# Privacy Papers for Policy Makers

## 2013

The publication of "Privacy Papers for Policy Makers" was supported by AT&T, Microsoft, and GMAC.




January 1st, 2014

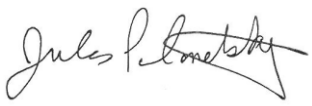
We are delighted to provide you with FPF's fourth annual "Privacy Papers for Policy Makers," representing cutting-edge research and analytical work on a variety of important privacy topics.

The featured papers analyze current and emerging privacy issues and propose solutions or offer free analysis that could lead to new approaches in privacy law. Academics, privacy advocates and Chief Privacy Officers on FPF's Advisory Board reviewed all submitted papers, emphasizing clarify, practicality and overall utility as the most important criteria for selection. We received many excellent submissions from scholars on both sides of the Atlantic, and we believe our Advisory Board has chosen a diverse and thought-provoking collection of papers. Additionally, two of the papers were recipients of the IAPP award for best papers presented at the 2013 Privacy Law Scholars Conference.

We hope this relevant and timely scholarship helps inform policy makers in Congress, at the FTC, and in other federal and state agencies as the address privacy issues. This compilation is also being provided to policy makers abroad.

We want to thank AT&T, Microsoft and GMAC for their special support of this project. And thank you for your interest in exploring new ways to think about privacy.

Sincerely yours,



Christopher Wolf
Founder and Co-Chair

Jules Polonetsky
Executive Director and Co-Chair

# Future of Privacy Forum Advisory Board

**Alessandro Acquisti**
Associate Professor of Information Technology and Public Policy at the Heinz College, Carnegie Mellon University

**Ellen Agress**
Senior Vice President and Deputy General Counsel, News Corporation

**Annie I. Antón**
Professor and Chair, Georgia Tech School of Interactive Computing

**Jonathan Avila**
Chief Privacy Officer
Walmart

**Stephen Balkam**
Chief Executive Officer,
Family Online Safety Institute

**Kenneth A. Bamberger**
Professor of Law, Berkeley School of Law

**Lael Bellamy**
Chief Privacy Officer, The Weather Channel

**Elise Berkower**
Associate General Counsel, Privacy,
The Nielsen Company

**Debra Berlyn**
President, Consumer Policy Solutions

**Joan (Jodie) Z. Bernstein**
Counsel, Kelley Drye & Warren, LLP and former director of the Bureau of Consumer Protection at the Federal Trade Commission

**Michael Blum**
General Counsel, Quantcast

**Bruce Boyden**
Assistant Professor of Law, Marquette University Law School

**Allen Brandt**
Corporate Counsel, Data Privacy & Protection, Graduate Management Admission Council (GMAC)

**Justin Brookman**
Director, Consumer Privacy, Center for Democracy & Technology

**Stuart N. Brotman**
Stuart N. Brotman Communications

**J. Beckwith Burr**
Deputy General Counsel and Chief Privacy Officer, Neustar

**James M. Byrne**
Chief Privacy Officer, Lockheed Martin Corporation

**Ryan Calo**
Assistant Professor, University of Washington School of Law
Affiliate Scholar, Stanford Center for Internet and Society

