



# **BCLT PRIVACY LAW FORUM: SILICON VALLEY**

**MARCH 21, 2013**



**BERKELEY CENTER FOR  
LAW & TECHNOLOGY**



# AGENDA

**8:30 am - 9:00 am** Breakfast & Registration  
Morning Presiding Officer Chris Jay Hoofnagle, BCLT and Berkeley Law

**9:10 am - 10:30 am** **Panel 1: The EU-US Privacy Collision**

- ▶ Paul Schwartz, BCLT and Berkeley Law
- ▶ Christopher Wolf, Hogan Lovells
- ▶ Karl-Nikolaus Peifer, University of Cologne Law School
- ▶ Michael Hintze, Microsoft Corporation

**10:30 am - 11:00 am** Break

**11:00 am - 12:15 pm** **Panel 2: Privacy and The Price of Free**

- ▶ Chris Jay Hoofnagle, BCLT and Berkeley Law
- ▶ Dalton Caldwell, App.Net
- ▶ Michael Glaser, Perkins Coie LLP
- ▶ Daren Orzechowski, White & Case LLP

**12:15 pm - 12:45 pm** Lunch  
Afternoon Presiding Officer Paul Schwartz, BCLT and Berkeley Law

**12:45 pm - 1:45 pm** **Keynote**

- ▶ Travis LeBlanc, Special Assistant Attorney General, California Department of Justice

**1:45 pm - 3:15 pm** **Panel 3: The Management of Privacy Processes: The CPO and Beyond**

- ▶ Deirdre Mulligan, BCLT and UC Berkeley School of Information
- ▶ Kenneth Bamberger, BCLT and Berkeley Law
- ▶ Harriet Pearson, Hogan Lovells and Former Chief Privacy Officer, IBM
- ▶ Susan Lyon, Cooley LLP
- ▶ Michelle Dennedy, McAfee
- ▶ Scott Goss, Qualcomm Incorporated

**3:15 pm - 3:45 pm** Break

**3:45 pm - 5:00 pm** **Panel 4: Technology and Privacy Design**

- ▶ Deirdre Mulligan, BCLT and UC Berkeley School of Information
- ▶ Jennifer Urban, BCLT and Berkeley Law
- ▶ Jim DeGraw, Ropes & Gray LLP
- ▶ Gabriel Ramsey, Orrick, Herrington & Sutcliffe LLP

**5:00 pm - 6:00 pm** Closing Remarks by Robert Barr, BCLT Executive Director  
Reception

**TWEET WITH @BCLTATBOALT AND  
YOUR FELLOW ATTENDEES USING #BCLT**

# BCLT SPONSORS

## Partners

*Cooley LLP  
Covington & Burling LLP  
Fenwick & West LLP  
Orrick, Herrington & Sutcliffe LLP*

## Benefactors

*Fish & Richardson P.C.  
Kasowitz Benson Torres & Friedman LLP  
Kirkland & Ellis LLP  
Latham & Watkins LLP  
McDermott Will & Emery  
Morrison & Foerster LLP  
Skadden, Arps, Slate, Meagher & Flom LLP  
Weil, Gotshal & Manges LLP  
White & Case LLP  
Wilmer Cutler Pickering Hale and Dorr LLP  
Wilson, Sonsini, Goodrich & Rosati  
Winston & Strawn LLP*

## Corporate Benefactors

*Apple, Inc.  
Cisco Systems  
Google Inc.  
Microsoft Corporation  
Nokia  
RPX Corporation  
SAP  
Tessera Technologies  
Warner Bros.  
Yahoo!*

## Members

*Alston & Bird LLP  
Baker Botts LLP  
Baker & McKenzie LLP  
Bingham McCutchen LLP  
Durie Tangri LLP  
Finnegan Henderson Farabow Garrett &  
Dunner LLP  
GTC Law Group LLP & Affiliates  
Gunderson Dettmer Stough Villeneuve  
Franklin & Hachigian, LLP  
Haynes and Boone, LLP  
Hogan Lovells LLP  
Hickman Palermo Truong Becker Bingham  
Wong LLP  
Irell & Manella LLP  
Keker & Van Nest LLP  
Kilpatrick Townsend & Stockton LLP  
Knobbe Martens Olson & Bear LLP  
Morgan, Lewis & Bockius LLP  
Munger, Tolles & Olson LLP  
Ropes & Gray LLP  
Sidley Austin LLP  
Simpson Thacher & Bartlett LLP  
Turner Boyd LLP  
Van Pelt, Yi & James LLP  
Weaver Austin Villeneuve & Sampson LLP*

