4th Annual
Cybersecurity Law Institute

May 25-26, 2016  •  Georgetown University Law Center, Washington, DC

Co-sponsored by the ABA Cybersecurity Task Force, the Center on Privacy & Technology and the U.S. Chamber of Commerce

CLE
Up to 12.5 CLE credit hours (based on a 60-minute credit hour), including up to 1.25 optional hours of ethics
Up to 15.0 CLE credit hours (based on a 50-minute credit hour), including up to 1.5 optional hours of ethics
Up to 12.0 Continuing Privacy Education credits
**Institute Summary**

At our 4th annual Institute, in the capital where cybersecurity regulations and enforcement decisions are made, you will be able to receive pragmatic advice from the most knowledgeable legal cybersecurity professionals in the country. These experts, from private practice, the government and corporate world, will share proven tips, valuable lessons learned and insightful prognostications about the year ahead. You owe it to your clients and yourself to attend the only law school-sponsored CLE program in the country that is devoted 100% to cybersecurity legal developments.

---

**Wednesday, May 25**

7:30-9:30 am  
**Registration and Continental Breakfast**  
Sponsored by WilmerHale

8:00-9:30 am  
.jsoupOptional Primer: Top 10 Things You Need to Know

PANELLISTS

- **Rena Mears**, BuckleySandler LLP  
- **Harriet Pearson**, Hogan Lovells  
- **Randy V. Sabett**, Cooley LLP

- Review the basics during this popular session reprise  
- Understand why cybersecurity is a “team sport” and where all the players and attorneys fit in  
- Explore governance and oversight, counseling, incidence preparedness and response

9:30-9:45 am  
**Networking Break**

9:45-10:00 am  
**Welcome and Overview**  
Alisha Avril, Program Attorney

10:00-11:30 am  
**Congratulations, You Are Responsible for Cybersecurity Legal Matters! What Must Corporate Counsel Learn?**

MODERATOR  
**Christina Ayiotis**, Cybersecurity Consultant, Program Co-Chair

PANELLISTS

- **Michelle Beistle**, Counsel & Chief Compliance Officer, Unisys  
- **Suzanne Rich Folsom**, General Counsel, Chief Compliance Officer & Senior Vice President, Government Affairs, United States Steel  
- **Cristin Flynn Goodwin**, Assistant General Counsel, Microsoft  
- **Karen I. Moreno**, Counsel, Information Technology Law, Exxon Mobil Corporation

- Prepare to be a leader in cyber matters at the Board level  
- Understand the role of in-house counsel in developing and enhancing cybersecurity programs  
- Grasp the role of the NIST framework: Is it the de facto standard of care?  
- Learn to be prepared with a cybersecurity program that complies with multiple overlapping frameworks, regulations, orders, and guidance

11:30 am-12:30 pm  
**Regulator Report: How Is Government Addressing Cybersecurity in Key Sectors?**

MODERATOR  
**Kim Peretti**, Alston & Bird LLP

PANELLISTS

- **Kathleen Benway**, Assistant Chief, Enforcement Bureau, Federal Communications Commission  
- **Maria Filipakis**, Executive Deputy Superintendent for Capital Markets, New York State Department of Financial Services (Invited)  
- **David Shonka**, Deputy General Counsel, Federal Trade Commission

- Examine regulatory priorities  
- Review enforcement developments  
- Obtain answers from federal and state officials

12:30-12:45 pm  
**Boxed Lunch Distribution**

12:45-2:15 pm  
**CONCURRENT SESSIONS:**

- **Session A: The Technical Basics of Cybersecurity and Forensics**

  **SPEAKERS**

  - **Jim Butler**, Senior Director, Global Security & Compliance, CareerBuilder.com  
  - **Thomas J. Hibarger**, Managing Director, Stroz Friedberg

  - Examine basic technical tools and their use in the law field  
  - Review key principles in information security and forensics  
  - Receive a tutorial on technical basics on cyber and forensics  
  - Ask your toughest questions about technical concepts

- **Session B: International Cyber Law Issues: Reviewing Other Countries’ Approaches**