**Anna-Lisa Corrales**
General Counsel and Secretary
Jaguar Land Rover North America, LLC
Jaguar Land Rover Canada ULC

**Dr. Ann Cavoukian**
Information and Privacy Commissioner of Ontario

**Brian Chase**
General Counsel, Foursquare Labs, Inc.

**Danielle Citron**
Professor of Law, University of Maryland Law School

**Allison Cohen**
Managing Counsel, Toyota

**Maureen Cooney**
Head of Privacy, Sprint

**Lorrie Faith Cranor**
Associate Professor of Computer Science and Engineering,
Carnegie Mellon University

**Mary Culnan**
Professor Emeritus, Bentley University

**Simon Davies**
Founder, Privacy International

**Kim Dawson**
Senior Director of Privacy,
Nordstrom, Inc.

**Michelle De Mooy**
Senior Associate, National Priorities,
Consumer Action

**Elizabeth Denham**
Information and Privacy Commissioner for British Columbia

**Michelle Dennedy**
Chief Privacy Officer, McAfee, Inc.

**Benjamin Edelman**
Assistant Professor, Harvard Business School

**Erin Egan**
Chief Privacy Officer, Policy, Facebook

**Keith Enright**
Senior Corporate Counsel, Google

**Leigh Feldman**
Chief Privacy Counsel, American Express

**Alex Fowler**
Global Privacy & Public Policy Lead, Mozilla

**Eric Friedberg**
Co-President, Stroz Friedberg

**Christine Frye**
Senior Vice President, Chief Privacy Officer, Bank of America

**Arkadi Gerney**
Senior Fellow
Center for American Progress

**Julie Gibson**
Global Privacy Program Leader
The Procter & Gamble Company

**Jennifer Barrett Glasgow**
Chief Privacy Officer
Acxiom

**Scott Goss**
Senior Privacy Counsel, Qualcomm

**Kimberly Gray**
Chief Privacy Officer, IMS Health

**Sean Hanley**
Director of Compliance, Zynga Game Network, Inc.

**Pamela Jones Harbour**
Former Federal Trade Commissioner;
Partner,Fulbright & Jaworski LLP

**Woodrow Hartzog**
Assistant Professor
Cumberland School of Law, Samford University and Affiliate Scholar, The Center for Internet & Society at Stanford Law School

**Eric Heath**
Director of Legal – Global Privacy,
LinkedIn

**Rita S. Heimes**
Clinical Professor and Director, Center for Law and Innovation, University of Maine School of Law

**Megan Hertzler**
Director of Information Governance, Xcel Energy

**Michael Ho**
Chief Executive Officer, Bering Media

**David Hoffman**
Director of Security Policy and Global Privacy Officer, Intel

**Lara Kehoe Hoffman**
Privacy and Data Security Counsel, Autodesk

**Marcia Hoffman**
Staff Attorney, Electronic Frontier Foundation

**Chris Hoofnagle**
Director, Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic

**Jane Horvath**
Director of Global Privacy, Apple, Inc.

**Sandra R. Hughes**
Chief Executive Officer and President,
Sandra Hughes Strategies, Ltd.

**Brian Huseman**
Director, Public Policy, Amazon

# Future of Privacy Forum Advisory Board (continued)

**Jeff Jarvis**
Associate Professor; Director of the Interactive Program, Director of the Tow-Knight Center for Entrepreneurial Journalism at the City University of New York

**David Kahan**
General Counsel, Jumptap

**Ian Kerr**
Canada Research Chair in Ethics, Law & Technology,
University of Ottawa, Faculty of Law

**Bill Kerrigan**
Chief Executive Officer, Abine, Inc.

**Stephen Kline**
Senior Counsel, Privacy and Regulatory Matters, Omnicom Media Group

**Anne Klinefelter**
Associate Professor of Law, Director of the Law Library, University of North Carolina

**Fernando Laguarda**
Vice President, External Affairs and Policy Counselor, Time Warner Cable

**Barbara Lawler**
Chief Privacy Officer, Intuit

**Adam Lehman**
Chief Operating Officer and General Manager, Lotame Solutions

**Gerard Lewis**
Senior Counsel and Chief Privacy Officer, Comcast

**Chris Libertelli**
Head of Global Public Policy, Netflix

**Harry Lightsey**
Executive Director, Federal Affairs, General Motors

**Chris Lin**
Executive Vice President, General Counsel and Chief Privacy Officer, comScore, Inc.

**Brendon Lynch**
Chief Privacy Officer, Microsoft

**Mark MacCarthy**
Vice President of Public Policy, The Software & Information Industry Association

**Larry Magid**
Co-Founder and Co-Director, Connect Safely

**Wendy Mantel**
Privacy & IP Counsel
Hulu

**Debbie Matties**
Vice President, Privacy, CTIA-The Wireless Association

**Michael McCullough**
Vice President, Enterprise Information Management and Privacy, Macy's Inc.

**William McGeveran**
Associate Professor, University of Minnesota Law School

**Terry McQuay**
President, Nymity, Inc.

**Scott Meyer**
Chief Executive Officer, Evidon

**Doug Miller**
Global Privacy Leader, AOL, Inc.

**Maggie Mobley**
General Counsel and Chief Privacy Officer, Carrier IQ

**Marcus Morissette**
Privacy Counsel, eBay

**Saira Nayak**
Director of Policy, TRUSTe

**Jill Nissen**
Principal and Founder, Nissen Consulting

**Lina Ornelas**
General Director for Privacy Self-Regulation, Federal Institute for Access to Information and Data Protection Mexico

