Privacy+ Security Forum

October 21-23, 2015
Washington, DC
Pre-conference workshops Oct 21
Main Event Oct 22-23

A High-Caliber Event Uniting Privacy and Security

Our Mission
Hold a Truly Informative Event

Privacy and security professionals, lawyers, technologists, policymakers, and academics will connect and collaborate in a rigorous learning environment. Sessions will have valuable practical takeaways.

Our Focus
Unite Privacy and Data Security

We will be breaking down the separate silos of privacy and security.

Our Participants
An Event for Seasoned Professionals

- Privacy Professionals
- Security Professionals
- Chief Information Officers
- Law Firm Attorneys
- Academics
- Policymakers
- NGO / Think Tank
- Technologists

Although this event is designed for seasoned professionals, there will also be sessions that beginners can understand.

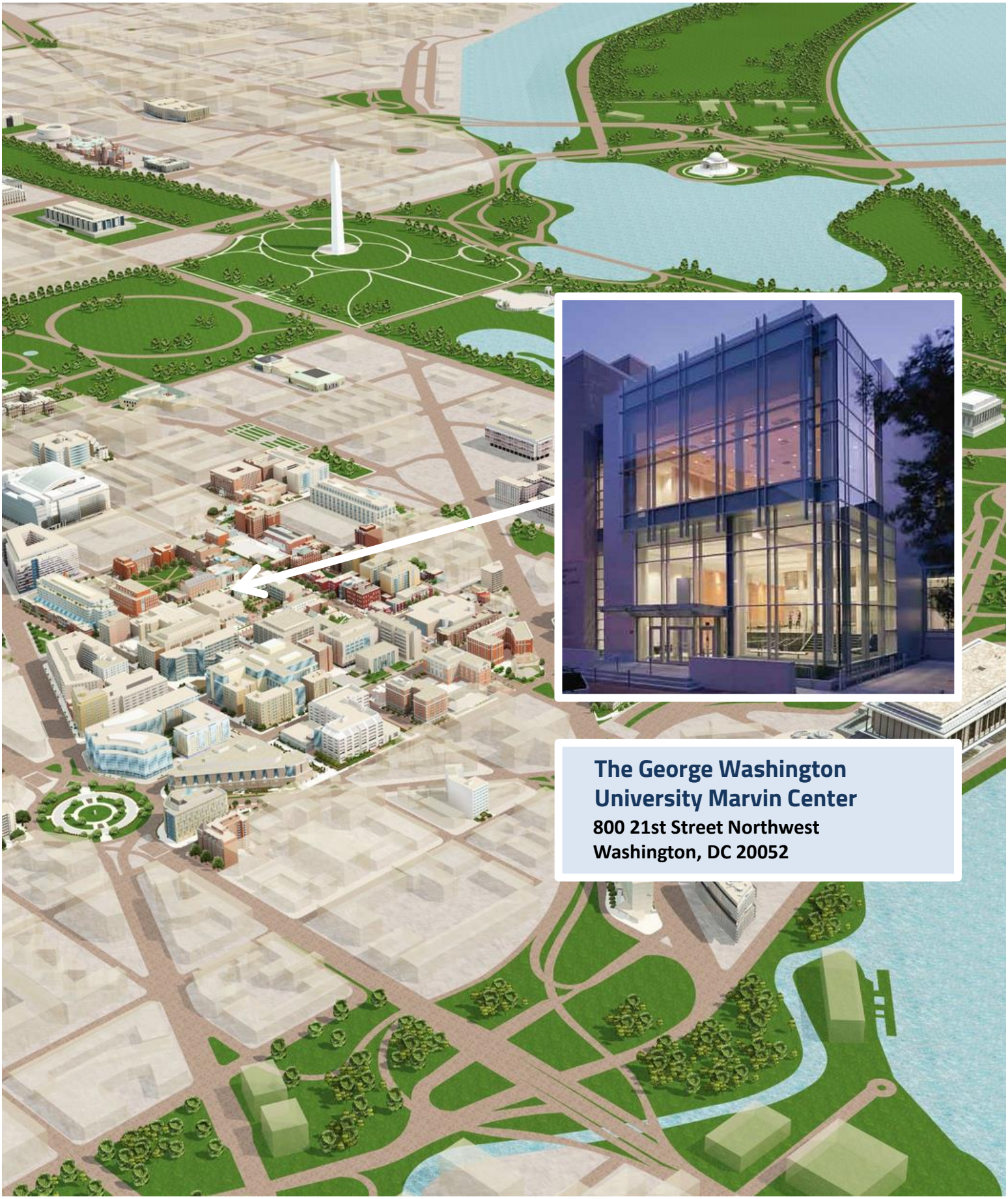
The Organizers

Professor Daniel Solove
John Marshall Harlan Research Professor
George Washington University Law School
President & CEO, TeachPrivacy

Professor Paul Schwartz
Jefferson E. Peyser Professor
U.C. Berkeley School of Law
Director, Berkeley Center for Law & Technology

www.privacyandsecurityforum.com

Venue



The George Washington University Marvin Center
800 21st Street Northwest
Washington, DC 20052

Rooms are available at special rates for attendees at the following hotels:

RENAISSANCE®
WASHINGTON DC
DUPONT CIRCLE HOTEL

Renaissance Washington DC

1143 New Hampshire Avenue NW
Washington, District Of Columbia 20037

Online Reservation: Go to the dedicated event link of the **Renaissance Hotel**.

Reservations Toll Free: 1-877-212-5752
Other hotel phone numbers may not accept reservation inquiries at the discounted rate.

THE Fairmont
WASHINGTON, D.C.

Fairmont Washington, DC

2401 M Street, NW
Washington, District of Columbia, 20037

Online Reservation: Go to the dedicated event link of the **Fairmont Hotel**.

Reservations Toll Free: 1-800-441-1414
Other hotel phone numbers may not accept reservation inquiries at the discounted rate.

Speakers + Expert Commentators

Alessandro Acquisti
Carnegyie Mellon University

Jim Adler
Metanautix

Sharon Anolik
Privacy Panacea

James Aquilina
Stroz Friedberg

Jennifer Archie
Latham & Walkins

Mohamed Ayad
Microsoft

Chris Babel
TRUSTe

Cliff Baker
Meditology

Ian Ballon
Greenbert Traurig

Elizabeth Banker
Twitter

Kevin Bankston
Cybersecurity Initiative New America

Devlin Barrett
Wall Street Journal

Daniel Barth-Jones
Columbia University

Kate Black
23andMe

Slade Bond
House Judiciary Committee

John Bowman
Promontory

Debbie Bromson
Jazz Pharmaceuticals

Geff Brown
Microsoft

Erika Brown Lee
U.S. Department of Justice

Jeff Brueggeman
AT&T

Devon Bryan
ADP

Aaron Burstein
FTC

Chris Calabrese
Center for Democracy& Technolgogy

Joseph Calandrino
Elysium Digital

David Cass
IBM

Bob Chaput
Clearwater Compliance

Danielle Citron
Maryland Law School

Ivelisse Clausell
Otsuka Pharmaceutical

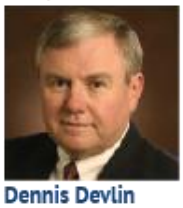
Lance Cotrell
Passages Ntrepid Corporation

