3
6	4	1
0	0	0

Default Cases

Total defaults certified to SCO
Interim suspension imposed
Indefinite suspension imposed

2021	2022	2023
3	9	6
2	9	4
7	6	0



Ohio Board of Professional Conduct

Disciplinary Case Statistics 2021-2023

Respondent with Prior Discipline

(includes discipline for misconduct and suspensions for non-compliance with CLE or attorney registration requirements.)

2021	2022	2023
13 (28%)	6 (19%)	4 (18%)

License Reinstatements

Upon application

Upon petition:

- Granted
- Denied
- Withdrawn

2021	2022	2023
14	13	9
4	1	2
0	2	0
1	1	0

Judicial Misconduct Cases (Board Dispositions)

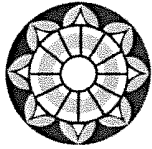
(includes all cases involving violations of the Code of Judicial Conduct when the respondent was a judicial officer or candidate at the time the misconduct occurred.)

	2021	2022	2023*
Total	4	4	5
Rule V cases	3	3	3
Judicial campaign misconduct (expedited)	1	1	2
Dismissals	0	1	1

* Two judicial misconduct cases were pending as of 12/31/2023.

Miscellaneous Disciplinary Dispositions

	2021	2022	2023
Resignations with discipline pending accepted	12	9	9
Resignations with discipline pending denied	0	0	0
Interim remedial suspension imposed	3	3	2
Child support default suspension imposed	1	0	0
Interim felony suspension imposed	3	8	12
Impairment suspension imposed	0	0	2
Reciprocal discipline imposed	4	2	2



Ohio Board of Professional Conduct

Disciplinary Case Statistics 2021-2023

Top Five Disciplinary Offenses of 2023

(based on total number of grievances opened for investigation and primary misconduct alleged)

1. Neglect/failure to protect client's interest
2. Judicial misconduct
3. Excessive fee
4. Misrepresentation/False Statement
5. Trial misconduct/IOLTA (tie)

2023
30%
13%
9%
7%
6%

Active Registered Attorneys

Awards to Victims of Lawyers by Lawyers' Fund for Client Protection

2021	2022	2023
43,626	44,399	43,249
\$545,891	\$998,363	\$749,942

Total Grievances Filed

Disciplinary Counsel (ODC)

Certified Grievance Committees (CGC)

Total Dismissals on Intake*

Dismissed after initial review by ODC

Dismissed after initial review by CGC

Total Grievances Investigated*

Opened for Investigation by ODC

Opened for Investigation by CGC

Complaints filed with the Board

2021	2022**	2023***
3,454	3,697	4,151
2,654 (77%)	2,719 (74%)	3,114 (75%)
801 (23%)	978 (25%)	1,037 (25%)
801	668	646
447 (13%)	285 (8%)	312 (8%)
354 (10%)	383 (10%)	334 (8%)
2,653	3,029	3,505
2,084 (60%)	2,434 (66%)	2,802 (68%)
570 (16%)	595 (16%)	703 (17%)
39	45	45

* Percentages based on total grievances

** 2022 totals do not reflect missing quarterly reports from Miami and Portage grievance committees.

*** 2023 totals do not reflect missing reports from Portage grievance committee.

Ohio Access to Justice Foundation

Attorney Unclaimed Funds

<https://www.ohiojusticefoundation.org/lawyers/unclaimedfunds>

IOLTA/IOTA for Lawyers

<https://www.ohiojusticefoundation.org/lawyers/iolta-iota-for-lawyers>

Retainers

- 1) Classic (deposit into operating account)
- 2) Advance payment (deposit into IOLTA_
 - a. Flat Fee, paid as earned
 - b. Hourly, paid as earned
- 3) Earned upon receipt flat fee (deposit into operating account)
 - a. Rule 1.5(d)(3) – advise in writing “may be entitled to refund”

Malpractice Insurance

Claims made

Report claims and circumstances which may lead to claims

Question in the Application

Does the applicant know of any circumstance, act error, or omission which could result in a professional liability claim made against any lawyer covered in question 1 whether or not a claim has actually been made?

Most policies have disciplinary coverage now with no deductible.

Conflict Waiver
(Informed Consent Confirmed in Writing)

“Informed consent” - the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.” Rule 1.0 (f)

- 1) writing may consist of a document signed by the client or one that the lawyer promptly records and transmits to the client following an oral consent.
- 2) If it is not feasible to obtain or transmit the writing at the time the client gives informed consent, then the lawyer must obtain or transmit it within a reasonable time thereafter.

Make the following a second slide

- 3) Written confirmation of consent does not supplant the need, in most cases, for the lawyer to talk with the client: (1) to explain the risks and advantages, if any, of representation burdened with a conflict of interest, as well as reasonably available alternatives; and (2) to afford the client a reasonable opportunity to consider the risks and alternatives and to raise questions and concerns.
- 4) The writing is required in order to impress upon clients the seriousness of the decision the client is being asked to make and to avoid disputes or ambiguities that might later occur in the absence of written consent. Rule 1.7, Comment 31

Three Documents You Must Have

- 1) Engagement letter or contract
- 2) Document retention policy
- 3) Termination letter

Document Retention Policy

During the course of our work for you on this matter, our office will create and maintain a paper file and an electronic file. Some documents may exist in both files, some in one or the other.

When our work for you on this matter is concluded, we will:

- 1) send you a “closing letter” stating that the representation has ended; and
- 2) return to you all original documents you have provided to us during the course of the representation.

It is our policy to remove and destroy from the paper file all documents that are publicly available. This includes pleadings that have been filed with the court, news articles, etc. We also remove and destroy from the paper file duplicates of documents we also have in electronic form. This may include expert reports, deposition transcripts, discovery responses, medical records, etc. In some cases, a protective order is entered by the court, which requires the return or destruction, at the conclusion of the case, of certain documents produced during the case. If such an order is entered by the court in your case, you will be made aware of it at the time of the order. We will obey any such order and return or destroy the documents as required by the order.

The remainder of our file will be maintained for seven years from the date of the closing letter we send to you. If you want to review the file or obtain a copy of part or all of it, you may do so by sending a written request to one of the attorneys managing your file or their legal assistants.

On or after the seventh anniversary of our closing letter to you, at a time convenient to us, we will destroy the remaining file in a manner designed to ensure confidentiality. If we believe there is a reason to maintain the file for a longer period, we may do so.

If you have any questions about this policy, please contact us to discuss your questions or concerns. By accepting our representation in this matter, you agree to the terms of this policy.

Rev. 6/2020

How Long Must I Keep a File

It Depends

At least 4 years if client not a minor or incompetent

Some parts of some files - 7 years

Section 2305.117 | Action upon a legal malpractice claim.

Ohio Revised Code / Title 23 Courts-Common Pleas /
Chapter 2305 Jurisdiction; Limitation Of Actions

Effective: June 2, 2021 Latest Legislation: House Bill 133, Senate Bill 13 - 134th General Assembly

(A) Except as otherwise provided in this section, an action upon a legal malpractice claim against an attorney or a law firm or legal professional association shall be commenced within one year after the cause of action accrued.

(B) Except as to persons within the age of minority or of unsound mind as provided by section 2305.16 of the Revised Code, and except as provided in divisions (C) and (D) of this section, both of the following apply:

(1) No action upon a legal malpractice claim against an attorney or a law firm or legal professional association shall be commenced more than four years after the occurrence of the act or omission constituting the alleged basis of the legal malpractice claim.

(2) If an action upon a legal malpractice claim against an attorney or a law firm or legal professional association is not commenced within four years after the occurrence of the act or omission constituting the alleged basis of the claim, then, any action upon that claim is barred.

(C)(1) If a person making a legal malpractice claim against an attorney or a law firm or legal professional association, in the exercise of reasonable care and diligence, could not have discovered the injury resulting from the act or omission constituting the alleged basis of the claim within three years after the occurrence of the act or omission, but, in the exercise of reasonable care and diligence, discovers the injury resulting from that act or omission before the expiration of the four-year period specified in division (B)(1) of this section, the

person may commence an action upon the claim not later than one year after the person discovers the injury resulting from that act or omission.

(2) A person who commences an action upon a legal malpractice claim under the circumstances described in division (C)(1) of this section has the affirmative burden of proving, by clear and convincing evidence, that the person, with reasonable care and diligence, could not have discovered the injury resulting from the act or omission constituting the alleged basis of the claim within the three-year period described in that division.

(D) An action upon a legal malpractice claim against an attorney or a law firm or legal professional association arising from an act or omission related to the attorney's, law firm's, or legal professional association's issuance of an opinion of title issued prior to June 16, 2021, shall be commenced within one year after the cause of action accrued without regard to when the act or omission constituting the alleged basis of the legal malpractice claim occurred.

Last updated June 15, 2021 at 5:03 PM

Available Versions of this Section

June 2, 2021 – Amended by House Bill 133, Senate Bill 13 - 134th General Assembly

Confidentiality and Conflict of Interest Policy

The Firm's obligations of confidentiality and avoiding conflicts of interest apply to every employee, not just the attorneys.

Confidentiality

As an employee of the Firm you will have access to: attorney-client communications. This includes correspondence and emails between attorneys of the Firm and clients, as well as communications you have with the client in your capacity as an employee of the Firm; Confidential client information. This includes all information relating to the representation of a client, including but not limited to information provided to the Firm by the client and information gathered by the Firm; attorney work product. This is anything that includes the mental impressions, thoughts, or analysis of an attorney and includes, for example, memoranda, evaluations, reports, mock trial presentations, and mock trial results.

In essence, everything you come into contact with at work must be held in confidence by you and not discussed or shared with anyone other than another employee of the Firm. Even information contained in publicly filed documents or public media is subject to Rule 1.6 of the Rules of Professional Conduct which prohibits the disclosure of information relating to the representation of a client. There is no prohibition and truthfully revealing that the Firm represents a client when the fact of that representation is contained in a publicly filed pleading (When we are counsel of record for a party) or when the representation otherwise cannot reasonably be disputed. However, any discussion of the facts, even as disclosed in the publicly filed documents, must strictly comply with the Rule 1.6 (confidentiality) and Rule 3.6 (trial publicity). The safest course is to simply refrain from discussing the facts of any matter in which we are counsel.

Conflict of Interest




The conflict of interest rules are complicated and conflicts may arise that are not obvious. Non-attorney employees should make an involved attorney aware of any relationship between an employee of the Firm and any party or witness to an open matter. Additionally, if an employee possesses information pertinent to a case that the employee did not obtain through the media or at the Firm, that information should be passed along to an attorney involved in the case.

As an employee of the Firm and an agent of its lawyers, you must adhere to the ethical rules that binds the lawyers. And just like every other topic - if you have questions, ask, don't assume.



Business Blog

Protecting the privacy of health information: A baker's dozen takeaways from FTC cases

By: Elisa Jillson | July 25, 2023 |   

In the past few months, the FTC has announced case after case involving consumers' sensitive health data, alleging violations of both Section 5 of the FTC Act and the FTC's [Health Breach Notification Rule](#). The privacy of health information is top of mind for consumers – and so it's top of mind for the FTC. Companies collecting or using health data, listen up. There are a number of key messages from [BetterHelp](#), [GoodRx](#), [Premom](#), [Vitagene](#), and other FTC matters that you need to hear.

Health Privacy: The Basics

Understand the breadth of "health information." Health information isn't just about medications, procedures, and diagnoses. Rather, it's anything that conveys information – or enables an inference – about a consumer's health. Indeed, *Premom*, *BetterHelp*, *GoodRx*, and [Flo Health](#) make clear that the fact that a consumer is using a particular health-related app or website – one related to mental health or fertility, for example – or how they interact with that app (say, turning "pregnancy mode" on or off) may itself be health information. Our [guidance on health and location](#) highlights the fact that location data can convey health information. For example, repeated trips to a cancer treatment facility may convey highly sensitive information about an individual's health. To stay on the right side of the FTC Act, take a broad view of what constitutes health data and protect it accordingly.

Your obligation to protect the privacy of health information is a given. The need for privacy-by-design is (or should be!) axiomatic at this point, especially when it comes to sensitive personal information. If you're collecting or using consumers' health data, assess and document the risks to that data and implement robust safeguards to protect it, such as a written privacy program, privacy training and supervision, and data retention, purpose, and use limitations. Even if you don't think that's necessary, the FTC may say otherwise, as the complaints in [BetterHelp](#) and [GoodRx](#) show. In those

actions, the FTC specifically alleged that the companies' failure to have appropriate privacy policies and procedures contributed to the alleged unfair privacy practices. To comply with the law, interweave your tech decisions with privacy considerations.

Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers. In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out. *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information. *GoodRx* and *Premom* underscore that this conduct may also violate the [Health Breach Notification Rule](#), which requires notification to consumers, the FTC, and, in some cases, the media, of disclosures of health information without consumers' authorization. Need to understand more about the implications of tracking? Check out [FTC guidance on pixel tracking](#) and [FTC-HHS joint letters to hospitals and telehealth providers](#) for more information on tracking-related privacy concerns.

Don't share consumers' health information improperly – and don't receive it either. After cases like *BetterHelp*, *GoodRx*, *Premom*, and *Flo*, it's pretty clear that unauthorized disclosure of consumers' health information to other companies can land the sender of that data in hot water. But, depending on the facts, the *recipient* of that data could also face liability under Section 5. If you receive information from other companies for advertising or marketing purposes (for example), you may have a responsibility under Section 5 to take steps (such as procedural and technical measures) to ensure you don't engage in the unauthorized receipt, use, or onward disclosure of sensitive information. Merely using a standard, out-of-the-box contract or terms of use to prohibit sending certain information may not be enough.