**Kimberley Overs**
Assistant General Counsel, Pfizer, Inc.

**Harriet Pearson**
Partner, Hogan Lovells US, LLP

**Christina Peters**
Senior Counsel, Security and Privacy, IBM

**Robert Quinn**
Chief Privacy Officer and Senior Vice President for Federal Regulatory, AT&T

**MeMe Rasmussen**
VP, Chief Privacy Officer, Associate General Counsel, Adobe Systems

**Katie Ratté**
Executive Counsel, Privacy Policy and Strategy, The Walt Disney Company

**Joel R. Reidenberg**
Professor of Law, Fordham University School of Law

**Neil Richards**
Professor of Law, Washington University Law School

**Shirley Rooker**
President, Call for Action

**Mike Sands**
President and Chief Executive Officer, BrightTag

**Patrick Sayler**
Chief Executive Officer
Gigya, Inc.

**Russell Schrader**
Chief Privacy Officer and Associate General Counsel – Global Enterprise Risk, Visa, Inc.

**Paul Schwartz**
Professor of Law, University of California-Berkeley School of Law

**Evan Selinger, Ph.D.**
Associated Professor, Philosophy Department, Rochester Institute of Technology (RIT); MAGIC Center Head of Research Communications, Community & Ethics, RIT Fellow, Institute for Ethics and Emerging Technology

**Ho Shin**
General Counsel, Millennial Media

**Meredith Sidewater**
Senior Vice President and General Counsel, Lexis Nexis Risk Solutions

**Al Silipigni**
Senior Vice President, Chief Privacy Officer, HSBC

**Dale Skivington**
Chief Privacy Officer, Dell

**Will Smith**
Chief Executive Officer, Euclid, Inc.

**Daniel Solove**
Professor of Law, George Washington University Law School

**Cindy Southworth**
Vice President of Development & Innovation, National Network to End Domestic Violence (NNEDV)

**JoAnn Stonier**
SVP and Global Privacy & Data Protection Officer, MasterCard, Inc.

**Lior Jacob Strahilevitz**
Sidley Austin Professor of Law, University of Chicago Law School

**Greg Stuart**
Chief Executive Officer, Mobile Marketing Association

**Chris Sundermeier**
General Counsel, Chief Privacy Officer, Reputation.com

**Peter Swire**
Nancy J. & Lawrence P. Huang Professor, Scheller College of Business, Georgia Institute of Technology

**Omer Tene**
Associate Professor, College of Management School of Law,
Rishon Le Zion, Israel

**Adam Thierer**
Senior Research Fellow, Mercatus Center, George Mason University

**Anne Toth**
Trustworks Privacy Advisors

# Future of Privacy Forum Advisory Board (continued)

**Catherine Tucker**
Mark Hyman, Jr. Career Development Professor and Associate Professor of Management Science, Sloan School of Management, MIT

**David C. Vladeck**
Professor, Georgetown University, Former Director of the Bureau of Consumer Protection, Federal Trade Commission (FTC)

**Hilary Wandall**
Chief Privacy Officer, Merck & Co., Inc.

**Daniel J. Weitzner**
Co-Director, MIT CSAIL Decentralized Information Group; W3C Technology and Society Policy Director; Former Deputy Chief Technology Officer, The White House Office of Science and Technology Policy

**Yael Weinman**
Vice President, Global Privacy and General Counsel, Information Technology Industry Council

**Robert Yonaitis**
Senior Vice President of Engineering and Chief Research Scientist, Ave Point, Inc.

**Karen Zacharia**
Chief Privacy Officer, Verizon Communications, Inc.

**Michael Zimmer**
Assistant Professor in the School of Information Studies, University of Wisconsin-Milwaukee

**Oracle**

**United Health Group**

**Yahoo!**

(As of December 31, 2013)

# Table of Contents



*Recipients of the IAPP award for best papers at the 2013 Privacy Law Scholars Conference

# Digital Market Manipulation

M. Ryan Calo

Forthcoming in the *George Washington Law Review*.
Full paper available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703

**Executive Summary:**

Jon Hanson and Douglas Kysar coined the term "market manipulation" in 1999 to describe how companies exploit the cognitive limitations of consumers. Everything costs $9.99 because consumers see the price as closer to $9 than $10. Although widely cited by academics, the concept of market manipulation has had only a modest impact on consumer protection law.