Lorrie Cranor
Carnegie Mellon University

Paul Davis
Cisco

Behnam Dayanim
Paul Hastings

Lothar Determann
Baker & McKenzie



Dennis Devlin
SAVANTURE

Jan Dhont
Alston & Bird

Denelle Dixon-Thayer
Mozilla

Melanie Dougherty Thomas
Inform

Jenny Durkan
Quinn Emanuel

Heather Egan Sussman
Ropes & Gray

Khaled El Emam
Privacy Analytics

Scott Erven
Protiviti

Mark Faber
Prudential Financial

Donna Fickett
Navigate

Michelle Dennedy
Cisco

Thomas Finneran
IDennedy Project

Lara Flint
U.S. Senate Judiciary Committee

Jonathan Fox
McAfee

Dona Fraser
Entertainment Software Rating Board

D. Reed Freeman
WilmerHale

Susan Freiwald
USF School of Law

Leigh Freund
Network Advertising Initiative

Keithe Fricke
Catholic Health Partners

Jennifer Geetter
McDermott Will & Emery

Harley Geiger
Center for Democracy & Technology

Dipayan Ghosh
The White House

Rachel Glasser
GroupM

Speakers + Expert Commentators

Ian Glaser
Salesforce

Andrea Glorioso
Delegation of the EU to the US

Josh Goldfoot
Department of Justice

Daniel Goldstein
Treliant Risk Advisors

Kam Golpariani
Qualcomm

Alexis Goltra
Oracle

Scott Goss
Qualcomm

John Grant
Palantir

Kim Green
Zephyr Health

Adam Greene
Davis Wright Tremaine

Joseph Hall
Center for Democracy & Technology

Stacey Halota
Graham Holdings

Josh Harris
TRUSTe

Woodrow Hartzog
Samford University Cumberland Law

Justin Hemmings
Georgia Tech

Beth Hill
FordDirect

Jamie Hine
FTC

Mike Hintze
Microsoft

Dennis Hirsch
Capital University Law School

Sean B. Hoar
Davis Wright Tremaine

Kimberly Holmes
OneBeacon

Stuart Ingis
Venable

John Kropf
Northrop Grumman

Nathan Judish
Department of Justice

Constantine Karbaliotis
Nymity

Lara Kehoe Hoffman
Netflix

Janis Kestenbaum
Perkins Coie

Anthony Kim
Orrick Herrington & Sutcliffe

Jonathan King
CenturyLink

Sarah Kitchell
McDermott Will & Emery

Jacqueline Klosek
Goodwin Proctor

James Koenig
Paul Hastings

Michael C. Lamb
Reed Elsevier

Travis LeBlanc
FCC

Ronald Lee
Arnold & Porter

Naomi Lefkovitz
NIST

David Lieber
Google

Paul Luehr
Stroz Friedberg

Chris Madsen
Yahoo

Robert Mahini
Google

Fran Maier
GE Capital Bank

Aaron Massey
University of Maryland

Kristen J. Mathews
Proskauer

Debbie Matties
CTIA

Deven McGraw
HHS

Edward McNicholas
Sidley & Austin

Terrell McSweeny
FTC

Matthew Meade
Buchanan Ingersoll & Rooney

Jenny Menna
US Bank

Jon Mills
Boies, Schiller & Flexner

Maneesha Mithal
FTC

Kevin Moriarty
FTC

Kirk Nahra
Wiley Rein LLP

Saira Nayak
TUNE

Jon Neiditz
Kilpatrick Townsend & Stockton

Paul Ohm
Georgetown Law Center

Speakers + Expert Commentators

Nuala O'Connor
Center for Democracy & Technology

Eric O'Neill
Georgetown Group

Frank Pasquale
University Maryland Carey School of Law

Antonis Patrikios
Field Fisher

Pedro Pavón
Oracle

Harriet Pearson
Hogan Lovells

Doug Peddicord
Washington Health Strategies Group

Nancy Perkins
Arnold & Porter

Jules Polonetsky
Future of Privacy Forum

Katie Ratte
The Walt Disney Company

Al Raymond
TD Bank

Morgan Reed
The App Association

Joel Reidenberg
Fordham University

Becky Richards
NSA

Neil Richards
Washington University School of Law

Kari Rollins
Winston & Strawn

Steven Roosa
Holland & Knight

Michelle Rosenthal
T-Mobile

Paul Rosenzweig
Red Branch Consulting

K Royal
CellTrust

Todd Ruback
Ghostery

Ira Rubinstein
NYU Law School

Stephen Ruckman
BuckleySandler

David Rusting
U.C. Office of the President

Randy Sabett
Cooley

Al Saikali
Shook Hardy & Bacon

Peter E. Sand
MGM Resorts International

Lucia Savage
HHS

Florian Schaub
Carnegie Mellon University

Bruce Schneier
Security Technologist

Mark E. Schreiber
Locke Lord

Paul Schwartz
UC Berkeley School of Law

Adam Sedgewick
NIST

Evan Selinger
Rochester Institute of Technology

Nico Sell
Wickr

Stuart Shapiro
MITRE

David Sheidlower
BBDO

Rob Sherman
Facebook

Susan Shook
Procter & Gamble

Rebecca Shore-Suslowitz
Under Armour

Raj Singh
FordDirect

Sherrese Smith
Paul Hastings

Daniel Solove
George Washington University Law School

Lisa Sotto
Hunton & Williams

David Stampley
KimberLaw

Jay Stanley
ACLU

Gerry Stegmaier
Goodwin Procter

Jane Storero
Pepco Holding

Bob Sullivan
Independant Journalist

Michael Sussman
Perkins Cole

Peter Swire
Georgia Institute of Technology

Timothy Tobin
Hogan Lovells

Lourdes Turrecha
TeachPrivacy

Stuart Tyler
Intel

Laura VanDruff
FTC

Steven T. Visser
Navigant

Speakers + Expert Commentators

David Vladeck
Georgetown Law Center

Heidi Wachs
Jenner & Block

Ann Waldo
Waldo Law Offices

Hilary Wandall
Merck

Shaundra Watson
FTC

Yael Weinman
Verizon

Daniel Weitzner
MIT

Brad Weltman
Interactive Advertising Bureau

Heather West
Mozilla

Tim West
Accuvant

Stephen Wicker
Cornell University

Kurt Wimmer
Covington & Burling

Donna Wilson
Manatt

Peter Winn
University of Washington School of Law

Joel Winston
Hudson Cook

Christopher Wolf
Hogan Lovells

Christopher Yoo
University of Pennsylvania Law School

Heather Zachary
WilmerHale

Ruby Zefo
Intel

Ronise Zenon
U.C. San Diego

Chris Zoladz
Navigate

Marc Zwillinger
ZwillGen

CLE and CPE Credits

Participants are eligible to receive CLE credits with most state bars and CPE credits with IAPP and (ISC)[2].

1. CLE Credits. You will be able to earn CLE credits for attending this event. Written material will be provided to all participants. The credits awarded differ from state to state, and will be granted at the discretion of the individual state bars. The number of credits you will receive varies depending on how many sessions and workshops you attend. Each workshop is 3.0 hours and each session is 1.5 hours. Participants can take up to 2 workshops on Oct. 21. On Oct. 22-23, there are 8 session slots of 1.5 hours each. We are authorized to give up to 15.5 credits of CLE and 1.5 credits of ethics.

2. CPE Credits for IAPP. You will be able to earn CPE credits for IAPP. We are an approved provider with IAPP.

3. CPE Credits for (ISC)[2]. You will be able to earn CPE credits for certain (ISC)[2] certifications. Our event qualifies for Group B credits.

You might be able to obtain continuing professional education credits for other certifications. We recommend that you check first with the credentialing organization to make sure that our event will meet any required criteria and to know about the documentation you will need to submit.

We will have personnel at the event to assist you in documenting the sessions that you attended. To get credit, all you need to do is be sure to provide your name to our personnel taking down attendance at each session or sign any sign up sheets. Then, upon request, we will be able to generate documentation about the sessions you attended and the hours. We will maintain records pursuant to relevant bar and other requirements.

What makes the Privacy + Security Forum a unique event?

Our event distinguishes itself from others by:

- **Privacy + Security --** breaking down the silos between privacy and security.

- **Rigor and Real Knowledge Development --** being carefully designed so sessions have rigor and participants really learn.

Why combine privacy and security at the same event?

Privacy and security often exist in separate silos. Even privacy and security professionals who work down the hall from each other might rarely speak to each other. We must break down these silos because privacy and security are interrelated, and we cannot successfully achieve one without the other.

What is our vision of rigorous conference sessions?

We will work with speakers to ensure that their sessions are of real value to participants and provide **practical takeaway points**. We won't leave this to chance.

How does this event accommodate participants with very different levels of experience?

We will have different sessions for different types of participants. Each session will be assigned a level:

- **Level 101** is for foundational knowledge. These sessions focus on the basics. They will be rigorous, of course, but they won't assume much prior knowledge.

- **Level 201** is for experienced professionals. Level 201 sessions will assume a foundational knowledge and will explore topics with more depth.

- **Level 301** sessions will be for seasoned professionals who want to explore issues in an advanced way.

Who should attend?

- Privacy Professionals
- Security Professionals
- Chief Information Officers
- Law Firm Attorneys
- Academics
- Policymakers
- NGO / Think Tank
- Technologists

Although this event is designed for seasoned professionals, there will also be sessions that beginners can understand.

How does the event achieve greater rigor and knowledge development?

We aim to take the best elements from higher education and apply them to conferences.

- **Curricular Approach**. We see ourselves as trying to build a curriculum of sorts, a kind of miniature university.

- **Longer Sessions and More Depth**. We will have longer session times (between 1.5 hours to 3 hours) so topics can be covered in more detail.

- **Written Materials and Reading in Advance.** There will be written materials for sessions and assigned readings. These advance readings will provide greater focus for a session.

- **Participant Feedback.** We aim to collect a steady stream of participant input.

- **Scenario-Based Activities.** We encourage speakers to work through scenarios and be as concrete and practical as possible.

- **Our Involvement.** We will work closely with speakers to identify in advance the takeaways from each session.

Pre-Conference Workshops
Wednesday, October 21, 2015

TIME	ACTIVITY
8:00am – 9:00am	Breakfast and Introductory Remarks
9:00am – 10:30am	Concurrent Workshop 1 (Part 1 of 2)
10:30am – 11:00am	Break
11:00am – 12:30pm	Concurrent Workshop 1 (Part 2 of 2)
12:30pm – 1:30pm	Lunch
1:30pm – 3:00pm	Concurrent Workshop 2 (Part 1 of 2)
3:00pm – 3:30pm	Break
3:30pm – 5:00pm	Concurrent Workshop 2 (Part 2 of 2)

Day 1
Thursday, October 22, 2015

TIME	ACTIVITY
8:00am – 9:00am	Breakfast and Introductory Remarks
9:00am – 10:30am	Concurrent Session 1
10:30am – 11:00am	Break
11:00am – 12:30pm	Concurrent Session 2
12:30pm – 1:30pm	Lunch
1:30pm – 3:00pm	Concurrent Session 3
3:00pm – 3:30pm	Break
3:30pm – 5:00pm	Concurrent Session 4

Day 2
Friday, October 23, 2015

TIME	ACTIVITY
8:00am – 9:00am	Breakfast and Introductory Remarks
9:00am – 10:30am	Concurrent Session 5
10:30am – 11:00am	Break
11:00am – 12:30pm	Concurrent Session 6
12:30pm – 1:30pm	Lunch
1:30pm – 3:00pm	Concurrent Session 7
3:00pm – 3:30pm	Break
3:30pm – 5:00pm	Concurrent Session 8

Session Types

Workshops

Workshops provide a broad overview of a topic or more intensive background about a topic. Workshops are 3 hours long, with a 30-minute break.

Instructional Sessions

These sessions aim to instruct participants about particular areas of law or technology. Instructors will provide practical takeaways.

Policy Sessions

These sessions involve policy discussions about how privacy and security should be regulated.