  **MODERATOR**  
  **Emma J. Lovett**, Squadron Leader, Legal Officer, Royal Australian Air Force

  **PANELLISTS**

  - **Demetrios A. Eleftheriou**, Director of Global Privacy, Symantec Corporation  
  - **Jan Ellermann**, Senior Specialist, Data Protection Office, Europol  
  - **Christopher Painter**, Coordinator, Cyber Issues, U.S. Department of State

  Thanks to our Institute Sponsors

  - Cooley LLP  
  - The Cybersecurity Law Report  
  - Darktrace  
  - Hogan Lovells  
  - WilmerHale

  Thanks to our Co-Sponsors

  - ABA Cybersecurity Legal Task Force  
  - Center for Privacy and Technology  
  - U.S. Chamber of Commerce

This program will be available via live webcast (subject to change).

For more information, visit:  
[https://georgetown.inreachce.com/](https://georgetown.inreachce.com/)

@GeorgetownCLE  
#CSLI16
• Examine the French surveillance law and German data retention law
• Analyze UK mass surveillance and bulk collection
• Survey new laws on cybersecurity throughout the world
• Assess the breach notification landscape outside the U.S.

Session C Litigation Trends in Data Breaches

MODERATOR
Michelle Cohen, Patterson Belknap Webb & Tyler LLP

PANELISTS
Allison Brecher, Senior Litigation Counsel & Director of Information Management and Strategy, Marsh & McLennan Companies
Jay Edelson, Edelson PC
Douglas Meal, Ropes & Gray LLP
• Review post-breach trends after Wyndham, Neiman Marcus, and Target
• Learn practical steps to pursue when investigating a potential security incident.

2:15-2:45 pm
Networking Break

2:45-3:45 pm
CONCURRENT SESSIONS

Session A Privacy and Civil Liberties: Implications of Securing Cyber Environments

MODERATOR
Alan Raul, Sidley Austin LLP

PANELISTS
Joseph Alhadeff, Vice President, Global Public Policy, Oracle Corporation
Prof. Alvaro Bedoya, Executive Director, Center on Privacy & Technology, Georgetown University Law Center
Andrea Glorioso, Counselor, Digital Economy & Cyber Security, Delegation of the European Union to the U.S.
• Discuss the privacy and civil liberties concerns in sharing cyber threat information
• Review the issues in monitoring employee and other individuals’ use of information systems
• Explore how privacy concerns can be mitigated when data is shared with third parties
• Examine how global laws and proposed legislation define the boundaries of appropriate actions
• Study emerging cybersecurity organizational best practices to address privacy and civil liberties

Session B What Do You Need to Know About Protecting Controlled Unclassified Information?

MODERATOR
M. Peter Adler, Former Deputy General Counsel, SRA International, Inc.

PANELISTS
Mary Beth Bosco, Holland & Knight LLP
Annejanette Pickens, Associate General Counsel, General Dynamics Mission Systems, Inc.
Patrick Viscuso, Associate Director, CUI Security Oversight Office, U.S. National Archives and Records Administration
• Consider the emerging requirements under EO 13556, Safeguarding CUI
• Understand what CUI is and how it must be protected by federal contractors and subcontractors
• Assess the state of the final NARA rule, the FAR clause, and how to implement SP 800-171
• Analyze implementation issues faced by the defense community

Session C Always Connected, Always Vulnerable: The Internet of Things and Hacking Liability

MODERATOR
Daniel Mee, Goldberg Segalla

PANELISTS
Dan Caprio, Co-Founder & Chairman, The Providence Group
Steve Hoge, Principal Legal Counsel, Medtronic
Michael Woods, Associate General Counsel & Vice President, Verizon
• Identify and define the evolving issues, problems, and threats
• Review policies on wearables and implantables (SCIFs)
• Grasp the EOT/EPS standards
• Understand security by design and software assurance
• Explore the proliferation of IOT/CPS standards

3:55-4:55 pm
CONCURRENT SESSIONS:

Session A Tackling Vendor Risk

MODERATOR
Dori Anne Kuchinsky, Assistant General Counsel, Privacy, AOL Inc.