This Article demonstrates that the concept of market manipulation is descriptively and theoretically incomplete, and updates the framework for the realities of a marketplace that is mediated by technology. Today's firms fastidiously study consumers and, increasingly, personalize every aspect of their experience. They can also reach consumers anytime and anywhere, rather than waiting for the consumer to approach the marketplace. These and related trends mean that firms can not only take advantage of a general understanding of cognitive limitations, but can uncover and even trigger consumer frailty at an individual level.

A new theory of *digital* market manipulation reveals the limits of consumer protection law and exposes concrete economic and privacy harms that regulators will be hard-pressed to ignore. This Article thus both meaningfully advances the behavioral law and economics literature and harnesses that literature to explore and address an impending sea change in the way firms use data to persuade.

**Author:**

**M. Ryan Calo** is an assistant professor at the University of Washington School of Law and an affiliate scholar at the Stanford Law School Center for Internet and Society. He is a co-director of the University of Washington's Tech Policy Lab. Calo researches the intersection of law and emerging technology, with an emphasis on privacy and robotics. His work on these and other topics has appeared in law reviews and major news outlets, including the New York Times, the Wall Street Journal, and NPR. In 2013, Professor Calo testified before the full Judiciary Committee of the United States Senate regarding the domestic use of drones. Professor Calo serves on numerous advisory boards, including the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), the Future of Privacy Forum, and National Robotics Week. Professor Calo co-chairs the Robotics and Artificial Intelligence committee of the American Bar Association and is a member of the Executive Committee of the American Association of Law Schools (AALS) Section on Internet and Computer Law.

# Facing Real-Time Identification in Mobile Apps & Wearable Computers

Yana Welinder

Forthcoming in the *Santa Clara Computer and High Technology Law Journal*.
Full paper available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280968

**Executive Summary:**

This article explores the privacy implications of face recognition technology in mobile applications and wearable computers and provides recommendations for developing policy with respect to these uses. Face recognition apps in portable devices challenge individuals' ability to remain anonymous in public places. They can also link individuals' offline activities to their online profiles, generating a digital paper trail of their every move. The apps can therefore interfere with the ability to go off the radar, which is often considered essential for quiet reflection and daring experimentation - processes that are critical for a productive and democratic society. So given what we stand to lose, we ought to be cautious with groundbreaking technological progress. It does not mean that we have to move any slower, but we should think about potential consequences of the steps that we take.

This article maps out the recently launched face recognition apps and still developing wearable computing technologies, as well as some emerging regulatory responses. Based on these developments, it offers initial considerations for better policy responses to these uses. The article recommends solutions that focus on how the relevant individuals could be put on notice given that the apps will not only be using information about their users, but also about the persons being identified. It further recommends minimization of data collection and retention and discusses how biometric data can be kept secure. Today's face recognition apps mostly use photos from social networks. They therefore call for regulatory responses that consider the context in which users originally shared the photos. Most importantly, the article highlights that the Federal Trade Commission's first policy response to consumer applications that use face recognition did not follow the well-established principle of technology neutrality. The article argues that any regulation with respect to identification in real time should be technology neutral and narrowly address harmful uses of computer vision without hampering the development of useful applications.

**Author:**

**Yana Welinder** is a Legal Counsel at the Wikimedia Foundation and a Junior Affiliate Scholar at the Stanford Center for Internet & Society. Before joining Wikimedia, she was a Visiting Assistant Professor at California Western School of Law, where she taught Information Privacy Law and E-Commerce Law. Her research focuses on internet law, privacy, and intellectual property. She also works with net neutrality policy as a member to the UN Internet Governance Forum Dynamic Coalition on Net Neutrality. Yana has previously served as a Google Policy Fellow at the Electronic Frontier Foundation

and conducted research on the representation of privacy through user interface design as a fellow at Harvard Law School. She holds an LL.M. from Harvard Law School, a J.D. from University of Southern California, and an LL.B. from the London School of Economics and Political Science.