Media & Culture Sessions

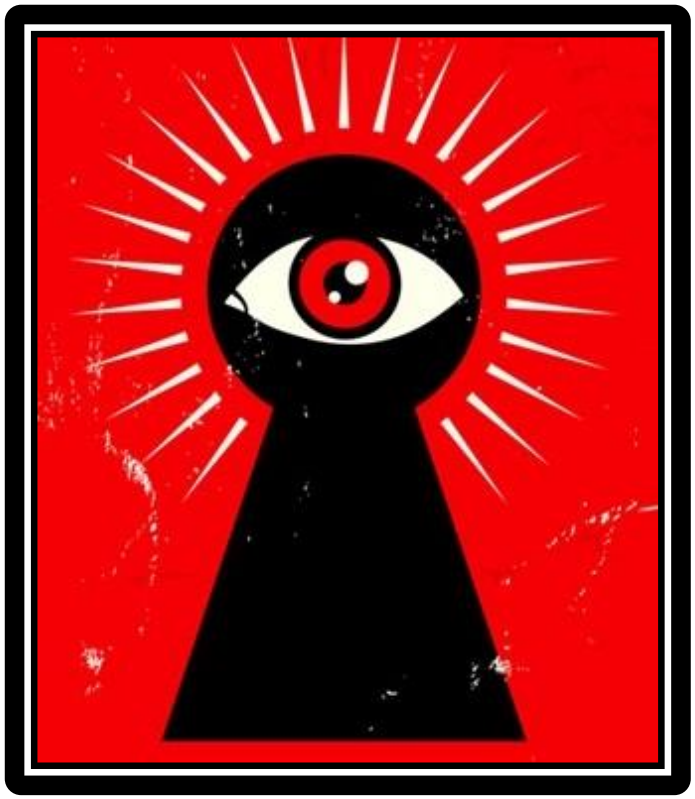
These sessions involve experts providing information about interesting resources and sharing their insights and perspectives.

Information Privacy Law: Foundations
(Workshop - Level 101)
Wed, Oct 21, 9:00 AM – 12:30 PM

This workshop will provide a short overview of information privacy law, demonstrating how various areas such as health privacy, consumer privacy, communications privacy, financial privacy, and data security are related. For privacy professionals, this is a great way to understand the whole field and fill gaps in your knowledge. For security professionals, this is a great introduction to information privacy law.

Daniel Solove
Professor at George Washington University Law School and President/CEO of TeachPrivacy

Randy Sabett
Special Counsel at Cooley, LLP



Understanding the FTC on Privacy and Data Security
(Workshop - Level 201)
Wed, Oct 21, 9:00 AM – 12:30 PM

This workshop will provide an in depth introduction to the FTC, examining how the FTC works, its various areas of jurisdiction, and its extensive body of consent decrees.

Woodrow Hartzog
Professor at Samford University Cumberland School of Law

Kevin Moriarty
Senior Attorney at Bureau of Consumer Protection, FTC

Data Security: Foundations
(Workshop - Level 101)
Wed, Oct 21, 9:00 AM – 12:30 PM

This workshop could also be titled: "Everything Privacy Professionals Should Know About Security But Were Afraid to Ask." It will cover common terms, various security standards, and key things that privacy professionals should know about technology.

David Rusting
CISO at U.C. Office of the President

Ronise Zenon
Mgr, Postmaster & IT Policy at U.C. San Diego

EU Privacy Law: Foundations
(Workshop - Level 101)
Wed, Oct 21, 1:30 PM – 5:00 PM

This workshop will provide an overview of EU privacy law, with a focus on the EU Data Protection Directive, US-EU Safe Harbor, BCRs, and the implications of the coming EU Privacy Legislation. For privacy professionals, this workshop will provide the foundation to understand what is going on in the EU. For security professionals, this workshop can be useful if they work at a global organization and want background on the EU.

Paul Schwartz
Professor, U.C. Berkeley Law School

John Bowman
Senior Principal, Promontory

Dennis Hirsch
Professor, Capital University Law School

PCI: The Essentials and Handling Data Breaches Involving Credit Card Data
(Workshop - Level 201)
Wed, Oct 21, 1:30 PM – 5:00 PM

This workshop will explore what you need to know about complying with the Payment Card Industry Data Security Standard (PCI) and how to handle data breaches involving credit card data. During this workshop we will discuss: (1) how to apply PCI and integrate compliance into an overall privacy and data security program; (2) how to minimize the scope of PCI through systems architecture and business process changes; (3) the unique aspects of handling data breaches involving credit card data. We will use real life case studies to demonstrate effective (and not so effective) breach response and negotiating fines and penalties with your card processor. We will share observations and lessons learned that no one in the credit card processing ecosystem will tell you.

Chris Zoladz
Founder, Navigate LLC

Donna Fickett
Managing Director, Navigate LLC

Data Security Law: Foundations
(Workshop - Level 101)
Wed, Oct 21, 1:30 PM – 5:00 PM

An overview of data security law – from HIPAA to GLBA to the FTC to Massachusetts to data breach notification. Learn about the different approaches that laws and regulations take to data security and the similarities and differences in each approach.

Lisa Sotto
Partner, Hunton & Williams LLP

Daniel Solove
Professor at George Washington University Law School and President/CEO of TeachPrivacy

David A. Stampley
Partner, KamberLaw

Susan Shook
Associate General Counsel, Procter & Gamble

California Privacy Law
(Workshop - Level 101)
Wed, Oct 21, 1:30 PM – 5:00 PM

In our California Privacy Law workshop, we will cover case studies and concrete compliance tasks and enforcement scenarios under California privacy laws, including (1) a jurisdictional overview (national and international applicability and preemption), (2) a selection of key California Privacy Laws, (3) how to establish or update a company's compliance program, (4) how to draft a Privacy Policy to comply with California law, (5) what other compliance documentation is needed or recommended, (6) enforcement, and (7) risk mitigation steps for companies within and outside California.

Lothar Determann
Partner, Baker & McKenzie LLP

GENERAL PRIVACY AND SECURITY

Privacy and Data Security Harms and Standing
(Instructional Session - Level 201)

This session will discuss the various approaches for defining privacy harms and how courts are reacting to them. The issue of standing will be covered extensively. What is the future of privacy and data security litigation for incidents? Is there a way to recognize harm, provide appropriate remedies to individuals who are harmed significantly, and avoid out-of-control costs?

Daniel Solove
Professor at George Washington University Law School and President/CEO of TeachPrivacy

Danielle Citron
Professor at University of Maryland Law School

Aaron Burstein
Attorney Advisor to FTC Commissioner Julie Brill

Do CPOs Need to Learn How to Code? The Skills Needed to Bridge the Law/Technology Divide
(Instructional Session - Level 201)

In this session, a law professor who previously worked as a computer programmer and the chief technologist of a consumer privacy organization will discuss what privacy professionals would benefit from knowing about technology.

Paul Ohm
Professor at Georgetown University Law Center

Joseph Lorenzo Hall
Chief Technologist, Center for Democracy & Technology

Privacy and Security in the Public vs. Private Sector: A Comparison
(Instructional Session - Level 101)

In this session, privacy officers with experience in both government privacy programs and corporate privacy programs will compare and contrast their experiences. What are the similarities and differences? What can each sector learn from the other?

Peter E. Sand
Executive Director of Privacy, MGM Resorts Int'l

John Kropf
Corporate Privacy Executive, Northrop Grumman Corp.

Yael Weinman
VP, Assistant General Counsel – Privacy at Verizon

Reed Freeman
Partner, WilmerHale

When Lawyers Talk With Engineers: Avoiding the Lost In Translation Problem
(Instructional Session - Level 101)

In this session, a software engineering professor and a law professor will demonstrate how engineers and lawyers can better communicate. Why does communication between lawyers and engineers often break down? Where is each side coming from? How does each side think? Through concrete exercises, this session will teach participants how to build a multi-disciplinary team and improve communication and understanding.

Aaron Massey
Professor of Software Engineering at U. Maryland Baltimore County

Peter Swire
Professor at Scheller College of Business Georgia Institute of Technology

Justin Hemmings
Research Associate at the Georgia Tech Scheller College of Business

Getting to Accountability: Effective Privacy and Security Management
(Instructional Session - Level 201)

This session provides you with the knowledge, resources and a plan to maximize the level of accountability. Accountability is the most important component of effective privacy and security management, yet it is often insufficiently developed in many programs. We will discuss privacy and security management activities throughout the organization not typically considered as part of a privacy program. What resources throughout your organization can you leverage for a privacy and security management program? How do you create a pragmatic plan to maximize the level of accountability?

Constantine Karbaliotis
Vice President, Privacy Office Solutions, NYMITY

Antonis Patrikios
Partner at Field Fisher

From the Economics to the Behavioral Economics of Privacy
(Instructional Session - Level 101)

In this session, Professor Acquisti will discuss his extensive empirical research in the behavioral economics of privacy and security. He will synthesize his wide body of work and highlight his most surprising and important findings, which reveal that many of our common assumptions about people's attitudes and behavior regarding privacy and security are wrong -- and these assumptions undergird many common practices and policies. Acquisti will explore the implications of his work and provide concrete and practical takeaways.

Alessandro Acquisti
Professor of Economics at Carnegie Mellon University

Legislating Privacy and Security: Lessons from the Legislative Process
(Instructional Session - Level 201)

This session will discuss lessons learned from inside and outside the legislative process. Why have many recent privacy and security laws failed to pass? What are the characteristics of successful privacy and security legislation? How can industry and legislators work together to find workable solutions? Is it conceivable for the US to break away from a sectoral approach and pass omnibus privacy legislation? What can privacy and security professionals learn about the legislative process that can make them more effective in their roles?

Heather West
Senior Policy Manager, Americas Principal, Mozilla

Lara Flint
Chief Counsel for National Security at U.S. Senate Judiciary Committee

Harley Geiger
Senior Counsel & Advocacy Director
Center for Democracy & Technology

Slade Bond
Democratic Counsel,
House Judiciary Committee

Privacy and Security at the Board Level: How to Interact with the Board of Directors

(Instructional Session - Level 201)

A company's board of directors has a unique and vital role to play in security and privacy. These issues will need to be on the board's agenda on a recurring basis. Boards operate in ways that may be foreign to the CISO or CPO who is asked for the first time to present at the board level. This session will focus on the essential elements of the Board's responsibilities for cybersecurity and data privacy. What keeps board members up at night? What do they expect from CISOs and CPOs? What is the most effective way to communicate with the board about privacy and security issues?

Harriet Pearson
Partner at Hogan Lovells and Former CPO and Cybersecurity Counsel at IBM Corp.

Jane Storero
Vice President, Corporate Governance, Corporate Secretary and Deputy General Counsel
Pepco Holdings, Inc.

Fran Maier
Founder, TRUSTe and Board Member, GE Capital Bank

Jenny Menna
Cybersecurity Partnership Executive, US Bank

Future Trends in Privacy and Security

(Policy Session - Level 101)

Our invited experts will bring along their crystal balls and peer into the future. What will be the top five privacy and security trends of the near future? What steps should organizations take now to prepare themselves?