PANELISTS
David C. Gryce, Arent Fox LLP
Anthony Johnson, Vice President & CISO, Fannie Mae
Carmen B. Krueger, Senior Vice President & General Manager, Cloud Operations, SAP National Security Services
• Explore the place of law firms as vendors of legal services
• Compare and contrast vendor and supply chain risk
• Review vendor contracting strategies to mitigate risk and avoid pitfalls
• Assess the value of ongoing auditing and testing of vendor security
• Learn to engage proactively and cooperatively with vendors to stay abreast of evolving security threats

Session B What Do CISOs Want Lawyers to Understand About Cybersecurity?

MODERATOR
Hillary L. Hageman, Vice President & Deputy General Counsel, CACI International Inc.

PANELISTS
Michael Papay, Vice President & CISO, Northrop Grumman Corporation
Dr. J.R. Reagan, Global Chief Information Security Officer, Deloitte Touche Tohmatsu Limited
• Assess what fosters effective collaboration between information security and legal
• Review the key elements of a successful relationship between CISOs and lawyers
• Examine how frequently CISOs and lawyers should engage
• Learn what lawyers need to know from the CISO’s perspective

Session C Information Sharing: You Want To Share What With Whom?

MODERATOR
Justin Castillo, Head of Legal, BT Americas

PANELISTS
Susan B. Cassidy, Goldberg Segalla
John Martinez, Vice President & General Counsel, Raytheon Intelligence, Information and Services, Raytheon Company
Gregory T. Nojeim, Senior Counsel & Director, Freedom, Security & Technology Project, Center for Democracy & Technology
• Learn what questions should be asked before providing legal guidance for a new potential threat
• Assess the role of the ABA and other professional organizations
• Analyze potential liability protections
• Discuss the importance of timely decision-making and efficiency through documented processes
Thursday, May 26

8:00-8:30 am
Continental Breakfast

8:30-9:30 am
Keynote Address
Hon. Julie Brill, Commissioner, Federal Trade Commission

9:30-9:40 am
Networking Break

9:40-10:40 am
The National Security Side of Cyber Intrusions
MODERATOR
Andrew H. Tannenbaum, Cybersecurity Counsel, IBM
PANELISTS
Rajesh De, Mayer Brown LLP
Shawn Henry, President, CrowdStrike
• Understand the evolving threat landscape around state-sponsored attacks and the government’s role assisting companies with prevention, detection, and response
• Learn how to best work with the government in the aftermath of state-sponsored attacks
• Examine the shifting motives of adversaries, such as espionage and counter intel and the series of intrusions targeting “bulk pil”.
• Grasp the importance of needing to have alternative communication infrastructures as part of incident response
• Understand the impact of “Going Dark,” especially after the Paris attacks

4:55-6:00 pm
Networking Cocktail Reception
Sponsored by Darktrace

4:55-6:00 pm
Concurrent Sessions
10:50 am-12:05 pm
• Understand the impact of “Going Dark,” especially after the Paris attacks
• Grasp the importance of needing to have alternative communication infrastructures as part of incident response
• Learn how to best work with the government in the aftermath of state-sponsored attacks
• Examine the shifting motives of adversaries, such as espionage and counter intel and the series of intrusions targeting “bulk pil”.
• Grasp the importance of needing to have alternative communication infrastructures as part of incident response
• Understand the impact of “Going Dark,” especially after the Paris attacks

12:05-12:25pm
Boxed Lunch Distribution

12:25-1:40 pm
Concurrent Sessions
Session A De-Mystifying the “Dark Web”
MODERATOR
Etay Maor, Executive Security Advisor, IBM
PANELISTS
Matthew Devost, Managing Director, Accenture
Ralph Echemendia, “The Ethical Hacker”
Keith Mularski, Supervisory Special Agent, Federal Bureau of Investigation
• Learn what the “hidden internet” is and how to determine whether employees are accessing it
• Analyze the critical privacy, security, and anonymity concerns
• Explore the legal avenues to pursue if you are victimized by ransomware or cyber extortion
• Examine the ethics issues in gathering and using information available on the dark web

1:40-2:40 pm
Concurrent Sessions
Session B Developments in Payment Cards and Responses to Breaches
MODERATOR
Russell Schrader, General Counsel & Chief Privacy Officer, Commerce Signals Inc.
PANELISTS
Christopher Novak, Director, Verizon
Ronald Smalley, Vice President, Cyber Incident & Fraud Investigations, First Data
• Review the roles of the franchisor and the franchisee
• Examine the impact of CHIP/EMV rollout in the U.S. and internationally
• Grasp the impact of the burgeoning increase in e-commerce and of card not present breaches.