# A Framework for Benefit-Cost Analysis in Digital Privacy Debates

Adam Thierer

Published in *The George Mason Law Review*. Full paper available at:
http://www.georgemasonlawreview.org/doc/Thierer_Website.pdf

**Executive Summary:**

Policy debates surrounding online child safety and digital privacy share much in common. Both are complicated by thorny definitional disputes and highly subjective valuations of "harm." Both issues can be subject to intense cultural overreactions, or "technopanics." It is common to hear demands for technical quick fixes or silver bullet solutions that are simple yet sophisticated. In both cases, the purpose of regulation is some form of information control. Preventing exposure to objectionable content or communications is the primary goal of online safety regulation, whereas preventing the release of personal information is typically the goal of online privacy regulation. The common response is regulation of business practices or default service settings.

Once we recognize that online child safety and digital privacy concerns are linked by many similar factors, we can consider whether common solutions exist. Many of the solutions proposed to enhance online safety and privacy are regulatory in character. But information regulation is not a costless exercise. It entails both economic and social costs. Measuring those costs is an extraordinarily complicated and contentious matter, since both online child safety and digital privacy are riddled with emotional appeals and highly subjective assertions of harm.

This Article will make a seemingly contradictory argument: benefit-cost analysis ("BCA") is extremely challenging in online child safety and digital privacy debates, yet it remains essential that analysts and policy-makers attempt to conduct such reviews. While we will never be able to perfectly determine either the benefits or costs of online safety or privacy controls, the very act of conducting a regulatory impact analysis ("RIA") will help us to better understand the trade-offs associated with various regulatory proposals. However, precisely because those benefits and costs re-main so remarkably subjective and contentious, this Article will argue that we should look to employ less restrictive solutions—education and aware-ness efforts, empowerment tools, alternative enforcement mechanisms, etc.—before resorting to potentially costly and cumbersome legal and regulatory regimes that could disrupt the digital economy and the efficient pro-vision of services that consumers desire. This model has worked fairly effectively in the online safety context and can be applied to digital privacy concerns as well.

This Article focuses primarily on digital privacy policy and sketches out a framework for applying BCA to proposals aimed at limiting commercial online data collection, aggregation, and use. Information about online users is regularly collected by online operators to tailor advertising to them (so-called "targeted" or "behavioral" advertising), to offer them expanded functionality, or to provide them with additional service options. Such operators include social networking services, online search and e-mail providers, online advertisers, and other digital content

providers. While this produces many benefits for consumers—namely, a broad and growing diversity of online content and services for little or no charge—it also raises privacy concerns and results in calls for regulatory limitations on commercial data collection or reuse of personal information.

This Article does not focus on assertions of privacy rights against government, however. The benefit-cost calculus is clearly different when state actors, as opposed to private actors, are the focus of regulation. Governments have unique powers and responsibilities that qualify them for a different type of scrutiny.

To offer a more concrete example of how privacy-related BCA should work in practice, the recent actions of the Obama administration and the Federal Trade Commission ("FTC") are considered throughout the Article. The Obama administration has been remarkably active on commercial privacy issues over the past three years yet has largely failed to adequately consider the full range of costs associated with increased government activity on this front. It has also failed to conclusively show that any sort of market failure exists as it relates to commercial data collection or targeted online advertising or services.

At a minimum, this Article will make it clear why independent agencies should be required to carry out BCA of any privacy-related policies they are considering. Currently, many agencies, including the FTC and the Federal Communications Commission ("FCC"), are not required to conduct BCA or have their rulemaking activities approved by the White House Office of Information and Regulatory Affairs ("OIRA"), which oversees federal regulations issued by executive agencies. Regulatory impact analysis is important even if there are problems in defining, quantifying, and monetizing benefits—as is certainly the case for commercial online privacy concerns.