Mike Hintze
Chief Privacy Counsel, Microsoft

Lance Cottrell
Chief Scientist , Ntrepid

Kirk Nahra
Partner, Wiley Rein LLP

Breaking Glass Ceilings: Executive Women in Privacy and Security

(Instructional Session - Level 101)

In this session, seasoned CPOs and CISOs will share their experiences as women in the privacy, security, technology, and legal fields. Which field was easiest and hardest for them to enter? How was it different 15, 10, 5 years ago compared to how it is today? What were their most difficult challenges as women in these fields? How did they handle those challenges? Is privacy really an equal playing for women? If so, why do they think this is the case? What do they wish they did differently in their careers? What have they had to do differently today to keep up with the evolving intersection of privacy, security, law, and technology? Where do they see this field going and do they see a place for women there?

Sharon Anolik,
President, Privacy Panacea

Debbie Bromson
Head of Global Privacy and Senior Compliance Counsel, Jazz Pharmaceuticals

Ruby Zefo
VP & Chief Privacy & Security Counsel, Intel

K Royal
VP, AGC Privacy & Compliance at CellTrust Corporation

Lourdes Turrecha
Consultant on Law and Policy to TeachPrivacy

Switch Hitters: Learning from Professionals Who Do Both Privacy and Security
(Instructional Session - Level 201)

In this session, professionals who serve in roles in both privacy and security or who have served in each of these roles in prior positions, will discuss what they have learned from their experiences.

Al Raymond
Specialist Leader, Privacy & Data Protection, Deloitte & Touche

Ruby Zefo
VP & Chief Privacy & Security Counsel, Intel

David Cass,
VP & CISO, Cloud and SaaS Operational Services, IBM

Congruence and Tension: Where Privacy and Security Align and Where They Don't
(Instructional Session - Level 201)

A session that will map out where privacy can help further security goals and vice versa. The session will proceed systematically, issue-by-issue.

Dennis Devlin
CISO, CPO and SVP of Privacy Practice for SAVANTURE

Stacey Halota
Vice President, Information Security and Privacy
Graham Holdings

Are Good Security Measures Always Good for Privacy? A Discussion of NIST Frameworks
(Instructional Session - Level 301)

While implementing security measures is important for privacy, they can also create risks which can undermine individuals' privacy. Panelists will discuss the Framework for Improving Critical Infrastructure Cybersecurity and how it balances the potential conflict. Session attendees will also hear about the latest NIST privacy risk management tools that can be used in concert with cybersecurity risk management processes.

Adam Sedgewick
Senior Information Technology Policy Advisor
NIST

Naomi Lefkovitz
Senior Privacy Policy Advisor, NIST

Jeff Brueggeman
VP Global Public Policy & Deputy CPO, AT&T

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PRIVACY+SECURITY ENGINEERING + DESIGN

Privacy, Security, and Fairness by Design: What the FTC Does (and Doesn't Do)
(Instructional Session - Level 201)

Important privacy and security considerations are implicated in the design of various products and services. How do regulators approach such issues? In this session, FTC Commissioner Julie Brill and privacy attorney Kurt Wimmer will explore how the FTC has dealt with these issues by discussing the relevant FTC cases and writings.

Maneesha Mithal
Bureau of Consumer Protection, FTC

Kurt Wimmer
Partner, Covington

Privacy and Security by Design
(Instructional Session - Level 201)

Despite the enthusiasm of privacy regulators, privacy by design (PbD) has only achieved mixed acceptance in the marketplace. This session will analyze the activities of industry leaders, who rely on engineering approaches and related tools to implement privacy principles throughout the product development and the data management lifecycles It will explore how companies can develop best practices in PbD and how this approach can assist in the dialogue with regulators. This session will also introduce the concept of security by design, explore how it may convey different meanings to technologists, to privacy advocates, and to governments, and discuss the legal underpinnings of security by design. The session will conclude by comparing the competing visions of privacy by design and security by design and the challenges that these competing visions pose for industry, government, and civil society.

Ira Rubinstein
Research Fellow. and Adjunct Professor of Law at New York University School of Law

Ronald Lee
Partner, Arnold & Porter

Privacy Engineering
(Instructional Session - Level 201)

This session will explore privacy engineering, exploring in detail how to build privacy and security into products, processes, applications, and systems. How can principles and standards be practically leveraged to create a common methodology to address privacy and security challenges? This session is designed for both technologists as well as non-technologists. Participants should have a good foundation in privacy and have some basic security knowledge, but the session will be accessible to professionals in both privacy and security.

Michelle Dennedy
VP and Chief Privacy Officer at CISCO

Thomas Finneran
Principal Consultant for the IDennedy Project

Jonathan Fox
Director of Data Privacy
at McAfee

Stuart Tyler
Senior Privacy Engineer at Intel

Privacy Impact Assessment Scenario Exercise
(Instructional Session - Level 201)

The privacy impact assessment is the heart of the privacy professional's job. Conducting a PIA well is critical in managing privacy risks and ensuring successful outcomes. In this audience participatory session, you will be given an initial set of facts and help guide an interview of an engineer. Through the exercise, you will learn how to build positive working relationships, elicit key information, and develop solutions that satisfy the business, engineering, and legal teams.

Scott Goss
Senior Privacy Counsel, Qualcomm

Kam Golpariani
CIPT, Qualcomm

Engineering for Privacy: What Is Easy? What Is Difficult?

(Instructional Session - Level 101)

Privacy lawyers will ask engineers for seemingly easy things to do, such as "Please delete the data!" or "Let's access the audit logs." For engineers, such requests are often made without an understanding of how easy or difficult certain things are to do. In this session, engineers explain why some things are easy and other things are hard. This session will provide practical examples of how lawyers and privacy professionals can rethink their requests to get the desired outcome without major technical headaches.

John Grant
Civil Liberties Engineer,
Palantir

Daniel Weitzner
Director, MIT Decentralized Information Group
Information Technology Industry Council

SECURITY

The FTC and Data Security
(Instructional Session - Level 201)

This session will consist of a detailed discussion about the FTC's data security jurisprudence, with analysis of all ~55 cases and FTC reports and guidance.

Terrell McSweeny
FTC Commissioner

Woodrow Hartzog
Professor of Law at Samford University
Cumberland School of Law

Cybersecurity Policy: The Role of the Government
(Policy Session -- Level 201)

Cybersecurity is a shared challenge between the private sector and government -- neither community has all the tools, but both bring necessary resources. What is the government's role? What information or resources does it provide that the private sector can't access? What risks does government engagement bring? What should the government do to protect private networks?

Paul Rosenzweig
Senior Advisor, The Chertoff Group
Principal, Red Branch Consulting

Edward McNicholas
Partner, Sidley & Austin

Human Security Risks: How to Detect and Deal with Malicious Insiders, Chinese Espionage, and Other Threats
(Instructional Session -- Level 101)

Trusted Insiders can pose a significant threat to the intellectual property of an organization. Security professionals must not only look outward when securing a system, they must become spy hunters, looking for internal exploits and penetrations that may not be easy to detect. This session will be led by Eric O'Neill, the former FBI Counterintelligence Operative who helped capture spy Robert Phillip Hanssen. O'Neill's story is depicted in the movie *Breach*, starring Ryan Philippe as O'Neill. The session includes an analysis of the Chinese intelligence collection goals and other recent internal penetrations. It sets out key ways that an organization can address the insider threat.

Eric O'Neill
Former FBI Operative and Founding Partner,
The Georgetown Group

Authentication and Control Frameworks: Operationalizing a Safeguard

(Instructional Session - Level 201)

Authentication is one of the bedrocks of a secure environment. It is also explicitly required by nearly every standard, framework and regulation dealing with protecting data. But while authentication may appear to be a discreet control mechanism, it is most successfully deployed as part of a control framework. Without focusing on one particular standard, the speakers in this session will take a close look at how "proving you are who you say you are" sits in those overall frameworks.

David Sheidlower
Global Head of Information Security (CISO), BBDO

Stuart Shapiro
Principal Information Privacy and Security Engineer at MITRE Corporation

Ian Glazer
Senior Director of Identity at Salesforce.com and Vice Chair of the IDESG Management Council

What We Can Learn from DefCon – Hacking Comes in All Varieties

(Instructional Session – Level 101)

DEF CON is one of the oldest and largest hacker conventions around, and this year had demos and presentations of hacking into a new Tesla and stopping it while running; hacking cell phones through vulnerable apps and reaching employer networks; cracking access codes to medical devices which can then compromise hospital systems; and accessing GPS coordinates with the possibility of diverting drones while in flight. This session will explore how hackers and forensic hacking research at DefCon can teach privacy and security professionals what threats are coming next and how better to address next generation compromises.

Mark E. Schreiber
Privacy and Cyber Security Group, Locke Lord

Scott Erven
Associate Director at Protiviti

Nico Sell
Founder of Wickr

HEALTH PRIVACY + SECURITY

The FTC and Cross-Sector Enforcement in Health, Education, and Other Domains
(Instructional Session - Level 201)

The U.S. has a sectoral approach to privacy and security, with specific laws governing each sector. However, the FTC has jurisdiction that reaches beyond any one sector. This session will explore how the FTC regulates across sectors, with a special focus on its role with health data and education data.

Maneesha Mithal
Bureau of Consumer Protection, FTC

Jennifer Geetter
McDermott Will & Emery

Heidi Wachs
Special Counsel at Jenner & Block

Health Data Breaches and OCR Investigations
(Instructional Session - Level 201)

This session will explore complex data breaches involving PHI and the OCR investigations and negotiations that take place in the aftermath. How do breaches involving PHI differ from breaches involving other data? How should OCR investigations be navigated? How should the negotiations be handled? What role should privacy officers and security officers play in the process and how should they work together?