Insist your technology people and compliance staff communicate about your company's privacy practices. Does the right hand know what the left hand is doing? Companies using tracking technologies sometimes protest that their technical staff used pixels or software development kits without letting their compliance folks know. A key to compliance is to understand *all* of your data flows, regardless of which department or staff is in charge of the data. Start by mapping how data

comes into your company and how it moves once it's there. What are *all* of the sources of the personal information in your company's possession? How are you using and disclosing it? Are your privacy safeguards keeping up with the data flows? Are your promises to consumers consistent with how your business actually uses their information?

HIPAA-related claims

"HIPAA Compliant," "HIPAA Secure," and similar claims may deceive consumers. Compliance with HIPAA, the national law protecting the privacy of certain health information, has become a shorthand among patients and providers alike for health privacy protection. (Of course, businesses should keep in mind that Section 5 of the FTC Act also applies to most entities covered by HIPAA and requires companies to protect the privacy and security of consumers' health information.) Not surprisingly, companies offering health-related products and services often want to tout HIPAA compliance to give consumers comfort – even if these companies aren't actually covered by HIPAA or aren't actually complying with HIPAA. FTC enforcement actions like *GoodRx*, *BetterHelp*, [Henry Schein](#), and [SkyMed](#) make clear that HIPAA claims like that may deceive consumers, whether those consumers are health care providers (like the dentists in *Henry Schein*) or regular people (like the therapy patients in *BetterHelp*). Also, keep in mind that only one government agency – the Department of Health & Human Services' Office for Civil Rights (OCR) – can determine if a company is compliant with HIPAA. Be careful about loose language suggesting some government imprimatur that doesn't exist. Falsely conveying that kind of approval expressly or by implication violates the FTC Act.

Companies that provide HIPAA seals and certifications also may be liable for deceptive claims. Companies that provide certifications and seals about HIPAA compliance to other businesses should be aware of FTC precedent holding purported certifiers liable for deceptive representations. For example, in [Tested Green](#), the FTC alleged that the seller of "green" seals and certifications provided other companies with the means to deceive consumers, because those seals weren't backed up with evidence about real environmental practices. In [ECM](#), the FTC proved in court that a company that gave its business customers labels and certificates bearing false claims about biodegradability had provided "the means and instrumentalities" to deceive downstream consumers. The same principles apply in the health context. If a company provides a health-related seal or certification to others that falsely implies that the recipient is covered by HIPAA, is complying with HIPAA, has been reviewed by a government agency, or has received government approval, both the certifier and the user of that false certification could be subject to FTC enforcement action.

Other Health Privacy Practices

Reserving the right to make big changes to your privacy policy isn't real consent. It may be tempting to use your privacy policy to reserve the right to change your health data practices, so that any continued use of your service constitutes "consent" to the changes. Not so fast. The FTC's action in [Vitagene](#) makes clear that's not a lawful means for obtaining consent for material retroactive privacy policy changes. Importantly, the *Vitagene* complaint, which builds on (and goes beyond) the [Gateway Learning](#) and [Facebook](#) complaints, says the company's material retroactive changes were unfair even though the company had not yet implemented them. *Vitagene* underscores that announcing future broad data-sharing practices in that way can create a likelihood of substantial injury to consumers who never agreed to that sharing. Remember that a touchstone of FTC Act compliance is that consumers – not you – should be in control of their data and empowered to make real decisions about it.

Hidden euphemisms don't cut it. Rather than living up to their legal obligation to tell consumers the whole truth, some companies hide key terms about data practices in dense privacy policies or terms of service filled with ambiguous language that cloaks how they really use consumers' health information. For example, too many companies make enigmatic references in privacy policies to the "disclosure of information about the use of the services" when they should be laying their cards on the table by saying prominently (think front-and-center on the home page) "We share your health information with third-party advertising companies so that we can target you with ads." Euphemisms hidden in privacy policies can be unfair and deceptive. Even if you slip one past consumers, the FTC isn't fooled. The orders in our recent health privacy cases uniformly require affirmative express consent – consent that can be obtained only following a clear and conspicuous disclosure of *all* material facts. Hiding the ball and "clear and conspicuous" don't mesh.

You may be liable under the FTC Act for what you say and for what you *don't* say. You may think the FTC won't come your way because you aren't saying anything wrong, so there's no "deception." Not necessarily so. The FTC's complaints against [BetterHelp](#), [Practice Fusion](#), and [PaymentsMD](#) make clear that you may be deceiving consumers not only by what you say, but also by what you *fail* to say. It's crucial to disclose *all* material information to consumers about how you're using and disclosing their sensitive health information. And *BetterHelp*, [Premom](#), and [GoodRx](#) make clear that if your practices harm consumers, you may face FTC enforcement action, regardless of who said what.

Health privacy: A top priority for the FTC – and for your company

The FTC Act protects biometric data. Since announcing its [Biometric Policy Statement](#) in May, the FTC has brought enforcement actions about voice data ([Amazon/Alexa](#)), video data ([Ring](#)), and DNA information ([Vitagene](#)). DNA data is particularly sensitive because it conveys information not only about you, but also people you're related to. The FTC has also issued guidance about [selling genetic testing kits](#), and *Vitagene* shows that the FTC will back guidance up with enforcement action. As these cases demonstrate, it's of paramount importance that companies collecting this sensitive data keep it safe.

Reproductive information should be protected from prying eyes. It's no coincidence that the FTC has brought two actions focused on fertility apps ([Premom](#) and [Flo](#)) and issued [guidance](#) on reproductive privacy (among other issues). This is an area of crucial importance to consumers – and so it's of crucial importance to us. Companies dealing with this data are on notice that half-measures to protect privacy and security aren't enough.

There's a lot at stake. There's always been a lot at stake for consumers whose health data is exposed or misused. But some stakeholders have said there hasn't been enough at stake for the companies responsible. That argument doesn't hold water in the wake of the FTC's recent series of health and other cases. The *BetterHelp*, *GoodRx*, and *Premom* orders banned those companies from disclosing health data for advertising purposes – a sea change in the current advertising ecosystem. Recent orders have also required companies to pony up major money – from tens of thousands to millions of dollars in consumer redress (*BetterHelp*, *Vitagene*) or civil penalties (*GoodRx*, *PreMom*) – and to instruct recipients to delete data (*BetterHelp*, *GoodRx*, *Premom*, *Flo*) or DNA specimens (*Vitagene*). Other orders have held individuals liable for their companies' security practices ([Drizly](#)) or required companies to delete models and algorithms based on ill-gotten data (*Amazon/Alexa*, *Ring*, [Weight Watchers/Kurbo](#)). The upshot? Violating the law can be an expensive proposition for your company. Think twice (or thrice or more) before making decisions that could harm your customers and land you in legal hot water.



Business Blog

Operation AI Comply: continuing the crackdown on overpromises and AI-related lies

By: Julia Solomon Ensor | September 25, 2024 |   

Maybe you grew up daydreaming about artificial intelligence, or AI. You imagined its potential to change the future, possibly with an army of helpful robots to take on your least favorite human tasks. The Star Wars franchise had R2-D2. The Jetsons had Rosey. There was RoboCop. And when everything else was gone, the world had WALL-E, the stoic trash collector looking for love. Now, as a business owner, you're always watching for the next big invention to fine-tune processes and increase profitability. And some marketers can't resist taking advantage of that by using the language of AI and technology to try to make it seem like their products or services deliver all the answers.

Today, as part of Operation AI Comply, the FTC is [announcing five cases](#) exposing AI-related deception. First, we have four matters involving allegedly deceptive claims about AI-driven services, three of which are oldies but not-so-goodies: deceptive business opportunity scams that claim to use AI to help people earn more money, faster. We also have a settlement involving a company that offered a generative AI tool that let people create fake consumer reviews. Here's what you need to know:

- [DoNotPay](#): An FTC complaint claims U.K.-based DoNotPay told people its online subscription service acts as "the world's first robot lawyer" and an "AI lawyer" by using a chatbot to prepare "ironclad" documents for the U.S. legal system. The complaint also says DoNotPay told small businesses its service could check their websites for law violations and help them avoid significant legal fees. In fact, according to the complaint, DoNotPay's service didn't live up to the hype. You'll have 30 days to comment on a proposed settlement between FTC and DoNotPay, which requires DoNotPay to stop misleading people, pay \$193,000, and tell certain subscribers about the case.

- **[Ascend Ecom](#)**: An FTC complaint filed in California alleges a group of companies and their officers used deceptive earnings claims to convince people to invest in “risk free” business opportunities supposedly powered by AI. Then, when things went sour, the FTC says, the defendants refused to honor their “risk free” money-back guarantees, and threatened and intimidated people to keep them from publishing truthful reviews. According to the complaint, the defendants’ conduct violated the FTC Act, the [Business Opportunity Rule](#), and the [Consumer Review Fairness Act](#).
- **[Ecommerce Empire Builders](#)**: In a complaint filed in Pennsylvania, the FTC claims a company and its officer violated the FTC Act and the [Business Opportunity Rule](#) with their AI-infused earnings claims. According to the complaint, in addition to failing to provide required statements and disclosures, the defendants promised people they would quickly earn thousands of dollars a month in additional income by following proven strategies and investing in online stores “powered by artificial intelligence.” The complaint also says the defendants made clients sign contracts keeping them from writing and posting negative reviews, in violation of the [Consumer Review Fairness Act](#).
- **[FBA Machine](#)**: In June, the FTC filed a complaint against a group of New Jersey-based businesses and their owner, claiming they used deceptive earning claims to convince people to invest in a “surefire” business opportunity supposedly powered by AI. According to the complaint, the defendants promised people they could earn thousands of dollars in passive income. Then, the FTC says, the defendants threatened people who tried to share honest reviews, and told people they couldn’t get refunds unless they withdrew their complaints. According to the FTC, through these tactics, which violate the FTC Act, the [Business Opportunity Rule](#), and the [Consumer Review Fairness Act](#), the defendants defrauded their customers of more than \$15.9 million. The case is ongoing.
- **[Rytr](#)**: According to an FTC complaint, a Delaware-based company sold an AI-enabled writing assistant with a tool specifically designed for its customers to generate online reviews and testimonials. The problem? The complaint says Rytr customers could, with little input, generate an unlimited number of reviews with specific details that would almost certainly not be true for those users. According to the complaint, some Rytr customers used this tool to quickly generate thousands of false reviews that would have tricked people reading those reviews online. This, the FTC says, likely harmed many people and was unfair. Rytr has agreed to a proposed settlement prohibiting the company – or anyone working with it – from advertising or selling any service promoted for generating reviews. You can submit your public comments for 30 days.

So, what’s the takeaway?

First, if you're looking for AI-based tools to use in your business:

- **Be skeptical of AI-related products that claim they can fully replace a qualified human professional.** Firms are rushing to claim that their AI tools can replace the work of doctors, lawyers, and accountants. But when it comes to legal or financial advice, small mistakes lead to big problems, and not every firm can back up their claims with tools that are actually equipped to address complicated, fact-intensive cases. AI tools can be a good starting point, but be skeptical of claims that they can fully replace a professional.
- **Don't take shortcuts on reviews.** You know people read reviews before buying your product or service, and you might be tempted to use AI tools to help you fake your way to five stars. Don't do it. By posting fake reviews you betray your customers' trust and hurt honest businesses trying to compete fairly. And, you may violate the FTC Act and the FTC's [Rule on the Use of Consumer Reviews and Testimonials](#) in the process. We've published a guide with tips on [soliciting and paying for online reviews](#). Check it out and avoid problems.

Second, if you're tempted to mention AI in ads to boost sales:

- **Don't say you use AI tools if you don't.** Easy enough, right? If you're investigated by the FTC, our technologists and others can look at your product or service and figure out what's really going on. Be aware that just using an AI tool when you're developing your product is not the same as offering your customers a product with AI inside. Tell the truth.
- **A lie in robot's clothing is still a lie: the same old advertising principles apply.** The FTC expects you to have a reasonable basis for any claim you make about your product or service. If special rules apply to the product or service you offer, like business opportunities, you must follow those as well. Don't think using technological jargon or saying your product or program relies on AI changes the analysis. When it comes to business opportunities, if the FTC investigates you, we're going to check to see whether you can back up your earnings and other claims, and whether you're supplying appropriate disclosures to your customers. Don't claim your program uses new technologies to help people make more money unless that's true. Have concrete data demonstrating what you're promising is typical for your customers.

Finally, be informed:

- **These cases are just the latest** in the FTC's ongoing work to combat AI-related issues in the marketplace from every angle. We're checking to see whether products or services actually use AI as advertised, if so, whether they work as marketers say




they will. We're examining whether AI and other automated tools are being used for fraud, deception, unfair manipulation, or other harmful purposes. On the back end, we're looking at whether automated tools have biased or discriminatory impacts. You can read about other cases here: [Automators](#), [Career Step](#), [NGL Labs](#), [Rite Aid](#), [CRI Genetics](#).

- **For more information** on how to avoid getting swept up in one of our law enforcement efforts, check out the FTC's **AI and Your Business** series:
 - [Keep your AI claims in check](#)
 - [Chatbots, deepfakes, and voice clones: AI deception for sale](#)
 - [The Luring Test: AI and the engineering of consumer trust](#)
 - [Watching the detectives: Suspicious marketing claims for tools that spot AI-generated content](#)
 - [Can't lose what you never had: Claims about digital ownership and creation in the age of generative AI](#)
 - [Succor borne every minute](#)



Business Blog

Anonymous messaging app targeting teens: Read the disturbing allegations in FTC and Los Angeles DA action against NGL

By: Lesley Fair | July 9, 2024 |   

An anonymous messaging app marketed to kids and teens: What could possibly go wrong? A lot, [allege the FTC and the Los Angeles District Attorney's Office](#). A complaint against NGL Labs and founders Raj Vir and Joao Figueiredo alleges violations of the FTC Act, the Children's Online Privacy Protection Rule (COPPA), the Restore Online Shoppers' Confidence Act (ROSCA), and the California Business and Professions Code. The company also made AI-related claims the complaint challenges as deceptive. The \$5 million financial settlement merits your attention, but it's the permanent ban on marketing anonymous messaging apps to kids or teens that's particularly notable.