2:40-3:40 pm
Concurrent Sessions
Session C What Every Attorney Needs to Know About Dealing with Law Enforcement
MODERATOR
Korin A. Neff, Senior Vice President & Corporate Compliance Officer, Wyndham Worldwide Corporation
PANELISTS
Shane McGee, Chief Privacy Officer, FireEye, Inc.
Andrew S. Pack, Assistant U.S. Attorney, U.S. Attorney’s Office, New Jersey
• Review strategies to make working with law enforcement successful for you
• Receive an in-house lawyer’s guide to working with law enforcement
• Assess what to share and what not to share and how to protect proprietary information
• Assess the advantages and disadvantages of working with subpoenas and search warrants
Session C The Role of Insurance in Reducing Cybersecurity Risk

MODERATOR
Scott Godes, Barnes & Thornburg LLP

PANELISTS
Tom Finan, Chief Strategy Officer, Ark Network Security Solutions
Catherine A. Mulligan, Senior Vice President, Zurich North America
Greg Vernaci, Senior Vice President, American International Group, Inc.

• Explore the role of insurance in sound cybersecurity risk management and what risk managers and attorneys need to know
• Examine the evolution of cyber insurance and the types of coverage available
• Understand the key terms in policies and how they function in practice
• Grasp the importance of insurance review in vendor and business partner risk management
• Pinpoint how to answer security questions as part of the underwriting process
• Review the most recent case law

1:40-2:00 pm
Networking Break

2:00-3:30 pm
Responding to a Data Breach: How to Run a Cyber Investigation and Learn from the Breach

MODERATOR
Erez Liebermann, Chief Counsel, Cybersecurity & Privacy, Prudential Financial, Inc.

PANELISTS
Marshall Heilman, Vice President & Executive Director, IR and Red Team, Mandiant
W. Scott Nehs, Senior Vice President & General Counsel, Blue Cross Blue Shield Association
Tara M. Swaminatha, DLA Piper

• Learn how to best assist clients to evaluate a suspected breach or other unusual activity.
• Share best practices for organizing and overseeing a cyber investigation
• Understand when and how to assert the attorney-client privilege
• Receive tips on documenting the investigation and its findings
• Assess who should be involved in all phases of the investigation

3:30 pm
Adjournment
Institute conveniently from your office.

all that the Cybersecurity Law Institute breakout sessions to choose from, this is ed sessions post-program. With several This add-on includes access to all record-

Bonus-On Demand
as well as relevant sponsored webinars mid-year webinar to take place in 2016 Your registration for the Cybersecu-

Online Features
Post-Conference Webinar
Your registration for the Cybersecu-

Group Discounts
Group discounts are available for agencies, firms or companies registering three or more attendees at one time. If you would like to take advantage of the discounts listed below, please contact cle@law.georgetown.edu to receive the discount code.

3-5 registrants: $100 discount off each registration
6-9 registrants: $200 discount off each registration
10+ registrants: $300 discount off each registration

Disclaimer
Speakers are subject to change.

Special Needs or Dietary Restrictions
Email cle@law.georgetown.edu or call 202-662-9890.

Scholarships
Georgetown Law CLE endeavors to provide equal educational opportunities to all. We provide a limited number of scholarships on a case-by-case basis for both live programs and webcasts. Apply online at www.law.georgetown.edu/cle or submit your written request no later than 5:00 pm ET on May 5, 2016.

Cancellations/Rain-Checks/Substitutions
Cancellation and rain-check notices must be received by 5:00 pm ET on Thursday, May 19, 2016 for a refund (less $100 administrative fee). Rain checks for a future program will be granted for cancellations received after May 19th and prior to the start of the program. Substitutions are accepted at any time prior to the program. Registration for the live program is not transferable to the webcast or bonus on-demand access.