In Part I, this Article examines the use of BCA by federal agencies to assess the utility of government regulations. Part II considers how BCA can be applied to online privacy regulation and the challenges federal officials face when determining the potential benefits of regulation. Part III then elaborates on the cost considerations and other trade-offs that regulators face when evaluating the impact of privacy-related regulations. In Part IV, this Article will discuss alternative measures that can be taken by government regulators when attempting to address online safety and privacy concerns. This Article concludes that policymakers must consider BCA when proposing new rules but also recognize the utility of alternative remedies, such as education and awareness campaigns, to address consumer concerns about online safety and privacy.

**Author:**

**Adam Thierer** is a senior research fellow with the Technology Policy Program at the Mercatus Center at George Mason University. He specializes in technology, media, Internet, and free-speech policies, with a particular focus on online child safety and digital privacy. His writings have appeared in the Wall Street Journal, the Economist, the Washington Post, the Atlantic, and Forbes, and he has appeared

on national television and radio. Thierer is a frequent guest lecturer and has testified numerous times on Capitol Hill.

Thierer has authored or edited seven books on topics ranging from media regulation and child safety to the role of federalism in high-technology markets. He contributes to the Technology Liberation Front, a leading technology-policy blog. Thierer has served on several distinguished online-safety task forces, including Harvard University Law School's Internet Safety Technical Task Force. Previously, Thierer was president of the Progress and Freedom Foundation, director of telecommunications studies at the Cato Institute, and a senior fellow at the Heritage Foundation.

Thierer received his MA in international business management and trade theory at the University of Maryland and his BA in journalism and political philosophy from Indiana University.

# The FTC and the New Common Law of Privacy

Daniel J. Solove & Woodrow Hartzog

Forthcoming in the *Columbia Law Review*.
Full paper available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913

**Executive Summary:**

One of the great ironies about information privacy law is that the primary regulation of privacy in the United States has barely been studied in a scholarly way. Since the late 1990s, the Federal Trade Commission (FTC) has been enforcing companies' privacy policies through, among other things, its authority to police unfair and deceptive trade practices.

Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. Nevertheless, companies look to these agreements to guide their decisions regarding privacy practices. In practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States – more so than nearly any privacy statute and any common law tort. It is therefore quite surprising that so little scholarly attention has been devoted to the FTC's privacy jurisprudence.

In this Article, we endeavor to map this uncharted terrain. We explore how and why the FTC, and not contract law, came to dominate the enforcement of privacy policies. In the late 1990s, it was far from clear that the body of law regulating privacy policies would come from the FTC and not from traditional contract and promissory estoppel. We seek to understand why the FTC jurisprudence developed the way that it did and how it might develop in the future. We contend that the FTC's privacy jurisprudence is the functional equivalent to a body of common law, and we examine it as such.

Our primary thesis is that through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information. This jurisprudence has the foundations to grow even more robust. By clarifying its standards and looking beyond a company's privacy promises, the FTC is poised to enforce a holistic and robust privacy regulatory regime that draws upon industry standards and consumer expectations of privacy to remain potent, feasible, and adaptable in the face of technological change.

**Authors:**

**Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also Senior Policy Advisor at Hogan Lovells. Additionally, he is the founder of TeachPrivacy, a company that provides privacy and security training.

# The FTC and the New Common Law of Privacy

One of the world's leading experts in privacy law, Solove is the author of numerous books, including *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale 2011), *Privacy Law Fundamentals* (IAPP 2011),*Understanding Privacy* (Harvard 2008), and *The Future of Reputation: Gossip and Rumor in the Information Age* (Yale 2007). Additionally, he is also the author of a textbook, *Information Privacy Law*, as well as more than 40 articles. Solove has testified before Congress and has consulted in a number of high-profile privacy cases.

**Woodrow Hartzog** is an Assistant Professor at the Cumberland School of Law at Samford University. He is also an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research focuses on privacy, human-computer interaction, contracts, and robotics. His work has been or is scheduled to be published in numerous scholarly publications such as the *Columbia Law Review, California Law Review*, and *Michigan Law Review* and popular publications such as *The Atlantic* and *The Nation*. He has been quoted or referenced in numerous articles and broadcasts, including *NPR, the New York Times, the Los Angeles Times, USA Today,* and *Bloomberg*. He previously worked as a trademark attorney at the United States Patent and Trademark Office and in private practice. He has also served as a clerk for the Electronic Privacy Information Center.