Jennifer Archie
Partner, Latham & Watkins

Tim West
Enterprise Risk Practice Manager – Healthcare at Accuvant

Paul Luehr
Managing Director, Stroz Friedberg

The World Beyond HIPAA
(Instructional Session - Level 201)

More and more laws around the world are being amended and interpreted to regulate the collection, use, disclosure and disposal of health-related data, and the definition of what qualifies as health-related data can vary greatly. It is common to think of HIPAA first and foremost when thinking of health-related data, but HIPAA is only part of the equation. A number of other federal and state laws come into play, and data protection authorities around the globe are increasingly focused about this issue, including the FTC. Other areas of laws also interact with HIPAA, such as the common law, under which people have successfully sued in tort law for HIPAA violations. This session will explore the world of health data regulation beyond HIPAA.

Daniel J. Solove
Professor at George Washington University Law School and President/CEO of TeachPrivacy

Heather Egan Sussman
Partner, Ropes & Gray

Rebecca Shore-Suslowitz
Associate Counsel – Senior Manager, Global Privacy
Under Armour

Kate Black
Chief Privacy Officer and Corporate Counsel at 23andMe

New Health Information Technologies: Privacy and Security Risks

(Instructional Session - Level 201)

Medical information technology is rapidly evolving, including through innovative medical mobile applications, electronic health records, patient/physician online portals, and a variety of health monitoring devices. The emerging technologies offer great promise for preventive health care, medical treatment, data analytics, and research. But collecting, storing, and sharing personal health data through such technologies poses new privacy and security risks, and government, industry, and data protection experts are only beginning to appreciate, analyze and tackle these risks. This session will explore the range of risks involved and potential means of containing them through a discussion of various technologies, data use and sharing objectives and methodologies, and options for data protection solutions.

Nancy Perkins
Counsel, Arnold & Porter

Lucia Savage
Chief Privacy Officer, ONC at HHS

Ivelisse Clausell
Senior Compliance Counsel/Privacy Officer
Otsuka Pharmaceutical Development & Commercialization, Inc.

Hilary Wandall
AVP, Compliance & Global Privacy at Merck

Current and Future HHS Initiatives in Health Privacy

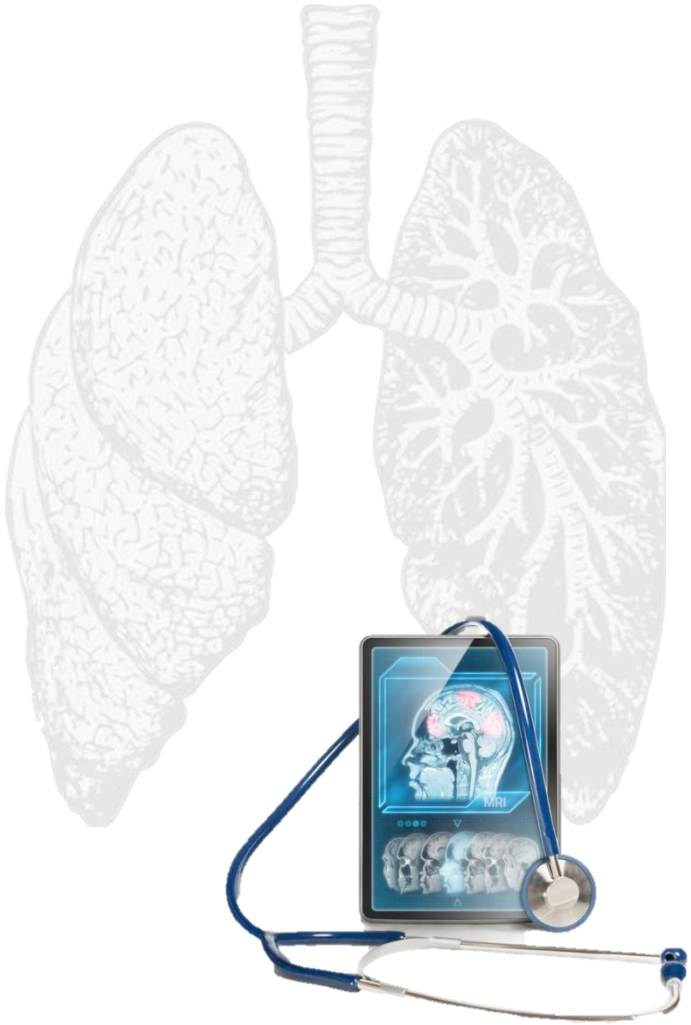
(Instructional Session – Level 201)

This session will focus on current and future initiatives at HHS: access guidance, the new portal, the upcoming audit, and cloud guidance.

Deven McGraw
Deputy Director for Health Information Privacy at HHS Office for Civil Rights

Adam Greene
Partner, Davis Wright Tremaine LLP

Kim Green
Chief Information Security & Privacy Officer at Zephyr Health



The Future of Research: What HIPAA Changes Are Being Proposed by Congress and HHS? What *Should* Be Changed?

(Instructional Session -- Level 201)

HIPAA and Research – it's like the weather; everyone complains about it, but no one does anything about it. Well, suddenly both Congress and HHS are proposing to do something. The bipartisan 21st Century Cures Act passed by the House contains provisions targeted at easing specific barriers to research. Plus, HHS has put forward a complex and lengthy change to the Common Rule re: research that proposes sweeping changes, particularly to biospecimens and consent. Are these the right fixes? Would there be unintended consequences of these proposals? In a complex, rapidly changing scientific environment that includes innovations from "n of 1" to "n of millions" trials, what changes in the legal environment make the most sense? This session will not only bring you up to date, but will also solicit your ideas about wise legislative and regulatory changes.

Ann Waldo
Principal, Waldo Law Offices

Doug Peddicord
President, Washington Health Strategies Group

Daniel Barth-Jones
Professor, Columbia University, Mailman School of Public Health

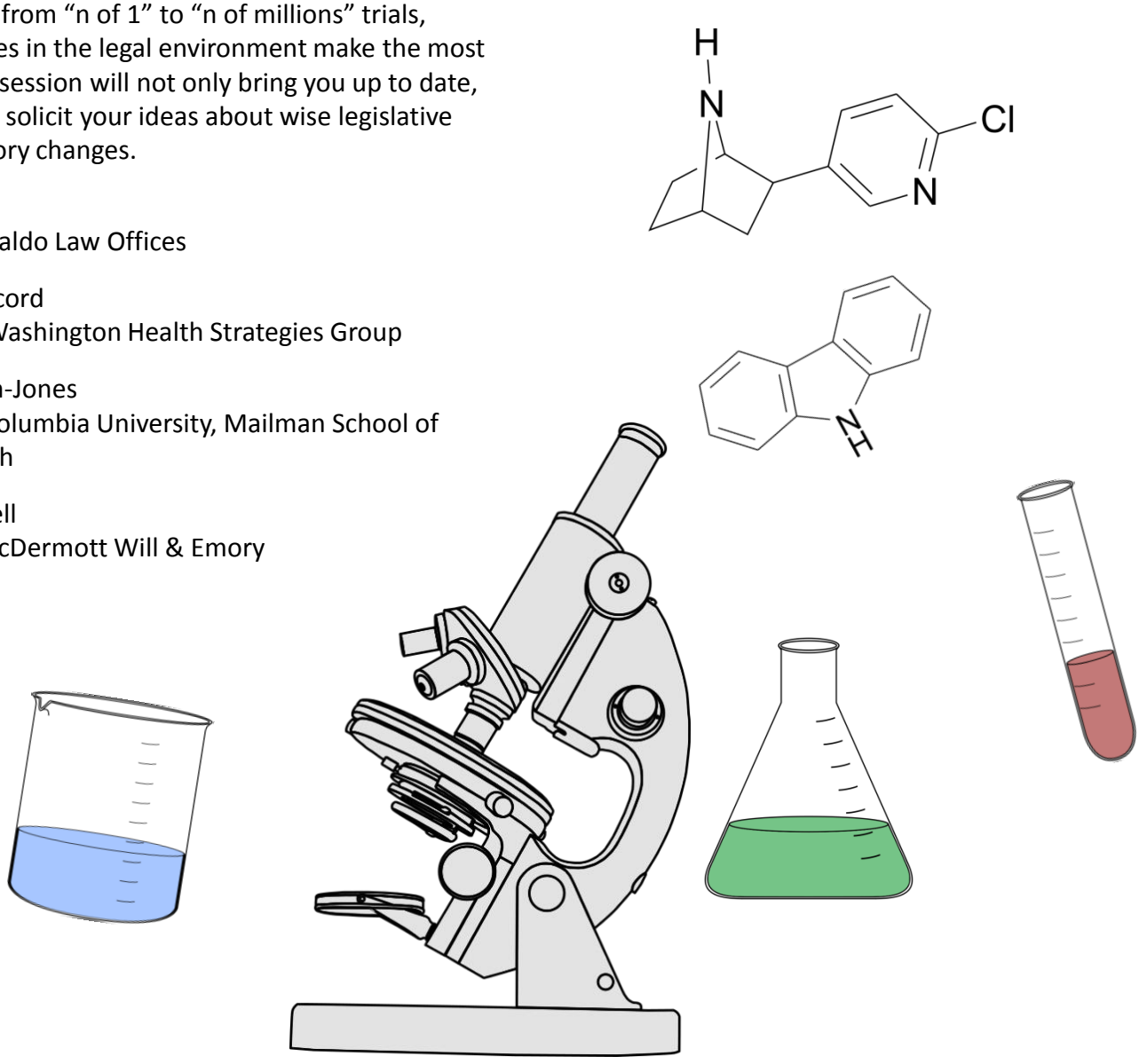
Sarah Kitchell
Attorney, McDermott Will & Emory

Health Data De-Identification

(Instructional Session - Level 301)

In this session, de-identification expert Professor Khaled El Emam, will discuss health data de-identification.

Khaled El Emam
Canada Research Chair, University of Ottawa
Founder & CEO, Privacy Analytics



COMMUNICATIONS PRIVACY + SECURITY

Communications Privacy and Security and FCC Enforcement

(Instructional Session - Level 201)

This session will involve a detailed discussion about FCC privacy and security enforcement and the current goals and direction of the FCC on these issues.