**THE BERKELEY LAW PRIVACY FORUM: SILICON VALLEY  
IS MADE POSSIBLE BY ALL BCLT SPONSORS**



ABSTRACT FROM A FORTHCOMING PAPER BY  
PAUL SCHWARTZ

# THE E.U.-U.S. PRIVACY COLLISION: A TURN TO INSTITUTIONS AND PROCEDURES

New conflicts in information privacy loom ahead for the US and the EU due to the Proposed Data Protection Regulation of the EU. This document, which creates directly binding law for all EU Member States, alters the current equilibrium achieved under the Data Protection Directive of 1995. The Directive stimulated a process of EU-US “lawmaking” through multi-party ad hoc networks, and led to multiple ways to accommodate the Directive’s rules for international data transfers. In contrast, the Proposed Regulation creates risks to the established processes and institutions.

In the aftermath of the Directive, ad hoc policy efforts between the US and EU have created numerous paths to “adequacy.” The policy instruments involved are the Safe Harbor; the two sets of Model Contractual Clauses; and the Binding Corporate Rules. A novel process of “lawmaking” has occurred and it has drawn on a large cast of characters, governmental and non-governmental. Building on Anu Bradford’s concept of “The Brussels Effect,” this paper argues that this policymaking has not been led exclusively by the EU, but has been a collaborative effort marked by accommodation and compromises. This resulting “lawmaking” is a productive outcome of the kinds of “harmonization networks” that Anne-Marie Slaughter has identified in her scholarship.

For the future, however, the Proposed Data Protection Regulation threatens to destabilize the current privacy policy equilibrium and prevent the kinds of decentralized global policymaking that has occurred in the past. To avert the privacy collision ahead, this paper advocates renewed attention to institutions and procedures. It also draws on lessons from policymaking under the Directive. This Article advocates a Revised Regulation that concentrates only on a limited set of non-uniform aspects of EU privacy law while also preserving future opportunities for creative global policymaking experimentation. It should do so through attention solely to the key conceptual definitions of data protection law. In addition, the Revised Regulation should not grant the Commission the power to act as a final arbiter of data protection through an ability to strike down decisions of national data protection authorities. The Revised Regulation should also limit the Commission’s power to issue further implementing and delegated acts over virtually any matter.



# PANEL I: THE EU-US PRIVACY COLLISION

## **Paul Schwartz,** *BCLT and Berkeley Law*

Paul Schwartz, Professor of Law at UC Berkeley School of Law, is a leading international expert on information privacy, copyright, telecommunications and information law. He has published widely on these topics. In the US, his articles and essays have appeared in periodicals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, Michigan Law Review, and N.Y.U. Law Review. His books include *Privacy Law Fundamentals* (2013) (co-author Daniel Solove) and *Information Privacy Law* (4th ed., 2011) (co-author Daniel Solove). Professor Schwartz has provided expert opinions, advice, and testimony to numerous governmental bodies in the United States, Canada, and Europe. He has also served as an organizer of the Privacy Law Salon, which is held annually in Miami.



## **Christopher Wolf,** *Hogan Lovells*

Christopher Wolf leads the global privacy practice at Hogan Lovells and is founder and co-chair of the Future of Privacy Forum, a think tank promoting the advancement of privacy. Chris has practiced law for 33 years, and started his focus on privacy with a pro bono case representing a gay sailor the Navy proposed to eject under Don't Ask, Don't Tell based on information it obtained illegally from AOL. Chris produced the first comprehensive privacy treatise for the Practising Law Institute, and is a frequent author and lecturer on privacy and Internet issues. He was the first privacy practitioner to testify, in January 2012, before the Privacy Subcommittee of the United States Senate Judiciary Committee, and was the only privacy lawyer to speak at the 2011 eG8 in Paris. In conjunction with Berkeley scholars Paul Schwartz and Chris Hoofnagle, and GW Professor Daniel Solove, Chris is an organizer of the Privacy Law Salon series of conferences.



## **Karl-Nikolaus Peifer,** *University of Cologne Law School*

Professor Peifer is currently Director of the Institute for Media Law and Communications Law of the University of Cologne and Director of the Institute for Broadcasting Law at the University of Cologne. He studied law, economics and romanian languages at the Universities of Trier, Bonn, Hamburg and Kiel. He held positions as a researcher at the Max-Planck-Institute for Intellectual Property Law in Munich, as an Assistant Professor in Kiel, and as a Professor in Frankfurt/Oder and Bochum. He has been a judge at the Oberlandesgericht Hamm since 2003. His main fields of research are Intellectual Property and Media Law.