Among the most downloaded products in app stores, the NGL app is named for the text shorthand for "Not Gonna Lie," but based on the complaint allegations, it could stand for "Not Gonna be Legal." The app purports to allow users to receive anonymous messages from friends and social media contacts. The defendants expressly pitched it as a "fun yet safe place" for "young people" to "share their feelings without judgment from friends or societal pressures." For parents wary of their kids' use of an anonymous messaging app, the defendants assuaged their concerns by touting "world class AI content moderation" that enabled them to "filter out harmful language and bullying." Consumers who downloaded the app were prompted to create an account that collected a substantial amount of personal information, but NGL didn't ask how old they were and didn't use any form of age screening.

You'll want to read the [complaint](#) for details, but in general terms, app users could post pre-generated prompts to their social media accounts like "Send me a pickup line and I'll tell you if it worked" or "Share an opinion that'll get you cancelled" which allowed viewers of the prompts to write an anonymous message in response. In addition, many users received anonymous messages like "are

you straight?" "I've had a crush on you for years and you still dont know lmao," and "would you say yes if I asked you out – A." When a recipient opened the message, a button appeared inviting the person to find out "Who sent this?" with a paid NGL Pro subscription. Eager to learn the sender's identity, many recipients clicked on that button.

That's the briefest summary of what NGL told users and parents, but a closer look at the six-count [complaint](#) reveals what the FTC and the Los Angeles DA's Office say was really going on behind the scenes.

The FTC challenges the defendants' marketing of its anonymous messaging app to children and teens as an unfair practice. According to the complaint, defendant Figueiredo urged employees to get "kids who are popular to post and get their friends to post" and noted that the "best way is to reach out" on Instagram "by finding popular girls on high school cheer pages." As another NGL executive observed, "We need high schoolers not 20 something[s]." But for any parent of a teenager – or anyone who's been a teenager – the inevitable consequences of an anonymous messaging app targeting teens wouldn't be hard to predict. As one high school assistant principal told the defendants, students were using the app to send "threatening" and "sexually explicit content" that was "significantly affecting the mental health and well-being of our students." According to the complaint, NGL received numerous reports of cyberbullying, harassment, and self-harm and yet chose not to change its marketing strategy or how its product operated.

In addition, the FTC and the Los Angeles DA's Office allege the defendants used multiple misrepresentations to push their app. For example, many of those anonymous messages that users were told came from people they knew – for example, "one of your friends is hiding s[o]mething from u" – were actually fakes sent by the company itself in an effort to induce additional sales of the NGL Pro subscription to people eager to learn the identity of who had sent the message. But even after receiving numerous complaints describing the anonymous messages as "invasive," "anxiety inducing," and "hateful," NGL's in-house response was nothing short of gleeful. The complaint cites the following comment from defendant Figueiredo: "These ppl addicted . . . there's people sharing the [NGL App link] EVERY day and all they get is fake questions 🤔."

The FTC and the Los Angeles DA's Office say NGL's promise to parents to protect kids through the use of "world class AI content moderation" proved misleading, too. According to the complaint, the company's much vaunted AI often failed to filter out harmful language and bullying. It shouldn't take artificial intelligence to anticipate that teens hiding behind the cloak of anonymity would send messages like "You're ugly," "You're a loser," "You're fat," and "Everyone hates you." But a media outlet reported that the app failed to screen out hurtful (and all too predictable) messages of that sort.

What's more, even if users upgraded to NGL Pro, they still wouldn't be told who sent the message, rendering that claim deceptive, too. But that wasn't the only problem with the defendants' practices. According to the complaint, consumers who clicked on the "Who sent this?" button were not clearly told that this was a recurring negative option – not a one-time purchase – and that defendants would charge them \$9.99 (and later \$6.99) *per week* for NGL Pro.

The defendants were well aware of consumer complaints about unexpected charges and the ineffectiveness of the "Who sent this?" feature. Even Apple warned the defendants that their product "attempts to manipulate customers into making unwanted in-app purchases by not displaying the billed amount clearly and conspicuously to the users." How did the defendants respond? In a text discussion with defendants Vir and Figueiredo, NGL's Product Lead succinctly summarized the company's reaction to consumer complaints: "Lo! suckers." According to the FTC, the defendants' use of an online negative option to hype sales of their NGL Pro app violated [ROSCA](#), which requires companies that sell products online with negative options to clearly and conspicuously disclose all material terms of the transaction before obtaining the consumer's billing information and to get the consumer's express informed consent before making the charge.

The FTC also says the company collected and indefinitely stored users' personal data, including their Instagram and Snapchat usernames and profile pictures, information about their location, and their browsing history. The lawsuit alleges the defendants violated the [COPPA Rule](#) by failing to provide proper notice to parents, failing to get verifiable parental consent, and failing to provide a reasonable way for parents to stop further use of or delete the data of kids under 13.

The [complaint](#) also alleges multiple violations of California consumer protection laws.

The [proposed settlement](#) includes a \$5 million financial remedy – \$4.5 million for consumer redress and a \$500,000 civil penalty to the Los Angeles DA's office. But most importantly, the order bans the defendants from offering anonymous messaging apps to kids under 18. How long will that ban be in place? Forever.

Among other things, the settlement requires the defendants to implement an age gate to prevent current and future users under 18 from accessing the app and mandates the destruction of a substantial amount of user information in the defendants' possession. In addition, the defendants must get consumers' express informed consent before billing them for any negative option subscription, must provide a simple mechanism for cancelling those subscriptions, and must send reminders to consumers about negative option charges.

What guidance can other companies take from the settlement?

The FTC will use all of its tools to protect both kids *and* teens. Certainly [COPPA](#) is (and will remain) an important tool for protecting kids under 13 and for ensuring that parents – not tech companies – remain in control of children's personal information. But this action also reinforces the FTC's concern about information practices that pose a risk to teenagers' mental and physical health.

Don't tout your company's use of AI tools if you can't back up your claims with solid proof. The defendants' unfortunately named "Safety Center" accurately anticipated the apprehensions parents and educators would have about the app and attempted to assure them with promises that AI would solve the problem. Too many companies are exploiting the AI buzz *du jour* by making [false or deceptive claims about their supposed use of artificial intelligence](#). AI-related claims aren't puffery. They're objective representations subject to the FTC 's long-standing substantiation doctrine.

There's nothing "LOL-worthy" about ROSCA violations. For decades the FTC has used both the FTC Act and the [Restore Online Shoppers' Confidence Act](#) to fight back against illegal negative options. According to the complaint, the defendants enticed teens with anonymous questions like "would you say yes if I asked you out" and then presented them with that hard-to-resist "Who sent this?" button without clearly explaining that the company was enrolling them in a negative option subscription and charging them every week. That the defendants used this illegal bait-and-switch tactic against teens and then laughed about it adds brazen insult to the financial injury they inflicted.

DC-24-13476

CAUSE NO. _____

IN THE MATTER OF	§	IN THE DISTRICT COURT
	§	
STATE OF TEXAS	§	
	§	
and	§	DALLAS COUNTY, TEXAS
	§	191st
PIECES TECHNOLOGIES, INC.,	§	
Respondent	§	_____ JUDICIAL DISTRICT

**PETITION FOR APPROVAL AND ENTRY OF
ASSURANCE OF VOLUNTARY COMPLIANCE**

TO THE HONORABLE JUDGE OF SAID COURT:

COMES NOW the STATE OF TEXAS, acting by and through the Attorney General of Texas and in accordance with the requirements of the Texas Deceptive Trade Practices - Consumer Protection Act, TEX. BUS. & COM. CODE ANN. §17.58, respectfully files this petition asking the Court to review and approve the attached Assurance of Voluntary Compliance.

As evidenced by their signatures, the Assurance is agreed to by the respective parties.

Respectfully submitted,

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

JAMES LLOYD
Deputy Attorney General for Civil Litigation

RYAN S. BAASCH
Chief, Consumer Protection Division

Tyler Bridegan

TYLER BRIDEGAN

Assistant Attorney General

State Bar No. 24105530

Office of the Texas Attorney General

Consumer Protection Division

808 Travis Street, Suite 1520

Houston, Texas 77002

Email: Tyler.Bridegan@oag.texas.gov

JOHN C. HERNANDEZ

Assistant Attorney General

State Bar No. 24095819

Office of the Texas Attorney General

Consumer Protection Division

112 E. Pecan, Suite 735

San Antonio, Texas 78205

Email: JC.Hernandez@oag.texas.gov

KELLEY OWENS

Assistant Attorney General

State Bar No. 24118105

Consumer Protection Division

Office of the Attorney General of Texas

12221 Merit Drive, Suite 650

Dallas, Texas 75251

Kelley.Owens@oag.texas.gov

Dated: August 21, 2024

ATTORNEYS FOR THE STATE OF TEXAS

DC-24-13476

Cause No. _____

IN THE MATTER OF:

THE STATE OF TEXAS,
Petitioner

IN THE DISTRICT COURT OF

and

PIECES TECHNOLOGIES INC.,
Respondent.

191st DALLAS COUNTY, TEXAS
____ JUDICIAL DISTRICT

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance (“Assurance”) is made and entered into by and between Texas Attorney General Ken Paxton acting in the name of the State of Texas (“Petitioner” or “State”), by and through the Consumer Protection Division and Pieces Technologies, Inc. (“Respondent” or “Pieces,” and collectively with the State, the “Parties”), pursuant to Tex. Bus. & Com. Code § 17.58.

I. STIPULATIONS

1. This Court has jurisdiction over the subject matter at issue here as well as the Parties named in this matter.
2. The Consumer Protection Division of the Office of the Attorney General of Texas is authorized to investigate alleged violations of the Texas Deceptive Trade Practices – Consumer Protection Act (“DTPA”), Tex. Bus. & Com. Code §§ 17.41-.63, and to bring actions pursuant to Section 17.47 of the DTPA.
3. This Assurance is being entered into by the Parties for the sole purpose of compromising disputed claims by the State without the necessity for protracted and expensive litigation.

4. The Parties agree to the terms of this Assurance, and the Parties are fully authorized to sign and enter into this Assurance.
5. Respondent further acknowledges receipt of this Assurance and has full and actual notice of its terms.
6. This Assurance does not constitute an admission by Respondent of any violation of law, rule, or regulation, including and without limitation, the DTPA, and Respondent expressly denies any such liability for, violation of, or noncompliance with any such law, rule, or regulation.
7. Respondent waives all rights to appeal or otherwise challenge or contest the validity of this Assurance.

II. DEFINITIONS

8. “Marketing” and “advertising” means a communication by Respondent or a person acting on Respondent’s behalf in any medium intended to induce a person or entity to obtain products or services.
9. “Clear and conspicuous” means a disclosure that is easily noticeable and easily understandable by ordinary persons.

III. PARTIES

10. Respondent is Pieces Technologies, Inc., a registered Texas Foreign For-Profit Corporation, and its agents, successors, and assigns. Its principal place of business is located at 5201 N O’Connor Blvd., 300, Irving, Texas 75039.
11. Petitioner is the State of Texas acting by and through the Consumer Protection Division of the Office of the Attorney General as authorized under the DTPA, § 17.14-.63.

IV. ALLEGATIONS OF THE STATE OF TEXAS

12. Respondent currently operates an artificial intelligence-focused technology company in Texas that develops, markets, and deploys products and services for use by in-patient healthcare facilities, like hospitals. Its product offerings include, but are not limited to, generative artificial intelligence (“AI”) products. According to Respondent’s website, its products, among other things, are meant to be relied on by physicians and other medical staff to assist them with treating their patients (“Pieces summarizes, charts, and drafts clinical notes for your doctors and nurses in the [Electronic Health Record] – so they don’t have to.”).
13. To advertise and market its in-patient healthcare products and services, Respondent developed a series of metrics and benchmarks purporting to show that the outputs of its generative AI products were highly accurate. Many of Respondent’s “metrics” incorporated the word “hallucination,” which is a term commonly used to describe the phenomena of generative AI products creating an output that is incorrect or misleading. Specifically, Respondent advertised and marketed the accuracy of its products and services by claiming that they have a “critical hallucination rate” and “severe hallucination rate” of “<.001%” and “<1 per 100,000.”
14. The State alleges that Respondent’s representations regarding its generative AI products may have violated the DTPA because they were false, misleading, or deceptive.

V. RESPONDENT'S RESPONSE

15. Respondent denies any wrongdoing or liability and contends that it has not engaged in conduct that violates Texas law, including the DTPA, and that it has accurately set forth and represented its hallucination rate.

VI. RESPONDENT'S ASSURANCES

16. Respondent hereby agrees and voluntarily assures the State that it will comply with the provisions contained herein for the five (5) years after the effective date of this Assurance. This Assurance shall automatically terminate five (5) years after its effective date.
17. **Clear and Conspicuous Disclosures – Marketing and Advertising.** If in marketing or advertising its products and services Respondent includes direct or indirect statements regarding any metrics, benchmarks, or similar measurements describing the outputs of its generative AI products, Respondent must clearly and conspicuously disclose (1) the meaning or definition of such metric, benchmark, or similar measurement; and (2) the method, procedure, or any other process used by Respondent, or on Respondent's behalf, to calculate the metric, benchmark, or similar measurement used in Respondent's marketing or advertising of its products and services.
 - a) alternatively, Respondent may retain an independent, third-party auditor to assess, measure, or substantiate the performance or characteristics of its products and services, and all direct or indirect statements included in Respondent's marketing or advertising of its products and services must be consistent with, and substantiated by, the independent, third-party auditor's findings.

