GDPR – 90 Days Later

September 25, 2018

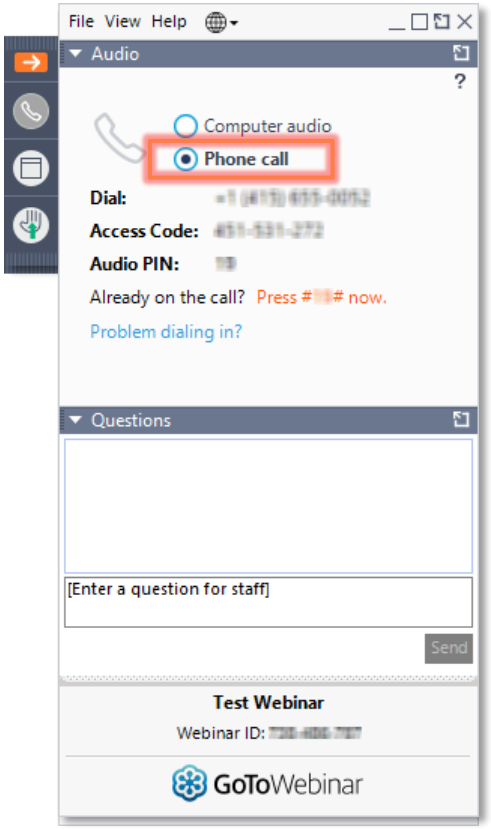
Gratia, Inc.

Audio Instructions

Select “Computer audio” to join via VOIP

OR

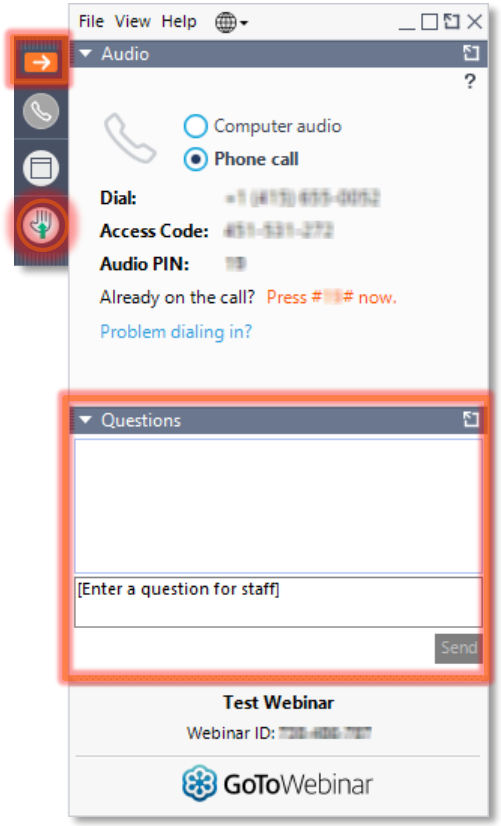
Select “Phone call” to dial in



Gratia, Inc.

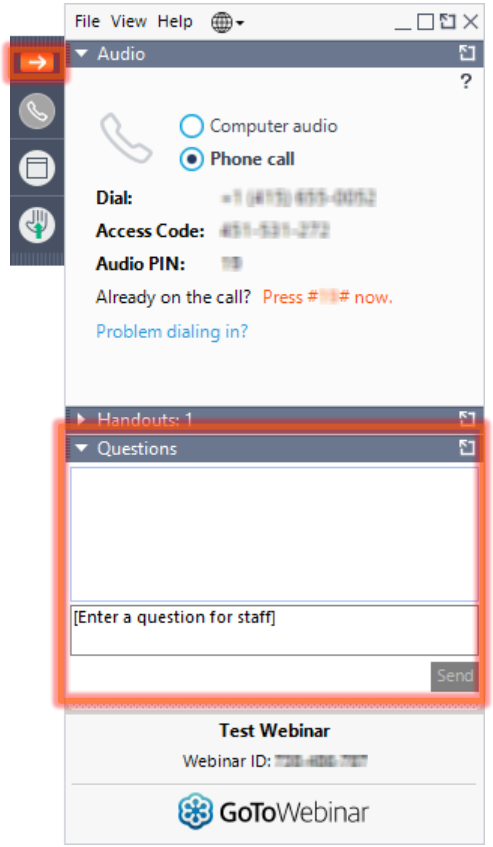
Today's Attendee Control Panel

- Grab Tab
- Handouts
- Questions



Gratia, Inc.