## **Michael Hintze,** *Microsoft Corporation*

Michael Hintze is Chief Privacy Counsel and an Assistant General Counsel in Microsoft Corporation's Legal and Corporate Affairs (LCA) group. He joined Microsoft in 1998, and his practice currently includes a number of regulatory and public policy issues, focused on privacy and related matters worldwide. Prior to joining Microsoft, Michael was an associate with the Washington, D.C.-based law firm of Steptoe & Johnson LLP, where his practice focused on export controls, the regulation of encryption technologies and commercial matters for technology companies. Michael is a graduate of the University of Washington and the Columbia University School of Law, where he served as Editor-in-Chief of the Columbia Human Rights Law Review. He is a regular speaker on data privacy issues, and has published articles on a range of subjects including privacy, U.S. export regulations, and capital punishment.





ABSTRACT FROM A FORTHCOMING PAPER BY  
CHRIS JAY HOOFNAGLE + JAN WHITTINGTON

# THE PRICE OF FREE: ACCOUNTING FOR THE COSTS OF THE INTERNET'S MOST POPULAR PRICE

Offers of “free” services abound on the internet. These offers cause a conundrum for consumer protection. Courts are apt to discount users’ claims against such services; one recently held that users are not “consumers” for purposes of California consumer protection law. Industry leaders push to monitor users ubiquitously, an imperative driven by the desire to fund “free” content. Policymakers struggle with this imperative and weigh it against vague consumer preferences for privacy, which users seem to happily abrogate to get the next new free service. These problems, we argue, flow from attention to the price of free offers instead of their costs.

To elucidate these costs, we apply a transaction cost economic (TCE) approach to “free” transactions with personal information. TCE provides a framework for analyzing these exchanges even where the price of the product seems to be zero. “Freemium” offers employ a form of cross-subsidy, a technique widely accepted in infrastructure industries, and a basic tool used to support the equitable delivery of products and services with the understanding that some have more willingness and ability to pay than others. However, we argue that information intensive companies misuse “free” to promote products and services that are packed with non-pecuniary costs. While behavioral economics may support an outright ban of free offers because of their biasing effects, TCE suggests other strategies for reform, focused upon placing business risk more firmly in the hands of businesses. These interventions go beyond the traditional transparency and accuracy requirements suggested by privacy law. They involve eliminating the avoidable costs that arise for consumers when compelled to provide personal information in order to try a “free” product, recognizing the role consumers play in the production and business of social networking services, and requiring each third party interested in access to a consumer’s personal information to obtain opt-in per consumer through full disclosure with terms of service and privacy policies.



# PANEL 2:

## PRIVACY AND THE PRICE OF FREE

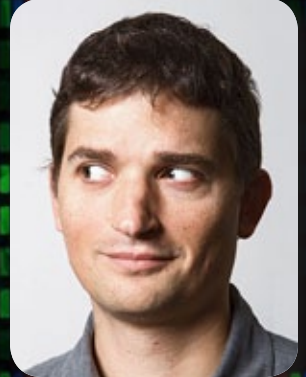
### **Chris Jay Hoofnagle**, *BCLT and Berkeley Law*

Chris Jay Hoofnagle is the director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Chris's recent work focuses on promoting competition among financial institutions to prevent identity theft. In *Identity Theft: Making the Unknown Known Known*, he discusses the problem of "synthetic identity theft," a form of crime where an impostor fabricates personal information and yet still can obtain credit accounts. Chris argues that the rise of this form of fraud demonstrates a fundamental failure in banks' anti-fraud gatekeeper function, and proposes market reforms for reducing identity theft.



### **Dalton Caldwell**, *App.Net*

Dalton is the CEO and co-founder of App.net, an ad-free social platform and API. App.net aims to be the backbone of the social web. App.net provides infrastructure developers can use to build applications and that members can use for meaningful interactions. Previously, Dalton founded the music-sharing service imeem in 2003, serving as CEO until its acquisition by MySpace in 2009. Dalton graduated with honors from Stanford University in 2003 with a B.S. in Symbolic Systems and B.A. in Psychology.