18. **Prohibitions Against Misrepresentations.** Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, whether acting directly or indirectly, must not:
- a) in connection with any product or service, make any false, misleading, or unsubstantiated representations, whether expressly or by implication, regarding any feature, characteristic, function, testing or appropriate use of any of its products, including, but not limited to, representations related to:
 - i. the accuracy, reliability, or efficacy of any of its products;
 - ii. the procedures and methodologies used to test its products;
 - iii. the procedures and methodologies used to monitor its products;
 - iv. the definition and/or meaning of any metrics used by Respondent; and
 - v. the data used by Respondent to train any of its products;
 - b) misrepresent or mislead, in any way, any customer or user of its products or services regarding the accuracy, functionality, purpose, or any other feature of its products; or
 - c) fail to disclose any financial or similar arrangements between Respondent and any person who, whether orally or in writing, participates in Respondent's marketing and advertising, or otherwise endorses or promotes any of Respondent's products or services.
19. **Clear and Conspicuous Disclosures – Customers.** Respondent must provide all its current and future customers, in connection with any of its products or services, documentation that clearly and conspicuously discloses any known or reasonably

knowable harmful or potentially harmful uses or misuses of its products or services.

This documentation must, at a minimum, include the following information:

- a) the type of data and/or models used to train its products and services;
- b) a detailed explanation of the intended purpose and use of its products and services, as well as any training or documentation needed to facilitate proper use of its products and services;
- c) any known, or reasonably knowable, limitations of its products or services, including risks to patients and healthcare providers from the use of the product or service, such as the risk of physical or financial injury in connection with a product or service's inaccurate output;
- d) any known, or reasonably knowable, misuses of a product or service that can increase the risk of inaccurate outputs or increase the risk of harm to individuals; and
- e) for each product or service, all other documentation reasonably necessary for a user to understand the nature and purpose of an output generated by a product or service, monitor for patterns of inaccuracy, and reasonably avoid misuse of the product or service.

20. **Acknowledgements of the Order.** Respondent must deliver a copy of this Assurance to: (1) all of its principals, officers, and directors; (2) all of its employees having managerial responsibilities for conduct related to the subject matter of this Assurance and all agents and representatives who participate in conduct related to the subject matter of this Assurance; and (3) any business entity resulting from any change in structure of Respondent.

- a) Delivery of this Assurance must occur within twenty (20) business days after the effective date of this Assurance for current personnel. For all others, delivery must occur before they assume their responsibilities.
- 21. **Compliance Monitoring.** Within thirty (30) business days of receipt of a written request from a representative of the State for information related to Respondent's compliance with any specific provision of this Assurance, Respondent must submit any requested information, which must be sworn under penalty of perjury, appear for depositions, or produce records for inspection and copying.

VII. RELEASE

- 22. This Assurance constitutes a complete settlement and release by the State of all claims that the State could have brought against Respondent based on the facts alleged herein.

VIII. GENERAL PROVISIONS

- 23. **Court Approval:** Respondent and Petitioner agree that the Attorney General will submit this Assurance to a district court of competent jurisdiction in Dallas County and request that the court approve this Assurance, pursuant to the terms set forth herein and Section 17.58 of the DTPA.
- 24. **No Private Right of Action:** Nothing in this Assurance shall create any private rights, causes of action, or remedies against Respondent and nothing in the Assurance shall be construed as a waiver of any private rights, causes of action, or remedies of any person against Respondent with respect to the practices or conduct described herein.
- 25. **Past and Future Practices:** Nothing herein constitutes approval or acquiescence by the State of Respondent's past practices, current efforts to reform their practices, or any future practices that Respondent may adopt or consider adopting. The State's decision

to enter into this Assurance or to limit current or future enforcement action otherwise unilaterally does not constitute approval or imply authorization for any past, present, or future business practice, nor may Respondent advertise or represent that the State approves or authorizes any of its past, present, or future business practices.

26. **Preservation of Future Enforcement Action:** Respondent and Petitioner agree that nothing in this Assurance shall be construed to affect any action or proceeding by any regulatory body or state agency, whether such action or proceeding is related to any issue addressed by this Assurance or otherwise.
27. **No Circumvention:** Respondent shall not participate, directly or indirectly, in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited in this Assurance or for any other purpose that would otherwise circumvent any part of this Assurance or the spirit or purposes of this Assurance.
28. **Authority:** The corporate signatory hereto is a corporate officer for the Respondent who is authorized to enter into this Assurance and has read this Assurance and agrees to entry of same.
29. **Conflict of Other Law:** To the extent that the provisions of this Assurance conflict with any Texas, local, or federal law or regulation that now exists, or is later enacted or amended, such law or regulation, and not this Assurance, shall apply. For the purpose of this Assurance, such conflict exists if conduct prohibited by this Assurance is required or expressly permitted by such Texas, local, or federal law or regulation, or if conduct required by this Assurance is prohibited by such Texas, local, or federal law or regulation.

30. **Entire Agreement:** This Assurance sets forth the entire agreement between the Parties. Respondent represents that Respondent has fully read and understands this Assurance, accepts the legal consequences involved in signing this Assurance, and that there are no other representations or agreements between the Parties not stated in writing herein.
31. **Modification or Rescission:** Respondent may request that this Assurance be modified at any time and may request that this Assurance be rescinded no earlier than one (1) year from its effective date. Such request must be in writing, addressed to the Chief of the Consumer Protection Division, and include a brief statement of the basis for the request. If the State, in its sole discretion, determines that modification or rescission is appropriate, the Parties shall enter into an agreement to rescind or modify this Assurance and file a notice and the agreement with the Court. The Parties acknowledge that factors bearing on modification or rescission may include, but are not limited to: (1) Respondent's full and complete compliance with this Assurance; (2) changes in the regulatory landscape, such as the promulgation of new state or federal laws or regulations; and (3) changes or developments in generative AI technology and related industry standards, metrics, benchmarks, or similar measurements describing the outputs of generative AI products.
32. **Written Agreement.** The Parties agree that this Assurance shall not be modified or rescinded except by written agreement signed by the Parties and filed with the Court as described in the preceding paragraph.
33. **Assessment of Court Costs:** The Parties shall bear their own costs.
34. **Effective Date:** The effective date of this Assurance is the date the Assurance is approved by the Court.

APPROVED AS TO FORM AND SUBSTANCE AND ENTRY REQUESTED:

PETITIONER:

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

JAMES LLOYD
Deputy Attorney General for Civil Litigation

RYAN S. BAASCH
Chief, Consumer Protection Division

DATE: August 21, 2024

/s/ *Tyler Bridegan*

TYLER BRIDEGAN
Assistant Attorney General
State Bar No. 24105530

Office of the Attorney General of Texas
Consumer Protection Division
P.O. Box 12548, Capitol Station
Austin, Texas 78711-2548
Tyler.Bridegan@oag.texas.gov

COUNSEL FOR PETITIONER, THE STATE OF TEXAS

APPROVED AS TO FORM AND SUBSTANCE AND ENTRY REQUESTED:

RESPONDENT:

Ruben Amarasingham
RUBEN AMARASINGHAM
CEO
Pieces Technologies Inc.

5201 N O'Connor Blvd., 300
Irving, Texas 75039

REPRESENTATIVE FOR RESPONDENT

DATE: August 5, 2024

Zach Mayer
ZACH MAYER
Mayer LLP
State Bar No. 24013118

750 N. Saint Paul Street, Suite 700
Dallas, Texas 75201
(214) 379-6900
zmayer@mayerllp.com

William B. Mateja
WILLIAM B. MATEJA
Sheppard, Mullin, Richter & Hampton LLP
State Bar No. 13185350
JASON HOGGAN
State Bar No. 24083188

2200 Ross Ave.
Dallas, TX 75201
(469) 391-7415
bmateja@sheppardmullin.com
jhoggan@sheppardmullin.com

ATTORNEYS FOR RESPONDENT

DATE: August 5, 2024

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Zoann Willis on behalf of Tyler Bridegan
Bar No. 24105530
zoann.willis@oag.texas.gov
Envelope ID: 91180403
Filing Code Description: Original Petition
Filing Description:
Status as of 8/28/2024 8:42 AM CST

Associated Case Party: STATE OF TEXAS

Name	BarNumber	Email	TimestampSubmitted	Status
Esther Chavez		esther.chavez@oag.texas.gov	8/21/2024 4:24:27 PM	SENT
Tyler Bridegan		tyler.bridegan@oag.texas.gov	8/21/2024 4:24:27 PM	SENT
JC Hernandez		jc.hernandez@oag.texas.gov	8/21/2024 4:24:27 PM	SENT
Kelley Owens		kelley.owens@oag.texas.gov	8/21/2024 4:24:27 PM	SENT

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Rebecca Herrmann		rebecca.herrmann@oag.texas.gov	8/21/2024 4:24:27 PM	SENT

Associated Case Party: PIECES TECHNOLOGIES INC.

Name	BarNumber	Email	TimestampSubmitted	Status
Zachary Mayer	24013118	zmayer@mayerllp.com	8/21/2024 4:24:27 PM	SENT
William Mateja	13185350	bmateja@sheppardmullin.com	8/21/2024 4:24:27 PM	SENT



Department of Financial Services

Attorney General James and DFS Superintendent Harris Secure \$11.3 Million from Auto Insurance Companies over Data Breaches



SHARE

Reports and Publications

Attorney General James and DFS Superintendent Harris Secure \$11.3 Million from Auto Insurance Companies over Data Breaches

GEICO and Travelers' Poor Data Security Allowed Hackers to Steal New Yorkers' Driver's License Numbers and Fraudulently Obtain Unemployment Benefits

November 25, 2024

NEW YORK – New York Attorney General Letitia James and New York State Department of Financial Services (DFS) Superintendent Adrienne A. Harris today secured \$11.3 million in penalties from two auto insurance companies, the Government Employees Insurance Company (GEICO) and The Travelers Indemnity Company (Travelers), for having poor data security which led to the personal information of more than 120,000 New Yorkers being compromised. These events were part of an industry-wide campaign by hackers to steal consumers' personal information, including driver's license numbers and dates of birth, from online automobile insurance quoting applications, including those used by GEICO and Travelers. The hackers then used some of the stolen driver's license information to file fraudulent unemployment claims at the height of the COVID-19 pandemic. The OAG investigation concluded that the auto insurance companies did not implement sufficient data security controls to protect consumers' private information. The DFS investigation concluded that the auto insurance companies did not comply with DFS's cybersecurity regulation that requires them to implement policies, procedures, and controls designed to protect consumer data and the financial institutions themselves. As a result of today's settlements, GEICO will pay \$9.75 million in penalties and Travelers will pay \$1.55 million.

"GEICO and Travelers offer drivers protection during times of emergencies, but these companies failed to protect consumers' personal information," **said Attorney General James.** "Data breaches can lead to serious fraud, and that is why it is important for all companies to take cybersecurity and data protection seriously. I thank the Department of Financial Services and the Department of Labor for their partnership and continued work to hold companies accountable when they fail to protect consumers."

"DFS's groundbreaking cybersecurity regulation establishes a vital foundation for ensuring the safety of sensitive consumer data and the resilience of financial institutions," **said Superintendent Harris.** "These enforcement actions reinforce the Department's commitment to ensuring that all licensees, especially those entrusted with consumer financial information like GEICO and Travelers, uphold their duty to implement robust measures that shield New Yorkers from potential data breaches and cyber threats. I thank the Attorney General's office for their coordination during these investigations."

Starting in November 2020, GEICO experienced a series of cyberattacks on its auto insurance quoting tools. Hackers were able to obtain New Yorkers' driver's license numbers from GEICO's publicly-facing website because GEICO failed to protect this information on the website's back

end. Despite being notified by DFS of an industry-wide cyberattack campaign to obtain driver's license numbers, and suffering, disclosing, and remediating separate cybersecurity incidents, GEICO failed to conduct a comprehensive review of its systems to prevent and detect future cyberattacks. After GEICO remediated its website vulnerabilities, hackers exploited vulnerabilities in GEICO's insurance agents' quoting tool, a separate platform from the consumer-facing insurance quotes website. The personal information of approximately 116,000 New York residents was exposed in the GEICO cyberattacks, with the vast majority being lifted from GEICO's insurance agents' quoting tool. Some of the exposed data was later used to file unemployment claims during the COVID-19 pandemic.

Travelers experienced a cyberattack on its auto insurance quoting tool for independent agents. Between January and April 2021, Travelers received several industry alerts warning that hackers were obtaining driver's license numbers through insurance quoting tools. In April 2021, hackers gained access to Travelers' agent portal through the use of compromised agent credentials, which allowed users to generate reports that included consumers' full driver's license numbers in plain text. The insurance agent portal was password protected but did not use multifactor authentication or any other compensating controls, making it easier to exploit. Travelers did not detect the breach of its agent portal for more than seven months and was alerted to the attack by a third-party prefill data provider. The Travelers attack exposed the personal information of approximately 4,000 New Yorkers.

Today's agreements require GEICO and Travelers to significantly enhance their security and pay penalties to the state. GEICO will pay \$9,750,000 in penalties, of which OAG secured \$4,750,000 and DFS secured \$5 million. Travelers will pay \$1,550,000 in penalties, of which OAG secured \$350,000 and DFS secured \$1,200,000.

In addition to the penalties, the OAG settlement agreement requires the companies to adopt a series of measures aimed at strengthening their cybersecurity practices going forward, including:

- Maintaining a comprehensive information security program designed to protect the security, confidentiality, and integrity of private information;
 - Developing and maintaining a data inventory of private information and ensuring the information is protected by safeguards;
 - Maintaining reasonable authentication procedures for access to private information;
 - Maintaining a logging and monitoring system, as well as reasonable policies and procedures designed to properly configure such system to alert on suspicious activity;
- and

- Enhancing their threat response procedures.

As part of this settlement with DFS, Geico agreed to conduct remedial measures, including a comprehensive cybersecurity risk assessment and penetration testing, and the development of an action plan to address any resulting concerns. Travelers agreed to review its systems, assess access controls, and improve protections against unauthorized access to NPI (nonpublic personal information).