GoToWebinar Housekeeping: Attendee Participation



Your Participation

Join audio:
•Choose "Computer audio" to use VoIP
•Choose "Phone call" and dial using the information provided

Questions/Comments:
•Submit questions and comments via the Questions panel.
•Please continue to submit your text questions and comments using the Questions Pane

Handouts:
A copy of today's presentation will be made available at the conclusion of this call.

Note: Today's presentation is also being recorded and will be posted on the Company website.

Gratia, Inc.

Meet the Speakers

Joseph M. Callow, Jr.
Litigation Partner
KMK Law
513.579.6419
jcallow@kmklaw.com

Wayne Kiphart
Co-Founder & Managing Partner
Gratia, Inc.
513.800.0660
wayne.kiphart@gratia-inc.com

Thomas Runge
Co-Founder & Managing Partner
Gratia, Inc.
513.800.0660
Thomas.runge@gratia-inc.com

Gratia, Inc.

Opportunity to Learn More

KMK Law and Gratia, Inc. will be presenting on Friday, October 12th

For more information and to learn how to register visit:
https://nku.eventsair.com/QuickEventWebsitePortal/cybersecurity/symposium

Gratia, Inc.

Objectives

- Refresher on GDPR and the potential impact it can have on your business
- Share key learnings after 90 days
- Discuss what you should be doing to protect your business in the future

Gratia, Inc.

GDPR Refresher (G-Day: May 25, 2018)

- GDPR, General Data Protection Regulation, is the EU's attempt to create a more comprehensive and more uniform data privacy regime for EU citizens.

- "GDPR is the most important change in data privacy regulation in 20 years." www.eugdpr.org.

- GDPR replaces and significantly expands the scope of the current Data Protection Directive ("DPD") and mandates more security and transparency in the storage and processing of personal data.

- Controllers can only process permissible data for six permissible lawful bases listed in the Regulation and the Regulation places restrictions on how consent can be obtained. (Art. 6).

Gratia, Inc.

GDPR Refresher

- Personal data shall be:
  - Processed lawfully, fairly and in a transparent manner (lawfulness, fairness, and transparency).
  - Collected for specified, explicit and legitimate purposes ("purpose limitation").
  - Limited to what is necessary in relation for the purposes for which they are processed (data minimization").
  - Accurate and up to date ("accuracy").
  - Kept in a form which permits identification for no longer than needed ("storage limitation").
  - Processed in a manner which ensures security of personal data ("integrity and confidentiality") (Art. 5(1) (a-f)).

- GDPR rights:
  - The right to rectification (Art. 15).
  - The right to erasure (Art. 16).
  - The right of data portability (Art. 17).
  - The right to restriction of processing (Art. 18).
  - The right of access (Art. 20).
  - The right to object (Art. 21).

Gratia, Inc.