### **Michael Glaser**, *Perkins Coie LLP*

Michael Glaser is a leading Partner in the Perkins Coie's Emerging Companies practice group. Michael is also involved in firm management as a member of the firm's Executive Committee. Michael has a background in finance and is a member of the Model Document Working Group for the National Venture Capital Association (NVCA). He has led clients in the consumer e-commerce, interactive entertainment, digital media, cloud services, and premise-based software, sectors through hundreds of venture capital transactions ranging from seed stage through mezzanine financings. Michael also has an active M&A practice, and has advised clients in complex mergers and strategic business combinations ranging in size from several million dollars to several hundred million dollars. Michael works with a number of non-profit organizations including Twestival and Jamie Oliver's Food Foundation.



### **Daren Orzechowski**, *White & Case LLP*

Daren Orzechowski is a member of White & Case's Intellectual Property Group. Practicing in all areas of intellectual property law, he handles both litigation and transactional matters for clients in a variety of industries, including information technology, software, outsourcing, sports and entertainment. His practice also includes matters involving trademarks and Internet-related issues. He regularly assists clients with intellectual property enforcement and licensing and has appeared before courts and tribunals throughout the United States. In addition to multinational corporate clients, Daren works with entrepreneurs and start-up companies and is a partner in White & Case's Emerging Companies practice.





# FORUM SPONSORS

Hogan  
Lovells

ROPES  
& GRAY

## TO ACCESS THE WIRELESS NETWORK:

1. Connect to the Four Seasons Meeting Network.
2. Once you have successfully connected, open your internet browser and you will be directed to the Four Seasons "Sign-in" page. You may need to close out of your browser first or try to access a website before being re-directed.
3. In the box labeled PIN enter PRIVACY13. You do not need to fill in your last name or room number. Hit submit. You should now be connected to the wireless network.



# KEYNOTE: TRAVIS LEBLANC



**Travis LeBlanc**, *Special Assistant Attorney General, California Department of Justice*

Travis LeBlanc is Special Assistant Attorney General of California. In this capacity, he oversees the California Department of Justice's work on technology, high tech crime, privacy, antitrust, and health care issues. He also advises California Attorney General Kamala D. Harris on significant appellate and constitutional matters. He is the architect of the California mobile apps framework and the lead attorney behind the privacy case against Delta for its mobile app privacy disclosures. From 2009-2011, LeBlanc was an attorney in the U.S. Department of Justice's Office of Legal Counsel, which advises the President, Attorney General, and general counsels of executive branch agencies on the constitutionality and legality of the programs and activities of the United States government. LeBlanc previously worked at Williams & Connolly LLP in Washington, DC and Kecker & Van Nest LLP in San Francisco. LeBlanc clerked for the Hon. Stephen Reinhardt on the United States Court of Appeals for the Ninth Circuit. He has an A.B. from Princeton University, M.P.A. from the John F. Kennedy School of Government at Harvard University, J.D. from Yale Law School, and an LL.M. in International Law from the University of Cambridge.

ABSTRACT FROM A FORTHCOMING PAPER BY  
DEIRDRE MULLIGAN + KEN BAMBERGER

# THE MANAGEMENT OF PRIVACY PROCESSES: THE CPO AND BEYOND

*How should privacy be operationalized in companies?*

*What level of independence and authority do privacy officers need so that they can embed a value as complicated as privacy into a complex organization?*

*If privacy is to be delivered through designs and defaults, as well as policy, where should privacy professionals be positioned?*

*And how does the law impact these questions?*

UC Berkeley Law Professor Ken Bamberger and UC Berkeley Information Professor Deirdre Mulligan have engaged in multi-year research to investigate privacy “on the ground”—how privacy protection actually works in corporations, and the legal, social and other pressures that define the privacy requirements firms must meet—in the U.S. and Europe.

Their work has involved dozens of interviews of chief privacy officers in the U.S., Germany, France, Spain and the UK, as well as discussions with regulators, lawyers and other corporate managers.

Their comparative findings are of direct relevance to privacy lawyers, privacy professionals, and corporate managers alike, as they:

- (1) reveal an evolving set of corporate privacy best practices to which the leading firms and regulators are turning across jurisdiction;
- (2) expose the real differences—and similarities—between privacy in the US and in Europe; and
- (3) weigh in on the heated legal reform debates in Washington and Brussels, informed by evidence of what policies have proven most effective on both sides of the Atlantic.