Since the implementation of the Cybersecurity Regulation and under Superintendent Harris, DFS has entered into consent orders with 12 entities for violations resulting in over 100 million in fines for New York State. DFS's Cybersecurity Regulation became effective in March 2017, with an updated amendment effective as of November 2023 designed to enhance cyber governance, mitigate risks, and strengthen protections for New York businesses and consumers against cyber threats. It has served as a model for other regulators, including the U.S. Federal Trade Commission, multiple states, the National Association of Insurance Commissioners (NAIC), and the CSBS Nonbank Model Data Security Law.

Attorney General James thanks the New York State Department of Labor's Office of Special Investigations for their work on this matter.

Attorney General James has taken several actions to hold companies accountable for having poor cybersecurity and to improve data security practices. In October 2024, Attorney General James [secured \\$2.25 million from a Capital Region health care provider](#) for failing to protect the private information and medical data of New Yorkers. In August 2024, Attorney General James and a multistate coalition [secured \\$4.5 from a biotech company](#) for failing to protect patient data. In July, Attorney General James launched two privacy guides, [a Business Guide to Website Privacy Controls](#) and [a Consumer Guide to Tracking on the Web](#), to help businesses and consumers protect themselves. In July, Attorney General James also [issued a consumer alert](#) to raise awareness about free credit monitoring and identity theft protection services available for millions of consumers impacted by the Change Healthcare data breach. In April 2023, Attorney General James [released a comprehensive data security guide](#) to help companies strengthen their data security practices. In January 2022, Attorney General James released [a business guide for credential stuffing attacks](#) that detailed how businesses could protect themselves and consumers.

Read the DFS GEICO and Travelers [consent orders](#).



Artificial Intelligence – Questions and Answers*

Brussels, 1 August 2024

Why do we need to regulate the use of Artificial Intelligence?

The EU AI Act is the world's first comprehensive AI law. It aims to address risks to health, safety and fundamental rights. The regulation also protects democracy, rule of law and the environment.

The uptake of AI systems has a strong potential to bring societal benefits, economic growth and enhance EU innovation and global competitiveness. However, in certain cases, the specific characteristics of certain AI systems may create new risks related to user safety, including physical safety, and fundamental rights. Some powerful AI models that are being widely used could even pose systemic risks.

This leads to legal uncertainty and potentially slower uptake of AI technologies by public authorities, businesses and citizens, due to the lack of trust. Disparate regulatory responses by national authorities would risk fragmenting the internal market.

Responding to these challenges, legislative action was needed to ensure a well-functioning internal market for AI systems where both benefits and risks are adequately addressed.

To whom does the AI Act apply?

The legal framework will apply to both public and private actors inside and outside the EU as long as the **AI system** is placed on the Union market, or its use has an impact on people located in the EU.

The obligations can affect both providers (e.g. a developer of a CV-screening tool) and deployers of AI systems (e.g. a bank buying this screening tool). There are certain exemptions to the regulation. Research, development and prototyping activities that take place before an AI system is released on the market are not subject to these regulations. Additionally, AI systems that are exclusively designed for military, defense or national security purposes, are also exempt, regardless of the type of entity carrying out those activities.

What are the risk categories?

The AI Act introduces a uniform framework across all EU Member States, based on a forward-looking definition of AI and a risk-based approach:

- **Unacceptable risk:** A very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights and will therefore be banned:
 - **Exploitation of vulnerabilities of persons, manipulation and use of subliminal techniques;**
 - **Social scoring** for public and private purposes;
 - **Individual predictive policing** based solely on profiling people;
 - **Untargeted scraping** of internet or CCTV for facial images to build-up or expand databases;
 - **Emotion recognition in the workplace and education institutions**, unless for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot);
 - **Biometric categorisation** of natural persons to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation. Labelling or filtering of datasets and categorising data in the field of law enforcement will still be possible;
 - **Real-time remote biometric identification in publicly accessible spaces by law enforcement**, subject to narrow exceptions (see below).
- The Commission will issue guidance on the prohibitions prior to their entry into force on 2 February 2025.

- **High-risk:** A limited number of AI systems defined in the proposal, potentially creating an adverse impact on people's safety or their fundamental rights (as protected by the EU Charter of Fundamental Rights), are considered to be high-risk. Annexed to the Act are the lists of high-risk AI systems, which can be reviewed to align with the evolution of AI use cases.
- These also include safety components of products covered by sectorial Union legislation. They will always be considered high-risk when subject to third-party conformity assessment under that sectorial legislation.
- Such high-risk AI systems include for example AI systems that assess whether somebody is able to receive a certain medical treatment, to get a certain job or loan to buy an apartment. Other high-risk AI systems are those being used by the police for profiling people or assessing their risk of committing a crime (unless prohibited under Article 5). And high-risk could also be AI systems operating robots, drones, or medical devices.
- **Specific transparency risk:** To foster trust, it is important to ensure transparency around the use of AI. Therefore, the AI Act introduces specific transparency requirements for certain AI applications, for example where there is a clear risk of manipulation (e.g. via the use of chatbots) or deep fakes. Users should be aware that they are interacting with a machine.
- **Minimal risk:** The majority of AI systems can be developed and used subject to the existing legislation without additional legal obligations. Voluntarily, providers of those systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

In addition, the AI Act considers **systemic risks** which could arise from **general-purpose AI models**, including **large generative AI models**. These can be used for a variety of tasks and are becoming the basis for many AI systems in the EU. Some of these models could carry systemic risks if they are very capable or widely used. For example, powerful models could cause serious accidents or be misused for far-reaching cyberattacks. Many individuals could be affected if a model propagates harmful biases across many applications.

How do I know whether an AI system is high-risk?

The AI Act sets out a solid methodology for the classification of AI systems as high-risk. This aims to provide legal certainty for businesses and other operators.

The risk classification is based on the intended purpose of the AI system, in line with the existing EU product safety legislation. It means that the classification depends on the function performed by the AI system and on the specific purpose and modalities for which the system is used.

AI systems can classify as high-risk in two cases:

- If the AI system is embedded as a safety component in products covered by existing product legislation (Annex I) or constitute such products themselves. This could be, for example, AI-based medical software.
- If the AI system is intended to be used for a high-risk use case, listed in an Annex III to the AI Act. The list includes use cases from in areas such as education, employment, law enforcement or migration.

The Commission is preparing guidelines for the high-risk classification, which will be published ahead of the application date for these rules.

What are examples for high-risk use cases as defined in Annex III?

Annex III comprises eight areas in which the use of AI can be particularly sensitive and lists concrete use cases for each area. An AI system classifies as high-risk if it is intended to be used for one of these use cases.

Examples are:

- AI systems used as safety components in certain **critical infrastructures** for instance in the fields of road traffic and the supply of water, gas, heating and electricity;
- **AI systems used in education and vocational training**, e.g. to evaluate learning outcomes and steer the learning process and monitoring of cheating;
- **AI systems used in employment and workers management** and access to self-employment, e.g. to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
- **AI systems used in the access to essential private and public services** and benefits (e.g. healthcare), **creditworthiness evaluation** of natural persons, and risk assessment and pricing in relation to **life and health insurance**;

- AI systems used in the fields of **law enforcement**, migration and **border control**, insofar as not already prohibited, as well as in administration of **justice** and **democratic processes**;
- AI systems used for **biometric identification, biometric categorisation and emotion recognition**, insofar as not prohibited.

What are the obligations for providers of high-risk AI systems?

Before **placing a high-risk AI system on the EU market** or otherwise putting it into service, providers must subject it to a **conformity assessment**. This will allow them to demonstrate that their system complies with the mandatory requirements for trustworthy AI (e.g. data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness). This assessment has to be repeated if the system or its purpose are substantially modified.

AI systems that serve as safety components of products covered by sectorial Union legislation will always be deemed high-risk when subject to third-party conformity assessment under that sectorial legislation. Moreover, all biometric systems, regardless of their application, will require third-party conformity assessment.

Providers of high-risk AI systems will also have to **implement quality and risk management systems** to ensure their compliance with the new requirements and minimise risks for users and affected persons, even after a product is placed on the market.

High-risk AI systems that are deployed by public authorities or entities acting on their behalf will have to be **registered in a public EU database**, unless those systems are used for law enforcement and migration. The latter will have to be registered in a non-public part of the database that will be only accessible to relevant supervisory authorities.

To ensure compliance throughout the lifecycle of the AI system, market surveillance authorities will conduct regular audits and facilitate post-market monitoring and will allow providers to voluntarily report any serious incidents or breaches of fundamental rights obligations that come to their attention. In exceptional cases, authorities may grant exemptions for specific high-risk AI systems to be placed on the market.

In case of a breach, the requirements will allow national authorities to have access to the information needed to investigate whether the use of the AI system complied with the law.

What would be the role of standardisation in the AI Act?

Under the AI Act, high-risk AI systems will be subject to specific requirements. European harmonised standards will play a key role in the implementation of these requirements.

In May 2023, the European Commission mandated the European standardisation organisations CEN and CENELEC to develop standards for these high-risk requirements. This mandate will now be amended, to align with the final text of the AI Act.

The European standardisation organisations will have until the end of April 2025 to develop and publish standards. The Commission will then evaluate and possibly endorse these standards, which will be published in the EU's Official Journal. Once published, those standards will grant a "presumption of conformity" to AI systems developed in accordance with them.

How are general-purpose AI models being regulated?

General-purpose AI models, including **large generative AI models**, can be used for a variety of tasks. Individual models may be integrated into a large number of AI systems.

It is crucial that a provider of an AI system integrating a general-purpose AI model has access to all necessary information to ensure the system is safe and compliant with the AI Act.

Therefore, the AI Act obliges providers of such models to **disclose certain information to downstream system providers**. Such **transparency** enables a better understanding of these models.

Model providers additionally need to have policies in place to ensure that they **respect copyright law** when training their models.

In addition, some of these models could pose **systemic risks**, because they are very capable or widely used.

Currently, general purpose AI models that were trained using **a total computing power of more than 10²⁵ FLOPs** are considered to pose systemic risks. The Commission may update or

supplement this threshold in light of technological advances and may also designate other models as posing systemic risks based on further criteria (e.g. number of users, or the degree of autonomy of the model).

Providers of models with systemic risks are obliged to **assess and mitigate risks, report serious incidents, conduct state-of-the-art tests and model evaluations** and ensure **cybersecurity** of their models.

Providers are invited to collaborate with the AI Office and other stakeholders to develop a Code of Practice, detailing the rules and thereby ensuring the safe and responsible development of their models. This Code should represent a central tool for providers of general-purpose AI models to demonstrate compliance.

Why is 10²⁵ FLOPs an appropriate threshold for GPAI with systemic risks?

FLOP is a proxy for model capabilities, and the exact FLOP threshold can be updated upwards or downwards by the Commission, e.g. in the light of progress in objectively measuring model capabilities and of developments in the computing power needed for a given performance level.

The capabilities of the models above this threshold are not yet well enough understood. They could pose systemic risks, which is why it is reasonable to subject their providers to the additional set of obligations.

What are the obligations regarding watermarking and labelling of the AI outputs set out in the AI Act?

The AI Act sets transparency rules for the content produced by generative AI to address the risk of manipulation, deception and misinformation.

It obliges providers of generative AI systems to mark the AI outputs in a machine-readable format and ensure they are detectable as artificially generated or manipulated. The technical solutions must be effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.

In addition, deployers of generative AI systems that generate or manipulate image, audio or video content constituting deep fakes must visibly disclose that the content has been artificially generated or manipulated. Deployers of an AI system that generates or manipulates text published with the purpose of informing the public on matters of public interest must also disclose that the text has been artificially generated or manipulated. This obligation does not apply where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content.

The AI Office will issue guidelines to provide further guidance for providers and deployers on the obligations in Article 50 which will become applicable two years after entry into force of the AI Act (on 2 August 2026).

The AI Office will also encourage and facilitate the development of Codes of Practice at Union level to streamlining the effective implementation of the obligations related to the detection and labelling of artificially generated or manipulated content.

Is the AI Act future-proof?

The AI Act sets a legal framework that is responsive to new developments, easy and quick to adapt and allows for frequent evaluation.

The AI Act sets result-oriented requirements and obligations but leaves the concrete technical solutions and operationalisation to industry-driven standards and codes of practice that are flexible to be adapted to different use cases and to enable new technological solutions.

In addition, the legislation itself can be amended by delegated and implementing acts, for example to review the list of high-risk use cases in Annex III.

Finally, there will be frequent evaluations of certain parts of the AI Act and eventually of the entire regulation, making sure that any need for revision and amendments is identified.

How does the AI Act regulate biometric identification?

The use of **real-time remote biometric identification in publicly accessible spaces** (i.e. facial recognition using CCTV) for law enforcement purposes is prohibited. Member States can introduce exceptions by law that would allow the use of real-time remote biometric identification in the

following cases:

- Law enforcement activities related to 16 specified very serious crimes;
- Targeted search for specific victims, abduction, trafficking and sexual exploitation of human beings, and missing persons; or
- The prevention of threat to the life or physical safety of persons or response to the present or foreseeable threat of a terror attack.

Any exceptional use would be subject to **prior authorisation by a judicial or independent administrative authority** whose decision is binding. In case of urgency, approval can be granted within 24 hours; if the authorisation is rejected all data and output must be deleted.

It would need to be preceded by **prior fundamental rights impact assessment** and should be **notified to the relevant market surveillance authority and the data protection authority**. In case of urgency, the use of the system may be commenced without registration.

The use of AI systems for **post remote biometric identification** (identification of persons in previously collected material) of persons under investigation requires **prior authorisation** from a judicial authority or an independent administrative authority, as well as notification to the relevant data protection and market surveillance authority.

Why are particular rules needed for remote biometric identification?