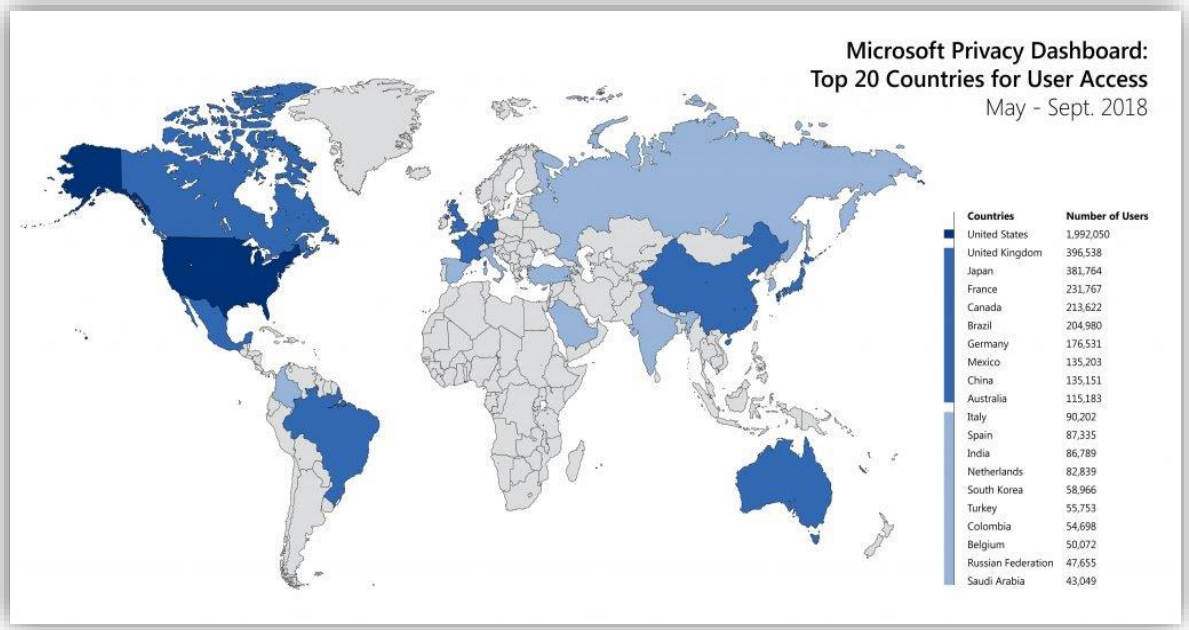
Safe Harbor and Privacy Shield

- July 4-5 - European Data Protection Board Meeting
- July 5 - European Parliament Resolution
- July 26 - EU Letter from the Commissioner for Justice to US Secretary of Commerce
- August 20 - US “Tech Letter” to US Secretary of State
- September 25-26 - EDPB Third Plenary Session, along with Privacy Shield’s annual review.
- US Cloud Act (March 2018)

Gratia, Inc.

Changes…for the better?

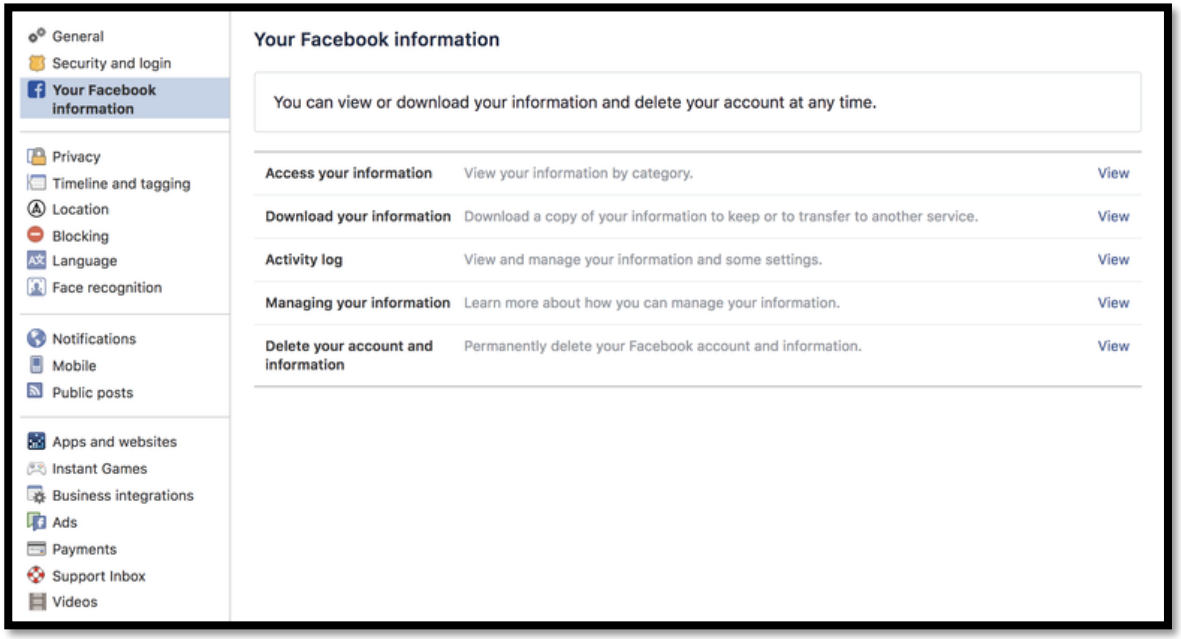
- People are becoming more aware of their privacy rights
  - In light of GDPR, Microsoft created a "privacy dashboard" where its customers can manage their privacy settings, see what data we have stored, and delete that data.
  - More than 5 million people have used Microsoft's privacy dashboard in the last 4 months to control their data – including 2 million Americans



Gratia, Inc.

Changes…for the better?

- People are becoming more aware of their privacy rights
  - Decline in Facebook users in America and Europe
  - “Those impacts [the decline of 3 million users in Europe] were purely due to the GDPR impact, not other engagement trends," said Facebook CFO David Wehner.