# PANEL 3:

## THE MANAGEMENT OF PRIVACY PROCESSES: THE CPO AND BEYOND

### **Deirdre Mulligan**, *BCLT and UC Berkeley School of Information*

Deirdre K. Mulligan is an Assistant Professor at the UC Berkeley School of Information. She was previously the Director of the Samuelson Law, Technology & Public Policy Clinic and a Clinical Professor of Law at Berkeley Law. Before coming to UC Berkeley, she was staff counsel at the Center for Democracy & Technology in Washington.



### **Kenneth Bamberger**, *BCLT and Berkeley Law*

Kenneth A. Bamberger is Professor of Law at UC Berkeley, where he teaches Administrative Law, The First Amendment, and Technology and Governance. His research focuses on issues of technology and corporate regulation. In particular, Kenneth's work explores the regulation of data protection and information privacy, the use of technology by administrative agencies, and the reliance on technology in corporate compliance. With Professor Deirdre Mulligan of the UC Berkeley School of Information and BCLT, he is principal investigator on a major project comparing corporate privacy protection in the US, Canada and Europe.



### **Harriet Pearson**, *Hogan Lovells and Former Chief Privacy Officer, IBM*

Harriet Pearson has over 20 years of global business experience in all aspects of privacy, cybersecurity and technology law, policy, and compliance. Harriet was one of the first Chief Privacy Officers in the Fortune 500 and is an internationally recognized corporate privacy and data security pioneer. Her practice focuses on counseling clients on privacy and information security policy and compliance matters such as cross-border data transfers, data security incident response and remediation, and information and cybersecurity risk management and governance.



### **Susan Lyon**, *Cooley LLP*

Susan Lyon is co-chair of Cooley LLP's Privacy practice group. Susan counsels clients from small start-ups to major Internet, technology, advertising and telecommunications companies on a wide range of U.S. and international privacy and data security issues. Representative areas of expertise include CAN-SPAM, FTC Act, Children's Online Privacy Protections Act (COPPA), telemarketing laws, data security and data breach notice obligations, behavioral targeting and advertising, online and mobile tracking and monitoring using automatic tracking technology, facial recognition and biometrics, cloud computing strategy, and legislative and regulatory policy and outreach.



### **Michelle Dennedy**, *McAfee*

Michelle Finneran Dennedy currently serves as VP and Chief Privacy Officer at McAfee. She is responsible for the development and implementation of McAfee data privacy policies and practices, working across business groups to drive data privacy excellence across the security continuum. Before joining McAfee, Michelle founded The iDennedy Project and ThelDentityProject.com. Michelle was the Vice President for Security & Privacy Solutions for the Oracle Corporation and Chief Data Governance Officer within the Cloud Computing division at Sun Microsystems, Inc. Michelle also served as Sun's Chief Privacy Officer. Michelle has a JD from Fordham University School of Law and a BS degree from Ohio State University.



### **Scott Goss**, *Qualcomm Incorporated*

As Qualcomm's first attorney focusing exclusively on privacy issues, Scott leads the company's efforts in designing, creating, and operating a comprehensive, consistent, and sustainable global privacy program. Scott has established the role of the Privacy Office as a new functional area within the global corporation responsible for: Helping drive the development and enhancement of industry-leading privacy features in all of Qualcomm's products and services; Training Qualcomm attorney's, project managers and developers on privacy issues and privacy best practices; Coordinating with Government Affairs to monitor worldwide developments in both privacy-related legal and regulatory matters as well as industry best practices.



ABSTRACT FROM EXISTING AND FORTHCOMING PAPERS BY  
JENNIFER URBAN + DEIRDRE MULLIGAN

# TECHNOLOGY AND PRIVACY BY DESIGN: HELP FROM EMPIRICAL EVIDENCE

A rising tide of privacy blunders in the high tech sector is at the forefront of the search for new regulatory approaches. Many of these privacy gaffes center on the privacy implications of interactions between users, or between users and third parties--such as application developers, or embedded content providers--enabled by operating systems, mobile communications, social network sites, and other platforms.

Until recently, adherence to Fair Information Practice Principles ("FIPPs") has been viewed as the standard for protecting privacy. More recently, however, FIPPs has proven inadequate to guide the design choices of companies in a manner that regulators and the public find acceptable.

Regulators across the globe have begun to demand more of corporations. In the past, privacy has been the sole bailiwick of lawyers. Now, under the rubric of "privacy by design," policymakers are calling on the private sector to use the distinct attributes of technology to harden privacy's protection.