Biometric identification can take different forms. Biometric authentication and verification i.e. to unlock a smartphone or for verification/authentication at border crossings to check a person's identity against his/her travel documents (one-to-one matching) remain unregulated, because they do not pose a significant risk to fundamental rights.

In contrast, biometric identification can also be used remotely for example to identify people in a crowd which can significantly impact privacy in the public space.

The accuracy of systems for facial recognition can be significantly influenced by a wide range of factors, such as camera quality, light, distance, database, algorithm, and the subject's ethnicity, age or gender. The same applies for gait and voice recognition and other biometric systems. Highly advanced systems are continuously reducing their false acceptance rates.

While a 99% accuracy rate may seem good in general, it is considerably risky when the result can lead to the suspicion of an innocent person. Even a 0.1% error rate can have a significant impact when applied to large populations, for example at train stations.

How do the rules protect fundamental rights?

There is already a strong protection for fundamental rights and for non-discrimination in place at EU and Member State level, but the complexity and opacity of certain AI applications ('black boxes') can pose a problem.

A human-centric approach to AI means to ensure AI applications comply with fundamental rights legislation. By integrating accountability and transparency requirements into the development of high-risk AI systems, and improving enforcement capabilities, we can ensure that these systems are designed with legal compliance in mind right from the start. Where breaches occur, such requirements will allow national authorities to have access to the information needed to investigate whether the use of AI complied with EU law.

Moreover, the AI Act requires that certain deployers of high-risk AI systems conduct a fundamental rights impact assessment.

What is a fundamental rights impact assessment? Who has to conduct such an assessment, and when?

Providers of high-risk AI systems need to carry out a risk assessment and design the system in a way that risks to health, safety and fundamental rights are minimised.

However, certain risks to fundamental rights can only be fully identified knowing the context of use of the high-risk AI system. When high-risk AI systems are used in particularly sensitive areas of possible power asymmetry, additional considerations of such risks are necessary.

Therefore, deployers that are bodies governed by public law or private operators providing public services, as well as operators providing high-risk AI systems that carry out credit worthiness assessments or price and risk assessments in life and health insurance, shall perform an assessment of the impact on fundamental rights and notify the national authority of the results.

In practice, many deployers will also have to carry out a data protection impact assessment. To avoid substantive overlaps in such cases, the fundamental rights impact assessment shall be conducted in conjunction with that data protection impact assessment.

How does this regulation address racial and gender bias in AI?

It is very important to underline that AI systems **do not create or reproduce bias**. Rather, when properly designed and used, **AI systems can contribute to reducing bias and existing structural discrimination**, and thus lead to more equitable and non-discriminatory decisions (e.g. in recruitment).

The **new mandatory requirements for all high-risk AI systems will serve this purpose**. AI systems must be **technically robust** to ensure they are fit for purpose and do not produce biased results, such as false positives or negatives, that disproportionately affect marginalised groups, including those based on racial or ethnic origin, sex, age, and other protected characteristics.

High-risk systems will also need to be **trained and tested with sufficiently representative datasets to minimise the risk of unfair biases** embedded in the model and ensure that these can be addressed through appropriate bias detection, correction and other mitigating measures.

They must also be **traceable and auditable**, ensuring that appropriate **documentation is kept**, including the data used to train the algorithm that would be key in ex-post investigations.

Compliance system before and after they are placed on the market will have to ensure these systems are **regularly monitored** and **potential risks are promptly addressed**.

When will the AI Act be fully applicable?

The AI Act will apply two years after entry into force on 2 August 2026, except for the following specific provisions:

- The prohibitions, definitions and provisions related to AI literacy will apply 6 months after entry into force on 2 February 2025;
- The rules on governance and the obligations for general purpose AI become applicable 12 months after entry into force on 2 August 2025;
- The obligations for high-risk AI systems that classify as high-risk because they are embedded in regulated products, listed in Annex II (list of Union harmonisation legislation), apply 36 months after entry into force on 2 August 2027.

How will the AI Act be enforced?

The AI Act establishes a two-tiered governance system, where **national authorities** are responsible for overseeing and enforcing rules for AI systems, while the EU level is responsible for governing general-purpose AI models.

To ensure EU-wide coherence and cooperation, the **European Artificial Intelligence Board** (AI Board) will be established, comprising representatives from Member States, with specialised subgroups for national regulators and other competent authorities.

The **AI Office**, the Commission's implementing body for the AI Act, will provide strategic guidance to the AI Board.

In addition, the AI Act establishes two advisory bodies to provide expert input: the **Scientific Panel** and the **Advisory Forum**. These bodies will offer valuable insights from stakeholders and interdisciplinary scientific communities, informing decision-making and ensuring a balanced approach to AI development.

Why is a European Artificial Intelligence Board needed and what will it do?

The European Artificial Intelligence Board comprises **high-level representatives of Member States** and the European Data Protection Supervisor. As a key advisor, the AI Board provides guidance on all matters related to AI policy, notably AI regulation, innovation and excellence policy and international cooperation on AI.

The AI Board plays a crucial role in ensuring the smooth, effective and harmonised implementation of the AI Act. The Board will serve as the forum where the AI regulators, namely the AI Office, national authorities and EPDS, can coordinate the consistent application of the AI Act.

What are the penalties for infringement?

Member States will have to lay down effective, proportionate and dissuasive penalties for

infringements of the rules for AI systems.

The Regulation sets out thresholds that need to be taken into account:

- **Up to €35m or 7%** of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements **on prohibited practices or non-compliance** related to requirements on data;
- **Up to €15m or 3%** of the total worldwide annual turnover of the preceding financial year for **non-compliance with any of the other requirements** or obligations of the Regulation;
- **Up to €7.5m or 1.5%** of the total worldwide annual turnover of the preceding financial year for the **supply of incorrect, incomplete or misleading information** to notified bodies and national competent authorities in reply to a request;
- For each category of infringement, the threshold would be the lower of the two amounts for SMEs and the higher for other companies.

The Commission can also enforce the rules on providers of general-purpose AI models by means of fines, taking into account the following threshold:

- **Up to €15m or 3%** of the total worldwide annual turnover of the preceding financial year for **non-compliance with any of the obligations** or measures requested by the Commission under the Regulation.

EU institutions, agencies or bodies are expected to lead by example, which is why they will also be subject to the rules and to possible penalties. The European Data Protection Supervisor will have the power to impose fines on them in case of non-compliance.

How will the General-Purpose AI Code of Practice be written?

The drawing-up of the first Code follows an inclusive and transparent process. A Code of Practice Plenary will be established to facilitate the iterative drafting process, consisting of all interested and eligible general-purpose AI model providers, downstream providers integrating a general-purpose AI model into their AI system, other industry organisations, other stakeholder organisations such as civil society or rightsholders organisations, as well as academia and other independent experts.

The AI Office has launched a call for expression of interest to participate in the drawing-up of the first Code of Practice. In parallel to this call for expression of interest a multi-stakeholder consultation to collect views and inputs from all interested stakeholders on the first Code of Practice is launched. Answers and submissions will form the basis of the first drafting iteration of the Code of Practice. From the start, the Code is therefore informed by a broad array of perspectives and expertise.

The Plenary will be structured in four Working Groups to allow for focused discussions on specific topics relevant to detail out obligations for providers of general-purpose AI models and general-purpose AI models with systemic risk. Plenary participants are free to choose one or more Working Groups they wish to engage in. Meetings are conducted exclusively online.

The AI Office will appoint Chairs and, as appropriate, Vice-Chairs for each of the four Working Groups of the Plenary, selected from interested independent experts. The Chairs will synthesise submissions and comments by Plenary participants to iteratively draft the first Code of Practice.

As the main addressees of the Code, providers of general-purpose AI models will be invited to dedicated workshops to contribute to informing each iterative drafting round, in addition to their Plenary participation.

After 9 months, the final version of the first Code of practice will be presented in a closing Plenary, expected to take place in April, and published. The closing Plenary gives general-purpose AI model providers the opportunity to express themselves whether they would envisage to use the Code.

If approved, how does the Code of Practice for general-purpose AI model providers serve as a central tool for compliance?

At the end of the Code of Practice drafting process, the AI Office and the AI Board will assess the adequacy of the Code and will publish their assessment. Following that assessment, the Commission may decide to approve a Code of Practice and give it general validity within the Union by means of implementing acts. If by the time the Regulation becomes applicable, the Code of Practice is not deemed adequate by the AI Office, the Commission may provide common rules for the implementation of the relevant obligations.

Providers of general-purpose AI models may therefore rely on the Code of Practice to demonstrate

compliance with the obligations set out in the AI Act.

As per the AI Act, the Code of Practice should include objectives, measures and as appropriate, key performance indicators (KPIs).

Providers adhering to the Code should regularly report to the AI Office on the implementation of measures taken and their outcomes, including as measured against key performance indicators as appropriate.

This facilitates enforcement by the AI Office, which is underpinned by the powers given to the Commission by the AI Act. This includes the ability to conduct evaluations of general-purpose AI models, request information and measures from model providers, and apply sanctions.

The AI Office will, as appropriate, encourage and facilitate the review and adaptation of the Code to reflect advancements in technology and state-of-the-art.

Once a harmonised standard is published and assessed as suitable to cover the relevant obligations by the AI Office, compliance with a European harmonised standard should grant providers the presumption of conformity.

Providers of general-purpose AI models should furthermore be able to demonstrate compliance using alternative adequate means, if Codes of Practice or harmonised standards are not available, or they choose not to rely on those.

Does the AI Act contain provisions regarding environmental protection and sustainability?

The objective of the AI proposal is to address risks to safety and fundamental rights, including the fundamental right to a high-level environmental protection. The environment is also one of the explicitly mentioned and protected legal interests.

The Commission is asked to request European standardisation organisations to produce a standardisation deliverable on reporting and documentation processes to improve AI systems' resource performance, such as reduction of energy and other resources consumption of the high-risk AI system during its lifecycle, and on energy efficient development of general-purpose AI models.

Furthermore, the Commission by two years after the date of application of the Regulation and every four years thereafter, is asked to submit a report on the review of the progress on the development of standardisation deliverables on energy efficient development of general-purpose models and assess the need for further measures or actions, including binding measures or actions.

In addition, providers of general-purpose AI models, which are trained on large data amounts and therefore prone to high energy consumption, are required to disclose energy consumption. In case of general-purpose AI models with systemic risks, energy efficiency furthermore needs to be assessed.

The Commission is empowered to develop appropriate and comparable measurement methodology for these disclosure obligations.

How can the new rules support innovation?

The regulatory framework can enhance the uptake of AI in two ways. On the one hand, increasing users' trust will increase the demand for AI used by companies and public authorities. On the other hand, by increasing legal certainty and harmonising rules, AI providers will access bigger markets, with products that users and consumers appreciate and purchase. Rules will apply only where strictly needed and in a way that minimises the burden for economic operators, with a light governance structure.

The AI Act further enables the creation of **regulatory sandboxes** and **real-world testing**, which provide a controlled environment to test innovative technologies for a limited time, thereby fostering innovation by companies, SMEs and start-ups in compliance with the AI Act. These, together with other measures such as the additional **Networks of AI Excellence Centres** and the **Public-Private Partnership on Artificial Intelligence, Data and Robotics**, and access to **Digital Innovation Hubs** and **Testing and Experimentation Facilities** will help build the right framework conditions for companies to develop and deploy AI.

Real world testing of High-Risk AI systems can be conducted for a maximum of 6 months (which can be prolonged by another 6 months). Prior to testing, a plan needs to be drawn up and submitted to the market surveillance authority, which has to approve the plan and specific testing conditions, with default tacit approval if no answer has been given within 30 days. Testing may be subject to unannounced inspections by the authority.

Real world testing can only be conducted given specific safeguards, e.g. users of the systems under real world testing have to provide informed consent, the testing must not have any negative effect on them, outcomes need to be reversible or disregarable, and their data needs to be deleted after conclusion of the testing. Special protection is to be granted to vulnerable groups, i.e. due to their age, physical or mental disability.

What role does the AI Pact play in the implementation of the AI Act?

Initiated by Commissioner Breton in May 2023, the AI Pact aims to enhance engagement between the AI Office and organisations (Pillar I) and to encourage the industry's voluntary commitment to start implementing the AI Act's requirements ahead of the legal deadline (Pillar II).

In particular, under Pillar I, participants will contribute to the creation of a collaborative community, sharing their experiences and knowledge. This includes workshops organised by the AI Office which provide participants with a better understanding of the AI Act, their responsibilities and how to prepare for its implementation. In turn, the AI Office can gather insights into best practices and challenges faced by the participants.

Under Pillar II, organisations are encouraged to proactively disclose the processes and practices they are implementing to anticipate compliance, through voluntary pledges. Pledges are intended as 'declarations of engagement' and will contain actions (planned or underway) to meet some of the AI Act's requirements.

The majority of rules of the AI Act (for example, some requirements on the high-risk AI systems) will apply at the end of a transitional period (i.e. the time between entry into force and date of applicability).

In this context and within the framework of the AI Pact, the AI Office calls on all organisations to proactively anticipate and implement some of the key provisions of the AI Act, with the aim of mitigating the risks to health, safety and fundamental rights as soon as possible.

More than 700 organisations have already expressed their interest in joining the AI Pact initiative, further to a call launched in November 2023. A first information session was held online on 6 May, with 300 participants. The official signing of the voluntary commitments is planned for autumn 2024. There will be a workshop on the AI Pact in the first week of September.

What is the international dimension of the EU's approach?

AI has consequences and challenges that transcend borders; therefore international cooperation is important. The AI Office is in charge of the European Union international engagement in the area of AI, on the basis of the AI Act and the Coordinated Plan on AI. The EU seeks to promote the responsible stewardship and good governance of AI in collaboration with international partners and in line with the rules-based multilateral system and the values it upholds.