Travis LeBlanc
Chief of the Bureau of Enforcement
FCC

Sherrese Smith
Partner, Paul Hastings LLC

Christopher Yoo
Professor at University of Pennsylvania Law School

EDUCATION PRIVACY + SECURITY

Student and Children's Data: FERPA, COPPA, and Beyond

(Instructional Session - Level 201)

This session will help organizations that handle student data and children's data identify priority areas for compliance, with a focus on new technologies in schools and advertising and marketing practices for children's data in general. We will discuss updates to the FTC COPPA rule FAQs, FERPA, new state laws, new self-regulatory measures, and efforts to pass a national student privacy law.

Jules Polonetsky
Executive Director, Future of Privacy Forum

Katie Ratte
Assistant General Counsel, Privacy and Global Public Policy, The Walt Disney Company

Joel Reidenberg,
Professor at Fordham Law School

SURVEILLANCE

Data and Goliath: A Conversation with Bruce Schneier on Surveillance
(Instructional Session - Level 101)

This session will involve a conversation between Becky Richards, Peter Swire, and Bruce Schneier about Schneier's new book *Data and Goliath* on corporate and government surveillance. Then the audience will have a chance to engage in Q&A with Schneier and the speakers. A major topic of discussion will be NSA surveillance.

Bruce Schneier
Fellow at the Berkman Center for Internet and Society at Harvard Law School, and CTO of Resilient Systems

Becky Richards
Chief Privacy Officer, NSA

Peter Swire
Professor at Scheller College of Business Georgia Institute of Technology

Federal and State Electronic Surveillance Laws and Their Impact on Organizations
(Instructional Session – Level 201)

This session will explore how ECPA and state electronic surveillance laws like CalECPA impact businesses and other organizations. To what extent does federal law (ECPA and others) preempt more protective state laws and when must companies comply with state laws? How do the constitutional cases interact with the statutory rules in this area? State electronic surveillance law affects a wide array of organizations and plays a more significant role than what many realize. The session will also discuss reform efforts underway regarding these laws and the implications of reform for businesses and other organizations.

Susan Freiwald
Professor, USF School of Law

Michael Sussmann
Partner, Perkins Coie

The Electronic Communications Privacy Act and Access to User Data: Advanced Issues
(Instructional Session -- Level 301)

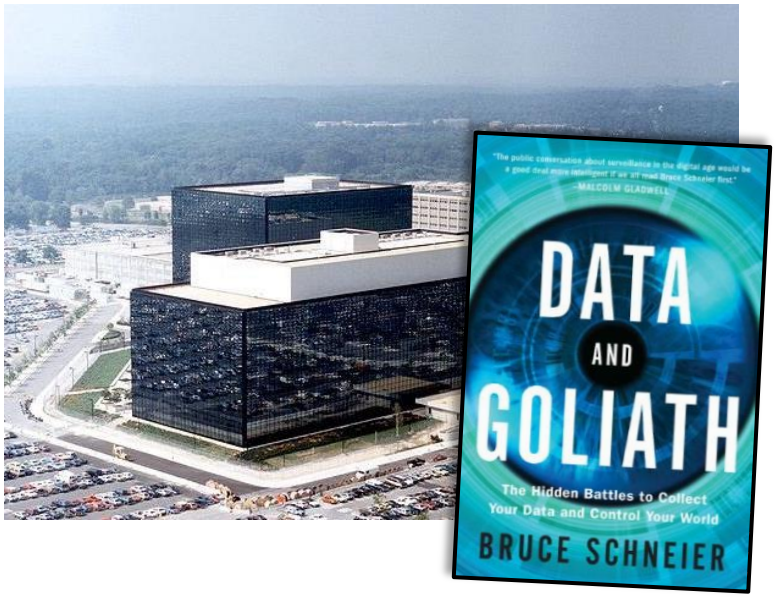
This session will focus on how the Electronic Communications Privacy Act (ECPA) applies to various ways in which the government and third parties have sought access to user data in new ways not envisioned by Congress when the law was passed in 1986. How does ECPA govern third-party access to user accounts after the user has died? Access by government regulators in non-criminal cases? When can providers access their own users' email content for advertising and other purposes? When can data be disclosed in response to the pressure of foreign governments to turn over user data? In what ways does implicit user consent based on disclosures in the Terms of Service impact these issues?

Marc Zwillinger
Founder, ZwillGen

Chris Madsen
Senior Legal Director, U.S. Law Enforcement & Security, Yahoo

Elizabeth Banker
Head Legal Counsel - Global Law Enforcement, Twitter

Nathan Judish
Senior Counsel, Computer Crime and Intellectual Property Section, U.S. DOJ



SURVEILLANCE

The Impact of Government Surveillance Law on Business

(Instructional Session - Level 101)

This session will focus on how government surveillance law is affecting businesses. Recently, in the *Schrems* case, the Safe Harbor Arrangement was deemed invalid because of the failure of U.S. law to reign in NSA surveillance. ECPA is in dire need of reform, a cause championed by many businesses. Microsoft is fighting government information gathering efforts for data maintained in Ireland. Government surveillance law is creating great difficulties for businesses – what can businesses do in response?

Nuala O'Connor
President & CEO, Center for Democracy & Technology

Gerry Stegmaier
Partner at Goodwin Procter

Frank Torres
Senior Policy Counsel, Microsoft

BIG DATA

Big Data and Discrimination

(Policy Session -- Level 101)

This session will explore the ways in which Big Data can have discriminatory effects. Even without discriminatory intent, Big Data can affect different groups of people in ways that have a significant impact on how they are treated, how decisions are made about them, opportunities available to them, or the kinds of messages they are exposed to. The session will focus around concrete case studies as a launching point to defining the problem and engaging in a discussion of the appropriate policy responses.

Dipayan Ghosh
Technology Policy, The White House

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
U.S. Department of Justice

Christopher Wolf
Partner at Hogan Lovells

INTERNATIONAL PRIVACY + SECURITY

EU Data Protection Regulation : What Will Change? What Remains the Same?

(Instructional Session - Level 201)

The EU Data Protection Regulation is a game-changer. It will be directly binding once enacted and appears headed to make important changes to the substantive and procedural law of EU privacy. This up-to-date session will explore how the EU Data Protection will alter the current status quo and identify practical steps companies can take now for compliance success under the new EU status quo for privacy.

Paul Schwartz
Professor at U.C. Berkeley Law School

Shaundra Watson
Senior Advisor to Chairwoman Edith Ramirez, FTC

Andrea Glorioso
Counsellor for the Digital Economy,
Delegation of the EU to the US

Interoperability and Cross-Border Data Transfer: APEC, EU BCRs, and Beyond

(Instructional Session - Level 301)

The publication of the EU-APEC Referential document in 2014 marked a significant step towards greater global interoperability of international data transfer frameworks and opened up the possibility of achieving dual certification under both APEC Cross Border Privacy Rules and EU Binding Corporate Rules. But how do you know if this is the right route for your business? This session will offer a deep-dive into the requirements of both data transfer frameworks and insights for companies considering going down this path as to exactly what the process involves and the potential benefits of incorporating dual certification into your data governance strategy.

Chris Babel
CEO, TRUSTe

Jan Dhont,
Partner, Alston & Bird

Josh Harris
Director of Policy, TRUSTe

The Sunken Safe Harbor: The ECJ's Decision and Beyond

(Instructional Session - Level 201)

What has changed for American companies after the ECJ's dramatic decision on October 6, 2015 invalidating the Safe Harbor? This panel will discuss the meaning of this decision, steps for American companies to take now, and likely future developments ahead in European data protection.

Lothar Determann
Partner, Baker & McKenzie LLP

Andrea Glorioso
Counsellor for the Digital Economy,
Delegation of the EU to the US

Donna Wilson
Partner at Manatt

Defining "Reasonable Data Security" and "Personal Data" Across Borders

(Instructional Session - Level 201)

How does one achieve "reasonable data privacy and security" when handling big data? Jurisdictions around the world differ in their definitions for "personal data" and what is considered "reasonable" when it comes to data usage and protection. What is the best way to secure big data in a way that satisfies the relevant standard, but also does not incur undue cost or impediments to innovation? Since the capture of "personal data" usually triggers enhanced security measures, transparency to data flows and categorizing data are the first steps in implementing an effective data governance plan. However, these definitions can differ depending on jurisdiction and the data's processing stage within its lifecycle. For example, German law provides for "pseudonymous data" which may allow pseudonymous device identifiers to escape "personal data" categorization. All of these variables will impact your compliance obligations and your company's competitive edge.

Saira Nayak
CPO, Tune

Jim Adler
VP & CPO, Metanautix

CONSUMER PRIVACY + SECURITY

Tracking and Targeting: Online, on Mobile Devices, and in Social Media

(Instructional Session – Level 301)

This session will focus on legal and self-regulatory compliance challenges faced by companies whose business models focus on tracking and targeting advertisements and content to consumers. It will explore different tracking and targeting business models and the thorny legal issues that they sometimes raise.

Reed Freeman
Partner, WilmerHale

Heather Zachary
Partner, WilmerHale

Brad Weltman
Senior Director of Public Policy, Interactive Advertising Bureau

Alexis Goltra
Chief Privacy Officer & Assistant General Counsel, Oracle Corporation

Understanding the Internet's Hidden Digital Architecture

(Instructional Session - Level 201)

As digital marketing has grown--with over $40 Billion annually spent in the US--the invisible plumbing has grown increasing complex. This session will break down this architecture into an easy to understand overview and will also discuss how it will change in the coming years, and what opportunities and risks that evolution entails.

Todd Ruback
Chief Privacy Officer, Ghostery

Rachel Glasser
Partner; Director Digital Privacy and Partner Activation at GroupM

Denelle Dixon-Thayer
Senior Vice President, Business and Legal Affairs, Mozilla

Privacy and Trust

(Instructional Session - Level 201)

Privacy rules are important not just for compliance with legal requirements, but also in establishing trust between companies and those people whose data they hold. In this session, a law professor (Richards), a tech company in-house counsel (Brown), and a cloud executive (King) will talk about privacy and trust, and how privacy rules can be used to create value between entities and users, establishing sustainable information relationships in the digital age.