Gratia, Inc.

Changes…for the better?

- Existing companies are offering consumers more privacy settings and options
  - Google (who is still fighting "Right to be Forgotten" laws and is the subject of a number of GDPR complaints) has been significantly increasing privacy options for users
  - "Right to be Forgotten"
    - In 2014, a Luxembourg court ruled anyone with ties to the European Union could request that search engines such as Google remove links about them under certain circumstances.
    - In a hearing this month, Europe's highest court was charged with deciding if this rule should be limited to within the EU's borders or if search engines are required to remove information from anywhere in the world.
    - The final decision — expected sometime next year — will represent a landmark moment for the question of who has the right to police the global internet.

Changes…for the better?

- New companies are offering privacy monitoring, online account management, and personal data removal
  - DeleteMe, a paid subscription service which maintains tabs on data collection and release, as well as removes data including names, current and past addresses, dates of birth, and aliases on your behalf
  - unroll.me can list everything you are subscribed to, making the job of unsubscribing from newsletters, company updates, and more far easier
  - Deseat.me is an automated option for requesting account removal and subscription deletion from online services.

Gratia, Inc.

Changes…for the better?

- Websites becoming faster and more efficient by removing third party tags and unnecessary user-tracking
    - For example, right after GDPR went into effect, USA Today's US version delivered an average web page load time of 9.86 seconds, as opposed to the UK at .42 seconds; France at .75 seconds; and Germany at .51 seconds.

Gratia, Inc.

Penalties / Enforcements

- First day GDPR was in effect, complaints filed against Google, Facebook, Instagram and WhatsApp in multiple countries.
  - Alleging companies were “blackmailing” users by requiring “forced consent” to continue services – either accept the new terms or lose your account

- Subsequent complaints filed against Apple, Amazon, LinkedIn, Google and Facebook.
  - Similar allegations regarding “forced consent”

Gratia, Inc.

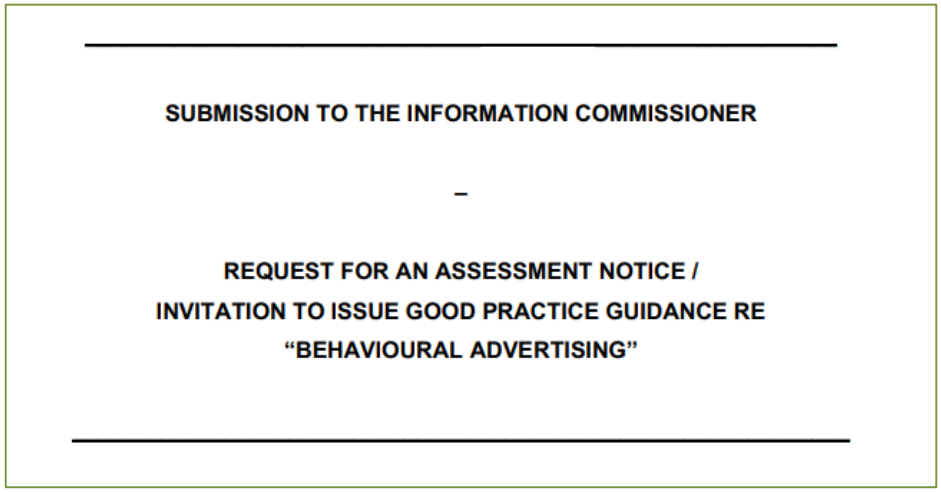
Penalties / Enforcements

- Complaints
  - Under GDPR, as with prior European privacy rules, anyone can file a complaint with the Information Commissioner's Office, or ICO, if they believe that their personal data has been misused.
  - In May, the ICO received 2,310 data protection complaints from individuals.
  - After GDPR enforcement began on May 25, complaints rose to 3,098 in June and reached 4,214 in July.
  - Multiple DPAs have seen an increase in data protection complaints over last 90 days.

Gratia, Inc.

Penalties / Enforcements

- Behavioral Advertising Complaint
  - In September, three parties filed a complaint asking the ICO to open an investigation "that will protect individuals from wide-scale and systemic breaches of the data protection regime by Google and others in the industry."
  - Complaint specifically raised concerns about the "behavioral advertising" industry



SUBMISSION TO THE INFORMATION COMMISSIONER

–

REQUEST FOR AN ASSESSMENT NOTICE /
INVITATION TO ISSUE GOOD PRACTICE GUIDANCE RE
"BEHAVIOURAL ADVERTISING"

Gratia, Inc.