The EU engages bilaterally and multilaterally to promote trustworthy, human-centric and ethical AI. Consequently, the EU is involved in multilateral forums where AI is discussed – notably G7, G20, the OECD, the Council of Europe, the Global Partnership on AI and the United Nations – and the EU has close bilateral ties with e.g. Canada, the US, India, Japan, South Korea, Singapore, and the Latin American and Caribbean region.

**Updated on 01/08/2024*

QANDA/21/1683

Press contacts:

[Thomas Regnier](#) (+32 2 29 9 1099)

[Patricia Poropat](#) (+32 2 298 04 85)

General public inquiries: [Europe Direct](#) by phone [00 800 67 89 10 11](#) or by [email](#)



The Colorado Artificial Intelligence Act

FPF U.S. Legislation Policy Brief

July 2024

Authored By: **Tatiana Rice**, Deputy Director, U.S. Legislation

Keir Lamont, Director, U.S. Legislation

Jordan Francis, Policy Counsel, U.S. Legislation

Executive Summary

This Policy Brief summarizes and analyzes key elements of the [Colorado AI Act](#) (CAIA), which was passed by the legislature on May 8, 2024 and signed by the Governor on May 17.¹ It further describes what the CAIA will do if enacted in its current form and identifies FPF’s most significant observations about the law.²

The CAIA is the first United States law to comprehensively regulate the development and use of high-risk artificial intelligence systems, and will come into effect on February 1, 2026—preceding even the European Union AI Act and therefore potentially becoming the first effective comprehensive AI law in the world. Highlights of the CAIA and our observations include:

- **Broader Potential Scope of Regulated Entities:** Unlike state data privacy laws, which typically apply to covered entities that meet certain thresholds, the CAIA applies to any person or entity that is a developer or deployer of a high-risk AI system. Additionally, one section of the law applies to any entity offering or deploying any consumer-facing AI system.
- **Role-Specific Obligations:** The CAIA apportions role-specific obligations for deployers and developers, akin to controllers and processors under data privacy regimes. Deployers, who directly interact with individuals and ultimately control how the system is used, are required to maintain risk management programs, conduct impact assessments, and provide relevant consumer rights. Developers, on the other hand, must provide the information and documentation needed for deployers to fulfill their responsibilities.
- **Duty of Care to Mitigate Algorithmic Discrimination:** Developers and deployers are subject to a duty of care to protect consumers from algorithmic discrimination, which in practice, likely means that enforcers of the CAIA will assess developer and deployer actions using a proportionality test. The definition of “algorithmic discrimination” appears to cover both intentional discrimination and disparate impact.
- **Novel Consumer Rights:** In addition to typical consumer rights seen in comparable legislation, such as the right to pre-use notice, the CAIA provides consumers with particular rights if an adverse decision is made by a high-risk AI system. In that event, the deployer must provide a consumer a statement of reasons, the right to correct, and appeal for human review, if feasible.
- **Attorney General Authority:** Though the CAIA does not create a private right of action, it grants the Colorado Attorney General significant authority to enforce the law and implement necessary regulations.

¹ The Colorado AI Act was introduced by Senate Majority Leader Robert Rodriguez and co-sponsored by Senators Cutter, Michaelson Jenet, Priola, Winter, Fenberg and House Representatives Titone, Rutinel, and Duran. The bill closely follows the framework established in Connecticut Senate Bill 2 by Connecticut Senator Maroney.

² The CAIA may undergo revisions pursuant to Attorney General rulemaking (detailed in Sec. 8) and the legislative task force established in companion bill [HB 1468](#).

This brief addresses the following elements of the CAIA:

1. **Scope & Regulated Entities**
2. **Algorithmic Discrimination**
3. **Developer Obligations**
4. **Deployer Obligations**
5. **Consumer Rights**
6. **Other Disclosures**
7. **Exemptions**
8. **Enforcement and Defenses**

1. Scope & Regulated Entities

Most of the CAIA regulates developers and deployers of “**high-risk artificial intelligence systems**” defined as “any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision.” (Sec. (Sec. 6-1-1701(9(a)). In turn, the two operative terms in that description are defined as follows:

1. A “**consequential decision**” is any decision that has a material, legal, or similarly significant effect on the provision of denial to, or the cost or terms of the following categories: education, employment, financial or lending services, essential government services, healthcare services, housing, insurance, or legal services. (Sec. 6-1-1701(3)).
2. A “**substantial factor**” is a factor generated by an AI system that is used to assist in making, and is capable of altering the outcome of, a consequential decision (Sec. 6-1-1701(11)).

“High-risk artificial intelligence system” excludes AI systems intended to perform a narrow procedural task or detect decision-making patterns or deviations from prior decision-making patterns. (Sec. 6-1-1701(9)(b)). The following technologies are also excluded, so far as they are not used to make or be a substantial factor in making a consequential decision:

- Anti-fraud (non-facial recognition);
- Anti-malware, anti-virus, and firewall;
- Video games;
- Calculators;
- Cybersecurity;
- Databases and data storage;
- Internet domain registration, website loading, and networking;
- Spam and robocall- filtering
- Spell-checking;
- Spreadsheets;
- Web caching or web hosting;
- Interactive technologies that provide users information (“chatbots”) **if such system is subject to an accepted use policy** that prohibits generating discriminatory or harmful content

Both developers and deployers of high-risk artificial intelligence systems (“high-risk AI systems”) must conduct business in Colorado for the law to apply. While a deployer is simply defined as anyone that deploys a high-risk AI system, a developer includes anyone who develops an AI system, as well as anyone who “**intentionally and substantially modifies**” an AI system in a manner that results in any new foreseeable risk of algorithmic discrimination. (Secs. 6-1-1701(6), 6-1-1701(10)).

Observations:

- **No Covered Entity Thresholds:** Unlike state data privacy laws, which typically apply to covered entities that collect or sell a certain amount of data or meet a revenue threshold, the CAIA applies to any person or entity that is a developer or deployer of a high-risk AI system. Though there are limited exemptions for small deployers, Governor Polis noted [particular concerns](#) with the law’s impact on the state’s innovation economy and competition.
- **Detailed List of Excluded Technologies:** Critics might find it redundant for the CAIA to list technologies excluded from the law’s scope since they ordinarily wouldn’t make or substantially influence consequential decisions. However, the bill sponsor likely included the list to maximize clarity and gain stakeholder support, avoiding arguments about overbreadth, as seen with the California Privacy Protection Agency’s [draft regulations](#) on “automated decisionmaking technology.” Consequently, the CAIA’s exclusions encompass all technologies excluded under the CPPA draft regulations, plus additional ones.
 - With the exclusion regarding chatbots, the basis for the exclusion itself—that there must be an accepted use policy—may be a way to incentivize ethical conduct without direct regulation.

2. Algorithmic Discrimination

A primary goal of the CAIA is to mitigate the risk of “**algorithmic discrimination**,” defined as any condition in which the use of an AI system results in an *unlawful* differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived protected class, including, e.g., age, color, disability, ethnicity, national origin, race, religion, reproductive health, sex, or veteran status. (Sec. 6-1-1701(1)). Self-testing for bias, activities that support increased diversification, and acts conducted by a private club that are currently exempted under civil rights law do not constitute “algorithmic discrimination.” (Sec. 6-1-1701(1)(b)).

Both developers and deployers are subject to a **duty of care**, meaning they must use “reasonable care” to protect consumers from “any **known or reasonably foreseeable risks of algorithmic discrimination** from the intended and contracted uses” of the high-risk AI system.

Developers and deployers maintain a rebuttable presumption of using reasonable care under this provision if they satisfy the obligations of the CAIA.

Observations:

- **Duty of Care Versus Prohibition:** Rather than include a prohibition against algorithmic discrimination, as seen in [California AB 2930](#) (2024) or the [District of Columbia's Stop Discrimination by Algorithm Act \(SDAA\)](#) (2021), the CAIA imposes a “duty of care” with a “reasonability” standard. In practice, this likely means the CAIA does not impose strict liability. Instead, developers and deployers may be assessed using a proportionality test, considering factors, circumstances, and industry standards, to determine whether they exercised reasonable care to prevent algorithmic discrimination.
- **Interaction with Existing Civil Rights Law:** Although most agree that civil rights laws already apply to AI systems in theory, civil rights experts [note](#) that the law is far behind the technology, making the CAIA a step in the right direction. Given the law’s intent, the CAIA will certainly interact with existing civil rights law, though it’s unclear precisely how. As a result, the CAIA has drawn criticism from industry for creating uncertainty, and civil society advocates for potentially weakening or conflicting with existing rights.

Some observations:

- **Clarifying the Status Quo:** The law’s definition of “algorithmic discrimination” as “unlawful differential treatment” may signal the bill sponsor’s intent not to expand existing civil rights law, but provide clarity that existing law applies to the AI context as well.
- **Disparate Impact:** The CAIA appears to cover both intentional discrimination and disparate impact, where seemingly neutral practices disproportionately affect one group of people with a protected characteristic more than another. In his [signing statement](#), Governor Polis urged the legislature to reexamine the law to focus primarily on intentional discrimination. However, [federal regulators](#), [data scientists](#), and [civil rights advocates](#) argue that disparate impact is a necessary component of ensuring AI non-discrimination.

3. Developer Obligations

Beyond the duty of care, developers must adhere to several transparency requirements outlined in Section 6-1-1702. Compliance with these requirements enables developers to maintain a rebuttable presumption that they exercised reasonable care to mitigate algorithmic discrimination. These obligations include:

Disclosures to Deployers: Developers must make available to deployers and other developers of the high-risk AI system a “**general statement**” describing the reasonably foreseeable uses and known harmful or inappropriate uses” of the system and the following forms of “**documentation**”:

1. **Information for Compliance:** Information necessary for the deployer to comply with their obligations under the law, including high-level summaries of the types of data used to train the system, known or reasonably foreseeable limitations of the system, the system purpose, and its intended benefits and uses (Sec. 6-1-1702 (2)(b));
2. **Evaluation & Mitigation:** Documentation describing how the system was evaluated for performance and mitigation of algorithmic discrimination, data governance measures concerning source and bias, intended outputs of the system, measures taken to mitigate known or reasonably foreseeable risks of algorithmic discrimination, and how the system should be used, not be used, and be monitored while in use (Sec. 6-1-1702 (2)(c));
3. **As Necessary:** Additional documentation reasonably necessary for a deployer to understand the systems' outputs and monitor its performance for risks of algorithmic discrimination (Sec. 6-1-1702 (2)(d));
4. **Facilitating Impact Assessments:** Information and documentation, "through artifacts such as model cards, dataset cards, or other impact assessments," necessary to complete an impact assessment, either by the deployer or a contracted third party (Sec. 6-1-1702 (3)).

Upon request by the Attorney General, a developer has ninety days to disclose the statement or documentation disclosed to deployers as described above (Sec. 6-1-1702 (7)).

Disclosures to the Public: Developers must make available on their website or in a public use case inventory—and update as necessary or within ninety days of an intentional and substantial modification—a statement summarizing (1) the types of high-risk AI systems it currently makes available to deployers or other developers; and (2) how the developer manages known or reasonably foreseeable risks of algorithmic discrimination (Sec. 6-1-1702 (4)).

Notification of Algorithmic Discrimination: Within ninety days of discovering, either through their own testing and analysis or via a credible report from a deployer, that their high-risk AI system has caused or is reasonably likely to have caused algorithmic discrimination, a developer must disclose those known or reasonably foreseeable risks to the attorney general and *all known deployers* (Sec. 6-1-1702 (5)).

Observations:

- **Comparison with Controller/Processor Distinction:** Similar to how "processors" are treated under many data privacy regimes, the CAIA places fewer affirmative obligations on the "developer" due to their lack of interaction directly with consumers or ability to ultimately control how the system is used. However, a deployer may also be subject to developer duties and liability if they significantly modify a system, creating a new or reasonably foreseeable risk of algorithmic discrimination.
- **Notifying Credible Reports of Discrimination:** The CAIA goes beyond what would have been required under Connecticut Senate Bill 2, on which this law was modeled, by requiring that developers alert the Attorney General if they identify or otherwise receive

from a deployer a **credible report** that a deployed high-risk AI system has caused algorithmic discrimination.

- This requirement has faced significant pushback from industry, who [argue](#) that developers are ill-equipped to discover algorithmic discrimination by their deployers. Similarly, it may be challenging to distinguish between a system exhibiting bias against a single individual and reporting each of those cases versus reporting an illegal pattern of disparate impact against a protected class.
- As detailed in the enforcement section, however, the developer maintains an affirmative defense against Attorney General enforcement arising from such discrimination if they cure any violation of the Act and are otherwise compliant with a recognized risk management framework.

4. Deployer Obligations

Deployers must comply with the requirements outlined in Section 6-1-1703, which mandate transparency, the establishment of internal AI governance practices and policies, and the provision and response to consumer rights. Like developers, deployers must adhere to a duty of care regarding algorithmic discrimination. They can benefit from a rebuttable presumption of having acted with care if they comply with the requirements of Section 6-1-1703 and any additional regulations issued by the Attorney General. These requirements include—

Risk Management Policy & Program: Deployers must implement a risk management policy and program to govern their deployment of a high-risk AI system (Sec. 6-1-1703 (2)). The risk management policy and program must (1) specify the principles, processes, and personnel used to identify and mitigate algorithmic discrimination; (2) be an iterative process that is reviewed and updated regularly; and (3) be reasonable, considering factors such as how the framework compares to the latest version of the “Artificial Intelligence Risk Management Framework” (AI RMF) published by the National Institute of Standards and Technology (NIST) and the size and complexity of the deployer (Sec. 6-1-1703 (2)(a)). One risk management policy and program can cover multiple high-risk AI systems deployed by the deployer (Sec. 6-1-1703 (2)(b)).