Neil Richards
Professor, Washington University School of Law

Emily Schlesinger
Privacy Attorney, Microsoft

Jonathan King
VP, Platform Strategy & Business Development at CenturyLink

Understanding the FTC: Lessons from FTC Investigations and Other Experiences
(Instructional Session - Level 201)

What should one do when the FTC knocks on the door? What works best when dealing with an FTC investigation? In this session, we will learn how to understand the FTC and how it operates. We will work through a concrete example of how to interact with the FTC.

Timothy Tobin
Partner at Hogan Lovells

Jamie Hine
Bureau of Consumer Protection, FTC

James Koenig
Privacy, Cyber and Data Management Practice
Paul Hastings LLP

Michael Lamb
Chief Counsel, Privacy and Information Governance
Reed Elsevier

Michelle Rosenthal
Senior Corporate Counsel at T-Mobile

Designing User Interfaces for Privacy
(Instructional Session – Level 301)

In this interactive workshop, we'll explore how to design user interfaces with privacy in mind. Participants will work through a scenario to design a real-life product experience that educates people on privacy and controls and provides important privacy information in context.

Rob Sherman
Deputy Chief Privacy Officer, Facebook

Morgan Reed
Executive Director, ACT – The App Association

Laura VanDruff
Division of Privacy and Identity Protection, FTC

FTC Privacy and Security Alumni: Reflections and Insights
(Instructional Session - Level 201)

A group of privacy and security professionals who used to work at the FTC on privacy and security issues will discuss their experiences at the FTC and the insights they learned about the agency and more generally.

Joel Winston
Partner at Hudson Cook LLP

Lydia Parnes
Partner, Wilson Sonsini Goodrich & Rosati

Debbie Matties
Vice President, Privacy – CTIA

Janis Kestenbaum
Partner, Perkins Coie

Robert Mahini
Senior Policy Counsel, Google

Privacy and Security Self-Regulation 2.0
(Instructional Session – Level 201)

There have been self-regulatory endeavors since the early days of privacy and security, but these days there are significant new challenges. How should self-regulation be kept up to date with rapidly advancing industries? How should self-regulation encourage best practices, privacy by design, and the interplay between emerging technologies and interconnected industries, especially those involving the Internet of Things?

Leigh Freund
President & CEO, Network Advertising Initiative (NAI)

Dona Fraser
VP Privacy Certified, Entertainment Software Rating Board (ESRB)

Stuart Ingis
Partner, Venable

THE INTERNET OF THINGS

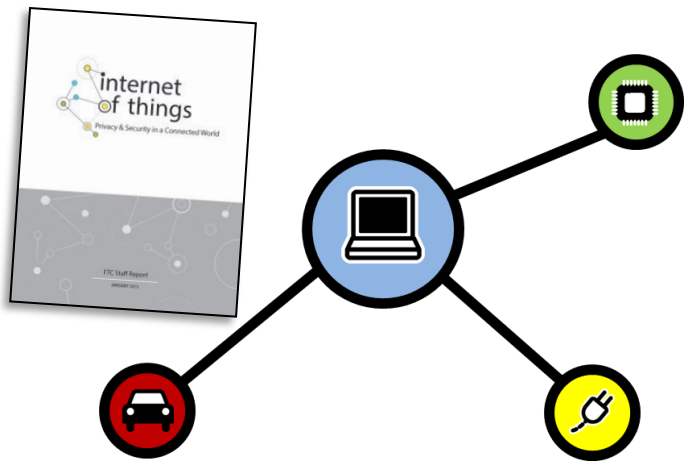
Privacy and Security for the Internet of Things
(Policy Session -- Level 201)

In early 2015, the FTC released a report on the privacy and security challenges posed by the Internet of Things. This session will begin with concrete case studies such as the connected car and smart grid. We will discuss how the promise to consumers is combined with a substantial threat to privacy in the form of increased collection of personally identifying information. We will also discuss the novel threats to information security that arise with these technologies. What measures are being implemented to address these issues? These case studies will then lead to a larger policy discussion. What is the role of regulation? To what extent must design be regulated? How should research into the revelatory nature of collected data inform policy development? Can notice-and-choice still work, or is the Internet of Things its death knell? Should the law regulate data collection or use?

Beth Hill
General Counsel and Chief Compliance Officer, FordDirect

Raj Singh
Chief Information Officer, FordDirect

Gerry Stegmaier
Partner at Goodwin Procter



Security Risks with the Internet of Things: Lessons from a Live Demonstration
(Instructional Session – Level 301)

During this session we will do a hands on demo using open-source tools and custom scripts to (1) conduct reconnaissance of real IoT devices in a test environment and (2) conduct denial of service attacks on these devices using open-source tools and custom scripts. We will then analyze the results in terms of legal requirements for secure design and legal liability for failure of critical IoT devices. Although at a 301 level, this session will be accessible for participants without a technical or security background.

Steven Roosa
Partner, Holland & Knight

Joseph A. Calandrino
Director, Stroz Friedberg

Designing Notice and Consent into the Internet of Things: A Hands-on Workshop
(Instructional Session - Level 201)

Privacy notices are often long, difficult to understand, and don't appear at opportune times. Constrained interfaces on mobile devices, wearables, and smart home devices exacerbate the issue. In this workshop Professor Lorrie Cranor and privacy researcher Dr. Florian Schaub offer concrete guidelines on how to select the most effective notice and consent mechanisms for a given system or device. They will present a taxonomy of notice options, based on their research, and guide participants through hands-on design exercises.

Lorrie Cranor, Professor of Computer Science and Engineering & Public Policy, Carnegie Mellon University

Florian Schaub, Postdoctoral Fellow, School of Computer Science, Carnegie Mellon University

THIRD PARTY RELATIONSHIPS

Vendor Management
(Instructional Session - Level 201)

What are the key parts of privacy and security vendor management? What role does a privacy office, a security office, a procurement office, and counsel play in the process? What level of vendor oversight is the government looking for, what level is best practice, and how does an organization focus limited resources to best reduce risk in this area? How important is a right to audit to obtain in contract? How important is it to actually audit vendors (especially with limited resources)? How much credence should be given to independent assessments, such as a SOC 2 report? Should vendors provide documents such as a risk analysis or internal policies to their customers, or does that actually raise more information security concerns than it addresses?

Kristen Mathews
Partner, Proskauer

Mark Faber
Vice President, Senior Regulatory Counsel – Privacy, Prudential Financial

Mohamed Ayad
Sr. Industry Solution Specialist , US Health and Life Sciences, Microsoft

High-Risk Data in the Cloud and the Internet of Things: What Really Works?
(Instructional Session – Level 301)

Cloud computing naturally diminished transparency and collaboration between customers and vendors, but the issues of trust, transparency and collaboration with vendors have become more critical with new data uses and threats , and never more so than as the world hurtles into the more complex networks of the Internet of Things. What are the most proven ways in which to gain confidence that a vendor has made the necessary investments and is willing and able to provide transparency? Do the ever-longer questionnaires between customers and vendors result in meaningful risk reduction? Can prioritization based on data classification enable the representations organizations need from the vendors handling information that really matters? This session will take on those questions as well as provide a toolkit for the vendor relationship lifecycle for high value/risk information, including detailed approaches for prioritization; due diligence; risk allocation, mitigation and shifting; monitoring; incident response collaboration; and evaluation.

Jon Neiditz
Partner, Kilpatrick Townsend & Stockton LLP

Stuart Tyler
Senior Privacy Engineer at Intel

Cliff Baker
Managing Partner, Meditology

Control in the Information Ecosystem: Who Has it? Does It Exist?

(Instructional Session - Level 201)

In today's business environment, with third-party data services growing exponentially, multi-layer outsourcing of data needs is becoming more and more common. Yet regulators such as the FTC, the NY Department of Financial Services, and the Securities and Exchange Commission have taken the position that this outsourcing does not mean an outsourcing of the primary businesses' responsibility for that data; businesses are being held responsible for breaches and other unintended data uses at their third-party vendors. How does this impact corporate obligations for data protection and breach response? If a company's data is breached at a third-party site, how can it ensure that the third-party will respond appropriately and enable the company to timely notify affected customers and regulators? More fundamentally, how much "control" can the company truly have over data held by a third party, particularly when that third party may share data with still more entities? And how effectively can that company prove what did not happen—e.g., what customer data was not compromised—in a security incident when the incident occurred off-site? This session will explore the data risks of sharing through unaligned control environments, and the issues of data ownership, custodianship, control, rights, and obligations in the third-party ecosystem.

Daniel J. Goldstein
Senior Director, Treliant Risk Advisors

Stephen M. Ruckman
Senior Associate, BuckleySandler LLP

Steven T. Visser
Managing Director, Navigant

CULTURE AND MEDIA

Privacy and Security Fiction Club
(Culture & Media Session - Level 101)

Many novels, such as Orwell's *1984*, have informed the policy debate about privacy and security. This session will feature top experts discussing their favorite novels and stories about privacy and security, including old classics and new hits.

Peter Winn,
Assistant U.S. Attorney, U.S. DOJ and Lecturer,
University of Washington School of Law

Joseph Jerome
Policy Counsel at Future of Privacy Forum

Jacqueline Klosek
Partner, Goodwin Proctor

Kevin Bankston
Director, Open Technology Institute and Co-Director,
Cybersecurity Initiative, New America

Heather West
Senior Policy Manager, Americas Principal, Mozilla

Privacy and Security Non-Fiction Club
(Culture & Media Session - Level 101)

What are the best non-fiction books and writings about privacy and security? What are the new and classic must-reads? This session will feature leading experts discussing the non-fiction works they deem to be essential to one's library.

Frank Pasquale
Professor at U. Maryland Carey School of Law

Evan Selinger
Professor, Dep't Philosophy, Rochester Institute of Technology

Jay Stanley
Senior Policy Analyst, ACLU

Others TBA

Privacy and Security Film and TV Club
(Culture & Media Session - Level 101)

This session features top experts discussing films and TV series with privacy and security themes. Are privacy and security portrayed realistically? What is the best privacy or security movie of all time?