Exhorting companies to embed privacy into design is all well and good, but before doing so regulators would do well to ensure that the concept of privacy they direct companies to embed will afford the desirable forms of protection for privacy. And, ideally, there would be a widely used set of methods and tools to aid in translating privacy into design. Today, unfortunately, neither is true.

UC Berkeley Law Professor Jennifer Urban and UC Berkeley Information Professor Deirdre Mulligan, along with the faculty and student colleagues, have engaged in complimentary research that can inform companies' efforts to avoid privacy missteps and design privacy into technology, products and services. Drawing on quantitative and qualitative investigations of consumer perspectives on privacy, and analytic work to identify the concepts of privacy concerns animating consumer concern in high-profile privacy gaffes, as well as an analysis of the tools and methodologies available to designers, Urban and Mulligan's research provides practitioners with insight in the contextual privacy concerns of users, the multiplicity of understandings about privacy operating on the ground, and a new tool for the privacy by design tool kit.



# PANEL 4: TECHNOLOGY AND PRIVACY DESIGN

## **Deirdre Mulligan**, *BCLT and UC Berkeley School of Information*

Deirdre Mulligan is an Assistant Professor at the UC Berkeley School of Information. She was previously the Director of the Samuelson Law, Technology & Public Policy Clinic and a Clinical Professor of Law at Berkeley Law. Before coming to UC Berkeley, she was staff counsel at the Center for Democracy & Technology in Washington.



## **Jennifer Urban**, *BCLT and Berkeley Law*

Jennifer Urban joined Berkeley Law in 2009 as an Assistant Clinical Professor of Law and Director of the Samuelson Law, Technology & Public Policy Clinic at the UC Berkeley School of Law. She comes to Berkeley Law from the University of Southern California's Gould School of Law, where she founded and directed the USC Intellectual Property & Technology Law Clinic and taught classes on issues related to intellectual property, privacy and individual rights in a world of rapid technological and societal change.



## **Jim DeGraw**, *Ropes & Gray LLP*

Jim DeGraw is a corporate technology partner who works with clients to anticipate and handle the legal issues ever-changing technologies present. He regularly leads transactions for which technology or IP assets are key drivers, provides clients with strategic advice on protecting and maximizing their investments in technology, and advises clients on handling and securing the data their businesses collect and process. Jim brings to any representation his computer science background and his experience of having spent years working for firm clients on technology matters while based in Asia.



## **Gabriel Ramsey**, *Orrick, Herrington & Sutcliffe LLP*

Gabriel Ramsey, a partner in the Silicon Valley office, a member of the Intellectual Property Group and a leader of the Entertainment and Gaming Group and the Internet Safety, Security and Privacy Group, focuses his practice on intellectual property litigation. In 2012, Gabriel was named one of the top 75 IP litigators in California by The Daily Journal. He has substantial experience in high technology- and entertainment-related matters involving copyright, trademark, trade secret and patent law. He has significant experience in carrying out Internet enforcement actions involving cybercrime, fraud and deceptive activity, brand violations, intellectual property infringement and privacy breaches. He also has handled many licensing matters and general commercial disputes.








Our privacy and cybersecurity lawyers are  
available in the Bay Area and around the world.  
Global coverage for global issues.

Ranked in the top tier by *Chambers Global* 2013

2,300 lawyers. 40+ offices. 22 countries. **[www.hoganlovells.com](http://www.hoganlovells.com)**





# ROPES & GRAY PROUDLY SUPPORTS THE BERKELEY CENTER FOR LAW AND TECHNOLOGY AND ITS 2ND ANNUAL PRIVACY LAW FORUM: SILICON VALLEY.

Offering a privacy and data security team recently named a “2012 Practice Group of the Year” by *Law360*, Ropes & Gray LLP is ranked by *Chambers USA 2012* and *Chambers Global 2012* as a leading “Privacy & Data Security Firm.”

Our privacy and data security team includes corporate lawyers, litigators and counselors who work together to help clients navigate complex and changing laws and expectations.

## ROPES & GRAY

BOSTON CHICAGO HONG KONG LONDON  
NEW YORK SAN FRANCISCO SEOUL SHANGHAI  
SILICON VALLEY TOKYO WASHINGTON, D.C.

[www.ropesgray.com](http://www.ropesgray.com)







Program Design by Kyle Halvorson  
[kylejhalvorson@gmail.com](mailto:kylejhalvorson@gmail.com)