Impact Assessments: Annually, and within ninety days after a substantial and intentional modification to a high-risk AI system, a deployer, or a third party contracted to the deployer, must conduct an impact assessment (Sec. 6-1-1703 (3)(a)). As detailed in Sec. 6-1-1703 (3)(b), impact assessments must include, to “the extent reasonably known by or available to the deployer,”—

1. **Purpose:** A statement disclosing the system’s purpose, intended use cases, deployment context, and benefits (and, if after an intentional and substantial modification, a statement disclosing the extent to which the [AI system] was used in a manner that was consistent with, or varied from, the developer’s intended uses);
2. **Risk:** Analysis of whether there are known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of those risks and mitigation steps taken;

3. **Data:** A description of categories of data processed as inputs and outputs produced by the system; and an overview of categories of data used to customize the system, if applicable;
4. **Testing:** Metrics used to evaluate the system's performance and known limitations;
5. **Transparency:** A description of transparency measures taken including those to disclose to an individual that the system is in use when it is in use; and
6. **Monitoring:** Description of post-deployment monitoring and user safeguards, such as the deployer's "oversight, use, and learning process" to address issues arising from deployment

One impact assessment may cover "a comparable set" of deployed systems, and an assessment completed for complying with another law or regulation can satisfy the requirements of the CAIA if that other assessment "is reasonably similar in scope and effect" to the one required under the CAIA (Sec. 6-1-1703 (3)(d) & (e)). Impact assessments, and all records concerning each impact assessment, shall be retained for at least three years after the final deployment of the system (Sec. 6-1-1703 (3)(f)).

Disclosures to the Public: Deployers must make available on their websites, and periodically update, a statement summarizing the types of high-risk AI systems currently deployed, how known or reasonably foreseeable risks of algorithmic discrimination arising from deployment are being managed, and, "[i]n detail, the nature, source, and extent of the information collected and used by the deployer" (Sec. 6-1-1703(5)).

Review and Notification of Algorithmic Discrimination: Annually, deployers, or third parties contracted by deployers, must review the deployment of the system to ensure that it is not causing algorithmic discrimination (Sec. 6-1-1703 (3)(g)). If a deployer learns, post-deployment, that a system has caused algorithmic discrimination then the deployer must send to the attorney general, without unreasonable delay and within ninety days of the discovery, notice of the discovery (Sec. 6-1-1703 (7)).

Observations:

- **The Leading Role of the Colorado Attorney General in AI Governance:** One of the discretionary rulemaking powers of the Colorado Attorney General is the authority to determine which AI risk management frameworks are suitable for compliance under the CAIA. Consequently, the Colorado AG may be poised to play a leading national role in setting AI governance standards.
- **Flexible Metrics to Mitigate Discrimination:** The CAIA mandates that deployers mitigate algorithmic discrimination and annually assess their systems for such issues, but the law does not specify explicit testing or auditing requirements. In contrast, legislation like New York City Local Law 144, which mandates specific auditing practices, has faced criticism for imposing standards that are either undeveloped or use

inappropriate metrics. The CAIA avoids this by allowing deployers the flexibility to choose how to measure and test for bias, as long as these assessments are conducted and documented. However, civil society advocates argue that this flexibility may give entities too much leeway to declare their systems non-discriminatory.

5. Consumer Rights

Deployers owe certain obligations to individuals. No later than the time that a deployer uses a high-risk AI system to make a consequential decision, a deployer must **notify** individuals about the use of the system and provide a **statement** that discloses (1) the purpose of the system and nature of its consequential decision, (2) contact information for the deployer, (3) a plain language description of the system, (4) instructions for how to access the deployer’s website disclosure, and (5) where applicable, inform individuals of their Colorado Privacy Act right to opt-out of profiling in furtherance of decisions with legal or similar significant effects. (Sec. 6-1-1703(4)(a)).

Where a deployer has used a high-risk artificial intelligence system to reach a consequential decision that is **adverse** to a person, the deployer is required to provide that person with an additional statement disclosing the “principal reason or reasons” for the decision including: (1) the degree to which and manner in which the system contributed to the decision, (2) the type of data processed by the system, and (3) the source or sources of the data. (Sec. 6-1-1703(4)(b)). In these circumstances, a deployer must also offer the person with (1) an opportunity to **correct** any inaccurate personal data the system processed for the decision and (2) an opportunity to **appeal** the decision that, where technically feasible and in the best interest of the person, allow for human review of the decision. ((6-1-1703(4)(b)(I) & (II)).

Observations:

- **Building upon Existing Privacy Law:** Broad-based data privacy rules are commonly regarded as a necessary first step for tackling the risks posed by high-risk AI systems. The CAIA implicitly builds upon the [Colorado Privacy Act](#) of 2022 (“CPA”) which establishes rights and data controller obligations for the use of personal information. Notably, Senate Majority Leader [Rodriguez](#) was a primary sponsor of both laws. In this section, the CAIA directly points to the CPA’s existing right to opt-out of profiling which presently exists in approximately 15 state ‘comprehensive’ privacy laws.
- **Contemporaneous Notice:** The CAIA requirement to provide individuals with notice “no later than the time” that a high-risk AI system is deployed to make a consequential decision is comparable to California Privacy Protection Agency’s [draft ADMT regulations](#) which would require a “pre-use” notice to be provided to a consumer before processing the consumer’s personal information using automated decisionmaking technology. The requirements for notices under CPPA’s draft regulations are more prescriptive than the CAIA’s disclosure requirements.

- **Alignment with Minnesota?** Minnesota’s recently enacted [comprehensive privacy law](#) contains a unique right to contest the result of significant profiling decisions (not just opt-out of such decisions) that resembles the CAIA. This law grants individuals the right to be informed about actions they could take to secure a different decision, review the personal data used in profiling, correct inaccurate data, and have the profiling decision reevaluated. While Minnesota’s law does not explicitly provide a right to human review, similar consumer rights to appeal the outcomes of significant automated decisions could become a standard feature in both AI and privacy-focused legislation.
- **Technical Feasibility:** The CAIA provides two exceptions to the right to human review of a high-risk AI system’s adverse consequential decision. First, human review should be “technically feasible,” and second, such review should be “in the best interest of the consumer” (noting that in some cases delay might pose a risk to life or safety). Stakeholders may seek clarification of both terms through Attorney General rulemaking. The concept of “technical feasibility” was first included in the [CA AB 331](#) (2023), though was focused on requests to be subject to an alternative selection process.

6. Other Disclosures

Upon request by the Attorney General, a developer, deployer, or a third party contracted by the deployer has ninety days to provide the role-specific documentation required by the CAIA. The Attorney General may then evaluate these documents for compliance with the CAIA (Sec. 6-1-1702(7), 6-1-1703(9)). However, the Act’s reporting and transparency requirements will not require a developer or deployer to disclose a **trade secret** or information protected from disclosure by state or federal law. (Sec. 6-1-1702(6), 6-1-1703(8)). To the extent that a deployer withholds information under this (or another) exception, they must notify a consumer and provide a basis for the withholding. Developers have an additional exemption from disclosing information that would create a **security risk**. (Sec. 6-1-1702(6)). The CAIA also provides that both developer and deployer records disclosed to the Attorney General are exempt from disclosure under the Colorado Open Records Act and that such disclosures do not constitute a waiver of attorney-client privilege. (Sec. 6-1-1702(7) & 6-1-1703(9)).

Additionally, **any entity** that deploys, offers, or makes available **an artificial intelligence system** intended to interact with consumers must disclose this to the consumer, unless it would be “obvious to a reasonable person” that they are interacting with an AI system. (Sec. 6-1-704).

Observations:

- **Broader than Comparable Laws:** This provision applies not only to developers and deployers but to any entity using any type of consumer-facing AI system. The obligation to disclose to individuals that they are interacting with an AI system is broader than [Utah SB 149 \(2024\)](#), which requires such disclosure only for generative AI systems, and

a [2019 California law](#) that prohibits using bots to interact with people online with the intent to mislead them, unless the bot's nature is disclosed.

7. Exemptions

The CAIA includes a number of specific and general carve-outs from its provisions, some of which will be familiar to stakeholders with experience in state privacy law and some that are novel.

Small Business Exemption: The CAIA contains a limited **small business exception** available only to certain deployers. Deployers that use a high-risk artificial intelligence system that employ fewer than fifty full-time employees and do not train the system with their own data are exempted from risk management program, impact assessment, and public disclosure obligations. (Sec. 6-1-1703(6)).

Entity-Based Exemptions: The CAIA contains several entity-based exemptions, including for: (1) **HIPAA-regulated 'covered entities'** in providing health care recommendations that are not considered to be high risk; (2) **insurers** regulated by [existing Colorado law](#) on algorithms and predictive models; and (3) **financial institutions** subject to substantially equivalent or more stringent rules that apply to the use of high-risk artificial intelligence systems. (Sec. 6-1-1705(5), (7), (8)).

Approved Technology Exemptions: The CAIA also provides exemptions for developers or deployers of a high-risk AI system that have been otherwise approved, certified, or cleared by a federal agency, such as the Food and Drug Administration (FDA) or is otherwise in compliance with standards established by a federal agency so long as the standards are substantially equivalent or more stringent than those contained in the CAIA.

Purpose-Based Exceptions: Finally, the CAIA contains several purposes-based exceptions that largely correspond to exceptions to the Colorado Privacy Act. These exceptions provide that CAIA shall not restrict a the ability of a developer or deployer to comply with existing laws, legal investigations, or cooperate with law enforcement; take action concerning legal claims; take immediate steps to protect life or physical safety; protect against security incidents or other illegal activity (*except through facial recognition technology*); engage in public interest research; effectual product recalls; identify and repair technical errors. Unlike the Colorado Privacy Act, the CAIA contains an exception for pre-deployment research, and testing and development activities, echoing some exceptions found in the European Union AI Act. (Sec. 6-1-1705(1)-(4)).

Observations:

- **Trade Secrets Controversy:** While a “trade secret” exception is a common element across state privacy laws, including this provision in the CAIA generated significant substantial civil society [opposition](#) as a potential loophole.
- **Small Business Carveout:** Unlike privacy laws, which typically base small business exceptions on annual revenue or data processing thresholds, the CAIA's threshold is based on the number of employees. While business size may not directly reflect the complexity or risk profile of an AI system, Connecticut Senator Maroney noted during the Senate hearing on SB 2, which the CAIA was modeled after, that this limited exemption responds to concerns from small businesses with limited resources, often using “off-the-shelf” AI products like hiring tools.
 - The reasoning behind the CAIA small business exemption differs from the approach taken by the Federal Trade Commission (FTC). Last year, the FTC initiated an [enforcement action](#) against Rite-Aid for employing "off-the-shelf" AI systems without adequate testing or monitoring.
 - An alternative model is under consideration with California [AB 2930](#) which would exclude deployers with fewer than 25 employees that use automated decision tools that impact fewer than 1,000 people per year from the requirement to conduct impact assessments.
- **Application of HIPAA-Covered Entity Exception:** The CAIA provides a carveout for HIPAA-regulated entities using an AI system for healthcare decisions, provided the healthcare provider implements the recommendation and it's not deemed high risk. Similar to the exclusion for chatbots in the definition of "high-risk artificial intelligence system," this exception may encourage keeping a "doctor in the loop" without direct regulation. However, it's unclear if the term "high risk" in this exemption aligns with the CAIA's definition of a "high-risk artificial intelligence system," which involves systems substantially influencing consequential decisions in healthcare services or another category of high-risk healthcare recommendations.

8. Enforcement and Defenses

The Attorney General has sole authority to enforce the CAIA (Sec. 6-1-1706(1)). There is no basis for a private right of action (Sec. 6-1-1706(6)).

If an enforcement action is brought by the Attorney General, a developer, deployer, or other person may assert an **affirmative defense** if they (1) discover and cure the violation based on feedback, adversarial testing, or an internal review process; and (2) are compliant with the NIST AI RMF, another recognized national or international risk management framework, or any other risk management framework designated by the Attorney General (Sec. 6-1-1706(3)). The developer, deployer, or other person who is subject to the enforcement action bears the burden of demonstrating the necessary elements of the affirmative defense (Sec. 6-1-1706(4)).

In addition to enforcement authority, the Attorney General has permissive rulemaking authority, as necessary for implementing and enforcing the CAIA, including:

- Documentation and requirements for developers;
- The contents of and requirements for the notices and disclosures by developers, deployers, and other persons offering a consumer-facing AI system;
- The content and requirements of the deployer's risk management policy and program;
- The content and requirements of the deployer's impact assessments;
- The requirements of the rebuttable presumptions; and
- The requirements for the affirmative defense and the process by which the Attorney General will recognize other risk management frameworks.

Observations:

- **Interoperability:** To avoid duplicative AI governance efforts, the CAIA includes mechanisms to facilitate interoperability with other regimes. These include allowing the use of impact assessments conducted under other laws to meet the CAIA's requirements and fulfilling the NIST AI RMF to satisfy the CAIA's risk management requirements or as a defense against enforcement actions.
- **Questions Around Enforcing Against Algorithmic Discrimination:** In the event of demonstrable discrimination arising from the use of an AI system, many questions remain about how such claims would be enforced: *would the Colorado Attorney General be able to bring two separate discrimination claims, given that they would be identical claims for the same conduct, raising potential double jeopardy concerns? Though there is no private right of action, can an individual use information disclosed under this law as a basis to exercise their existing civil rights? Conversely, if an action is brought against an entity for algorithmic discrimination under existing civil rights law, could the defendant utilize information or standards compliance under the CAIA as a defense?*

Unless clarified through amendments by the task force next legislative session or Attorney General rulemaking, many of these questions might only be addressed through litigation.

Did we miss anything? Contact Tatiana Rice, Deputy Director for U.S. Legislation at trice@fpf.org, or email to inquire about joining the FPF U.S. Legislation Working Group.

Disclaimer: This policy brief is for informational purposes only and should not be used as legal advice.