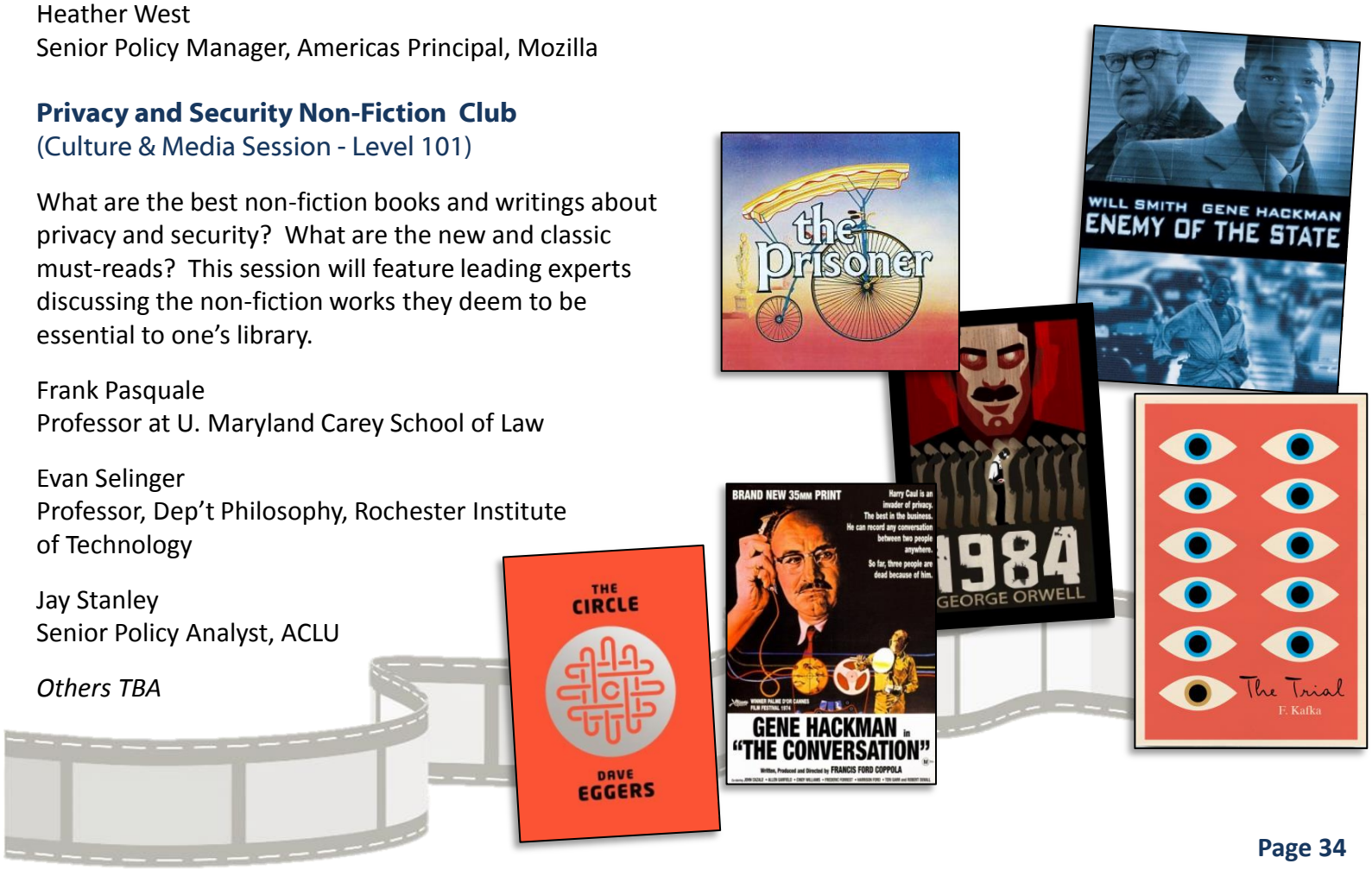
James Aquilina
Executive Managing Director, Stroz Friedberg

Lara Kehoe Hoffman
Global Director of Data Privacy and Security at Netflix

Chris Calabrese
Vice President, Policy
Center for Democracy & Technology

David Lieber
Senior Privacy Policy Counsel, Google

Ian Ballon
Shareholder, Greenberg Traurig



RISK MITIGATION + INCIDENT RESPONSE

Data Breach Response Scenario Exercise
(Instructional Session - Level 201)

What is the best way to handle a data breach? What are factors that affect the timing of informing law enforcement, federal and state privacy regulators, and affected customers? When and how should lawyers engage outside vendors (such as forensic experts and PR firms) in a response? This session will present a variety of different scenarios and provide step-by-step pragmatic advice.

James Aquilina
Executive Managing Director, Stroz Friedberg

Antony P. Kim
Partner , Orrick LLP

Jenny Durkan
Partner, Quinn Emanuel

PR for Data Security and Privacy Crises
(Instructional Session - Level 201)

In this session, PR expert Melanie Thomas will discuss how to handle PR in a data security or privacy incident. Through the use of one or more concrete scenarios, participants will explore step-by-step what to do and the consequences of making a PR misstep. Devlin Barrett, a reporter from the Wall Street Journal, who covers data security , will provide insight about how various statements and actions are perceived by the media.

Melanie Dougherty Thomas
Managing Director, Inform LLC

Devlin Barrett
Reporter, Wall Street Journal

Cyber Insurance: How It Works, How to Select a Policy, and Emerging Trends and Practices
(Instructional Session - Level 201)

This session will discuss the history of cyber insurance, including the evolution of cyber insurance products and judicial interpretations of cyber insurance policies. It will also review information system risks, measures that can mitigate those risks, the role of cyber insurance in transferring any remaining risks, and the types of cyber insurance coverage currently available.

Sean B. Hoar
Partner, Davis Wright Tremaine LLP

Kimberly Holmes
VP, Product Development, OneBeacon Professional Insurance

Keith Fricke
Principal Consultant, tw-Security

The Role of Privilege in Privacy and Security Investigations

(Instructional Session – Level 301)

Should portions of breach investigations be privileged? If so, what should be privileged and how? Is outside counsel needed, or will involvement of internal counsel suffice? Can a risk analysis (e.g., consistent with NIST 800-30) be privileged? Can a compliance assessment (e.g., an evaluation of compliance with one or more privacy or security regulations) be privileged? What about a security incident assessment? If any of these documents can be privileged, should they be? How can privilege be intentionally or unintentionally waived?

Adam Greene
Partner, Davis Wright Tremaine LLP

Bob Chaput,
CEO and Founder, Clearwater Compliance

Conducting a Privacy Investigation

(Instructional Session - Level 201)

This session examines both general investigations of possible misconduct as well as the investigations of privacy violations, including data breaches. In general investigations of misconduct, how can a company investigate potential misconduct without running afoul of data protection laws? How does a cross-border investigation affect that calculus? How does one deal with US governmental agencies demanding information that another jurisdiction's data protection laws might prohibit supplying? Regarding the privacy or data breach investigation, if someone is suspected of a privacy or data security violation, how and when should the suspect be approached?

Behnam Dayanim
Partner, Paul Hastings LLP

Pedro Pavón
Corporate Counsel at Oracle

Complex Legal Challenges with Data Breach Response and Cyber Forensics

(Instructional Session – Level 301)

When responding to a data breach, security professionals must often deal with very complicated challenges created by data security law. Providing individual notice can be challenging when certain data is encrypted. Investigating a breach might involve dealing with systems in the EU and having to deal with EU data protection laws. In this session, a group of CISOs will discuss the particular challenges they find most vexing about data breach response as well as how and when they work with privacy professionals and counsel to grapple with these difficult matters.

Devon Bryan
VP, Global Technical Security Services (CISO) at ADP

Paul Davis
Director - Advanced Threats Security Solutions Architecture Team at Cisco

Data Breach Liability
(Instructional Session – Level 201)

This session will examine when various parties are liable in private lawsuits arising from a data breach and to whom. How do plaintiffs meet the causation requirements? What are the successful and unsuccessful theories of liability? How do plaintiffs demonstrate the harm, how is it quantified, and is it even required? When might companies be liable to other companies? What technical and administrative measures can be implemented that will reduce liability risk?

Al Saikali
Partner at Shook Hardy & Bacon, LLP

Matthew Meade
Partner at Buchanan Ingersoll & Rooney PC

Kari Rollins
Partner, Winston & Strawn LLP

Data Breach Fallout: The Legal and Ethical Considerations Concerning Stolen Data
(Instructional Session – Level 201)

Data breach prevention and response are widely-discussed, but less studied are the legal and ethical considerations that apply to stolen data after it has been removed from the private to the public domain. What legal options are available to organizations seeking to contain a post-breach data feeding frenzy? And what limits should apply to the media in its access and use of private or confidential information that has concededly been stolen by hackers? This panel will discuss the legal, ethical, and practical considerations that must be confronted when confidential data is made public by criminal acts.

Michael Gottlieb
Partner, Boies, Schiller & Flexner

Jon Mills
Dean Emeritus & Counsel at Boies, Schiller and Flexner

Josh Goldfoot
Deputy Chief for Cyber, DOJ National Security Division

Bob Sullivan
Independent Journalist, formerly with MSNBC and NBC News

We extend a big thank you to our sponsors.

STROZ FRIEDBERG

TUNE

manatt

Buckley Sandler LLP

SafeGov

Microsoft

Treliant RISK ADVISORS

ROPES & GRAY

WILMERHALE

BOIES SCHILLER & FLEXNER

COVINGTON

McDermott Will & Emery

GHOSTERY

AllClear ID

TRUSTe

CYBERSPONSE ENABLED SECURITY

evolver

FierceITSecurity

berryseed digital media strategy

TEACHPRIVACY

If you are interested in our sponsorship options, please contact us at info@privacyandsecurityforum.com

Your Feedback

Our philosophy is to deliver an event that is tailored to our participants' needs.

We will listen to your suggestions.

We welcome your ideas for session topics.

Tell us the knowledge you want to know, and we'll bring it to you.