Substitutions
Registration for the live program is not transferable to the webcast or bonus on-demand access.

Course Materials
Course materials will be distributed prior to the program. Registrants will receive an email from the Georgetown Law CLE office at least one week before the program.

Satisfaction Guaranteed
We are confident you will value the information-sharing and networking at this conference. However, if you feel you have not received your money's worth by the end of the program, please contact a member of our registration team before leaving the conference. All refund requests will be reviewed carefully and are subject to approval by the Assistant Dean for Academic Conferences and Continuing Legal Education.

Questions? Contact Us
Georgetown Law CLE
600 New Jersey Avenue, NW
Washington, DC 20001
cle@law.georgetown.edu
202-662-9890

MCLE state credit rules vary for online CLE. Please check online at https://georgetown.inreachce.com/ to see if the program has been approved in your state. We will apply upon request in some states; alternatively, many states allow attorneys to apply on their own.

Continuing Privacy Education Credits
The International Association of Privacy Professionals (IAPP) will recognize up to 12.0 Continuing Privacy Education credit hours for attendance at the conference. After the event, attendees will submit each session for credit using the CPE submission form available at the Institute. If you have questions about the group designations of specific sessions, please email cle@law.georgetown.edu.

Bonus On-Demand Access
This add-on includes access to all recorded sessions post-program. You may receive CLE credit for some new sessions online. You cannot claim credit for taking the same sessions in person and online. If you register for this option, you will receive a separate email providing you with additional information on how to access the content online.

Cannot Attend in Person?
This program will be available via webcast and on-demand.
Registration Form

PLEASE PRINT OR TYPE. Payment must accompany registration.

Cybersecurity Law Institute (May 25-26, 2016)

- $1,195 Early-Bird Registration (due April 25 by 5:00PM ET)  
  - Bonus On-Demand Access $299
- $1,295 Regular Registration  
  - Bonus On-Demand Access $299
- $1,095 Georgetown Law Alumni Registration, Class of _________  
  - Bonus On-Demand Access $299
- $895 Government Registration  
  - Bonus On-Demand Access $299

Bonus On-Demand Access includes access to all recorded sessions post-program.

Please print clearly and list name exactly as you would like it to appear on your program name badge.

Name   Mr.   Ms.

Email address (please print clearly)

Firm/Organization

Job Title

Address

City  State  Zip

Phone

CLE credit?  ❑ Yes  ❑ No  What state(s)? __________________________  Bar number(s)? __________________________

Feel free to copy this form and pass it along to your associates.

❑ Please select this box if you prefer not to share mailing address information with our sponsors.

Your customer ID is: __________________ Enter the characters appearing on the top of the mailing label. Please enter this ID even if the label is addressed to someone else. Thank you!

To register for the live webcast, please visit our website: https://georgetown.inreachce.com/

THREE WAYS TO REGISTER:

1. ONLINE www.law.georgetown.edu/cle

2. MAIL with check payable to “Georgetown Law CLE” to address below

   Check enclosed #___________ $___________  Purchase Order attached to this form #___________

3. CALL us at 202-662-9890

Georgetown University Law Center  cle@law.georgetown.edu
Continuing Legal Education  202-662-9890
600 New Jersey Avenue, NW
Washington, DC 20001-2075
1. **Learn** how to take charge when cybersecurity is added to your corporate responsibilities

2. **Grasp** the nuts and bolts of cybersecurity and forensics i.e. what lawyers don’t know they don’t know

3. **Receive** an up-to-the-minute review of federal regulatory priorities from the regulators themselves

4. **Examine** the need-to-know cyber developments transpiring internationally

5. **Analyze** CUI and how to safeguard it

6. **Obtain** proven techniques for optimally addressing vendor risk

7. **Assess** the privacy and legal concerns of information sharing

8. **Identify** the most pressing law firm ethics issues surrounding cybersecurity

9. **Participate** in a debate on the use of active defense, including technical and legal issues

10. **Understand** how to best respond to a breach based on others’ past experiences