Penalties / Enforcements

- Behavioral Advertising Complaint
  - Every time a person visits a website and is shown "behavioral advertising" on a website, intimate personal data is collected
  - Advertising companies broadcast this data to solicit potential advertisers' bids for the attention of the specific individual visiting the website.
  - A data breach occurs because this broadcast fails to protect these intimate data against unauthorized access. Under the GDPR this is unlawful.

"There is a massive and systematic data breach at the heart of the behavioral advertising industry. Despite the two year lead-in period before the GDPR, adtech companies have failed to comply. Our complaint should trigger a EU-wide investigation in to the ad tech industry's practices, using Article 62 of the GDPR. The industry can fix this. Ads can be useful and relevant without broadcasting intimate personal data."

Gratia, Inc.

Penalties / Enforcements

- Potential GDPR penalties
  - British Airways
    - Computer hack from August 21 – September 5 compromised credit card data from 380,000 consumers.
    - It only took British Airways ***one day*** to announce it had been hit by a data breach (September 6)
    - British Airways asked for people's personal data over social media to comply with GDPR…

Gratia, Inc.

Penalties / Enforcements

- Potential GDPR penalties
    - Facebook
        - In July, Facebook received a fine of £500,000 ($664,000) in the UK resulting from the Cambridge Analytica scandal
            - Facebook oversaw a "privacy" regime in which Cambridge Analytica was able to glean the personal information of millions of the social platform's users from their friends playing a psychoanalysis test.
            - Facebook also failed to ensure that after such a practice was deemed wrong, the associated data was deleted,
        - This penalty that would have been $1.9 billion if GDPR had been in effect when the scandal took place

Penalties / Enforcements

- Potential GDPR penalties
  - Warnings to companies not complying
    - In July, France's data protection authority, the Commission Nationale de L'informatique et des Libertés (CNIL), published a formal warning to two companies
    - Teemo, Inc. (Teemo) and Fidzup SAS (Fidzup) allegedly collected and retained geolocation data in violation of the GDPR
    - The CNIL did not impose any fines on the companies, but stated that Teemo and Fidzup may be subject to penalties if they fail to obtain valid consent from data subjects and set an appropriate retention period for geolocation data within three months.

Gratia, Inc.

New Laws

- Canada
  - The Personal Information Protection and Electronic Documents Act
- Belgium
  - Data Protection Authority
- Brazil
  - The Brazilian Data Protection Act (Lei Geral de Proteção de Dados, or LGPD)
- Italy
  - Legislative Decree setting forth national implementation for the GDPR
- Spain (expected to pass before the end of 2018)
  - Organic Law on the Protection of Personal Data
- Nepal
  - House of Representatives have endorsed the Protection of Individual's Right to Privacy
- Thailand
  - Cabinet approved the Digital Identification Bill

Gratia, Inc.

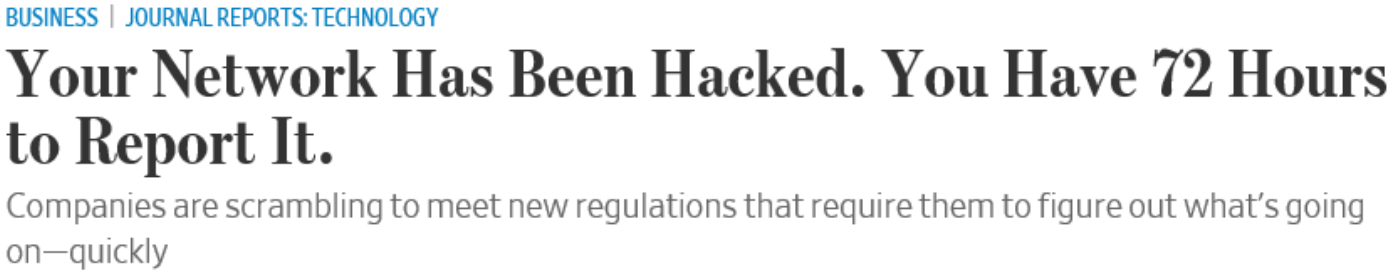
New Laws

- United States
  - California
    - The California Consumer Privacy Act of 2018
  - National standards?
    - The Trump Administration, on Sept. 4, 2018, formally announced its plans to establish U.S. consumer privacy standards.
    - The Internet Association (IA), a group of 40 major internet and technology firms, is strongly advocating for the establishment of a national privacy framework anchored by six privacy principles
      - Transparency, Controls, Access, Correction, Deletion, Portability

Gratia, Inc.

Challenges

- Practical business concerns
  - Complying with the GDPR often requires international collaboration, presenting cultural and linguistic challenges
  - Non-existent IT solutions have to be developed
  - Shortage of adequately trained staff
  - Difficulties complying with 72-hour data breach notification



BUSINESS | JOURNAL REPORTS: TECHNOLOGY

Your Network Has Been Hacked. You Have 72 Hours to Report It.

Companies are scrambling to meet new regulations that require them to figure out what's going on—quickly

Gratia, Inc.

Our Experiences in a GDPR World

- Understanding data collection, data flow and residency
- Communication
  - Explain internally what GDPR is, the impact it can have on the company and current processes
  - Involve all departments in data analysis
- Budget and plan for technical challenges
  - Cookie policy acceptance solution
  - General counsel involvement to review:
    - Processor
    - Sub-processor agreements
    - Policies
    - Information response templates

Gratia, Inc.

Technology

- Human Resources, Sales/Marketing, CRM/Support
- Phone systems (including recordings)
- Access control systems
- Technology
  - Website cookies
  - Google advertisement/analytics
  - Solutions specialized in tracking (hubspot, etc.)
- Data Removal/Anonymization/Information Request
  - Who owns the data management internally?
  - Which system included and what is their functionality?
  - What is communication process back to data subject?

Gratia, Inc.

Recommendations

- Understand how GDPR applies to your organization
- Utilize proven project plan to implement GDPR compliance
- Don’t look at this as a one time event
- Start analyzing website cookies
- Get some benadryl for the team
- Understand which data is needed for business purposes
- Assign a Data Processing Officer
- Start ASAP!

Gratia, Inc.

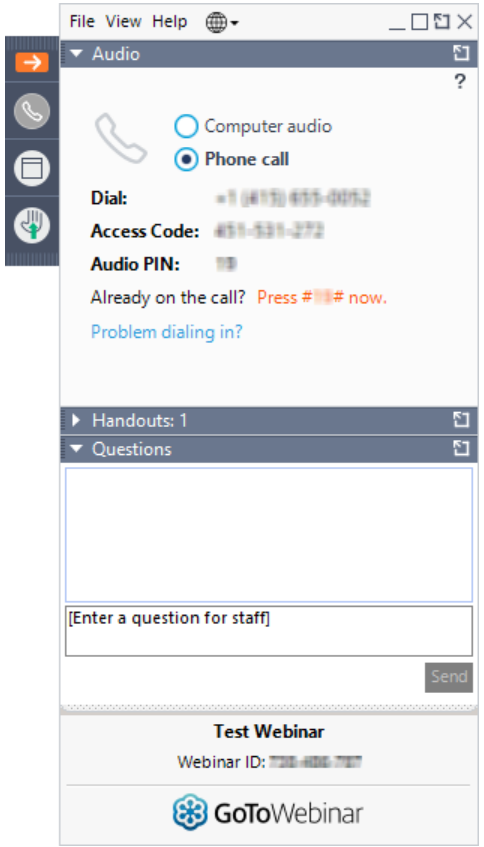
Moving Forward

- It is important for organizations to remain dedicated to GDPR compliance as the urgency of the initial compliance deadline fades into the past and new priorities emerge.
- Eyes on the changing legal landscape and whether a company needs to comply with additional privacy laws outside the GDPR
- Respond to consumer demand – as people become more aware of their privacy rights companies should continue to offer new ways for consumers to check and remove their personal information

Gratia, Inc.

Q&A from the Audience

Please type your message



Opportunity to Learn More

REGISTER TODAY

11th Annual Cybersecurity Symposium

October 11-12, 2018

Northern Kentucky University in the
James C. and Rachel M. Votruba Student Union

Contact Us

Joseph M. Callow, Jr.
Litigation Partner
KMK Law
513.579.6419
jcallow@kmklaw.com

Wayne Kiphart
Co-Founder & Managing Partner
Gratia, Inc.
513.800.0660
wayne.kiphart@gratia-inc.com

Thomas Runge
Co-Founder & Managing Partner
Gratia, Inc.
513.800.0660
Thomas.runge@gratia-inc.com

Gratia, Inc.