# Information Privacy in the Cloud

Paul M. Schwartz

Published in the *University of Pennsylvania Law Review*. Full paper available at: http://www.pennlawreview.com/print/?id=402

**Executive Summary:**

Cloud computing is the locating of computing resources on the Internet in a fashion that makes them highly dynamic and scalable. Moreover, cloud computing permits dramatic flexibility in processing decisions—and on a global basis. The rise of the cloud has also significantly challenged established legal paradigms. This Article analyzes current shortcomings of information privacy law in the context of the cloud. It develops normative proposals to allow the cloud to become a central part of the evolving Internet. These proposals rest on strong and effective protections for information privacy that are sensitive to technological changes.

This Article examines three areas of change in personal data processing due to the cloud. The first area of change concerns the nature of information processing at companies. For many organizations, data transmissions are no longer point-to-point transactions within one country; they are now increasingly international in nature. As a result of this development, the legal distinction between national and international data processing is less meaningful than in the past. The jurisdictional concepts of EU law do not fit well with these changes in the scale and nature of international data processing. This Article proposes modifications to the applicable EU jurisdictional law and, in particular, the sweeping rules of the Proposed Draft Regulation.

A second legal issue concerns the multi-directional nature of modern data flows, which occur today as a networked series of processes made to deliver a business result. Due to this development, established concepts of privacy law, such as the definition of "personal information" and the meaning of "automated processing" have become problematic. There is also no international harmonization of these concepts. As a result, European Union and U.S. officials may differ on whether certain cloud-based activities implicate the restrictions and regulations of privacy law. This Article applies the authors' tiered conception of personally identifiable information—"PII 2.0"—to create incentives for cloud companies to maintain information in an indentifiable or even nonidentifiable form and thus begin harmonizing the U.S. and EU approaches to PII.

A final change relates to a shift to a process-oriented management approach. Users no longer need to own technology, whether software or hardware, that is placed in the cloud. Rather, different parties in the cloud can contribute inputs and outputs and execute other kinds of actions. In short, technology has provided new answers to a question that Ronald Coase first posed in "The Nature of the Firm." New technologies and accompanying business models now allow firms to approach Coasian "make or buy" decisions in innovative ways. Yet, privacy law's approach to liability for privacy violations and data losses in the new "make or buy" world of the cloud may not create adequate incentives for the multiple parties who handle personal data. This Article explores the need for a model contract privacy law that would provide a core baseline of protections in business-to-consumer arrangements.

# Information Privacy in the Cloud

**Author:**

**Paul Schwartz** is a leading international expert on information privacy law. He is a professor at the University of California, Berkeley Law School and a director of the Berkeley Center for Law and Technology. He has testified before Congress and served as an advisor to international organizations, including Directorate Generals of the European Union. He assists numerous corporations and organizations with regulatory, policy and governance issues relating to information privacy. Schwartz is a frequent speaker at technology conferences and corporate events in the United States and abroad. He is a Special Advisor to the privacy and data security practice of Paul Hastings LLP.

Professor Schwarz is the author of many books, including the leading casebook, "Information Privacy Law," and the distilled guide, "Privacy Law Fundamentals," each with Daniel Solove. "Information Privacy Law," now in its fourth edition, is used in courses at more than 20 law schools. Schwartz's over fifty articles have appeared in journals such as the *Harvard Law Review, Yale Law Journal, Stanford Law Review*, *University of Chicago Law Review* and *California Law Review*. He publishes on a wide array of privacy and technology topics including data analytics, cloud computing, telecommunications surveillance, data security breaches, health care privacy, privacy governance, data mining, financial privacy, European data privacy law, and comparative privacy law.

# Obscurity by Design

Woodrow Hartzog & Frederic D. Stutzman

Published in the *Washington Law Review*. Full paper available at:
http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1247/88WLR385.pdf?sequence=1

**Executive Summary:**

Design-based solutions to confront technological privacy threats are becoming popular with regulators. One popular design solution, "Privacy by Design," has been described as "the philosophy and approach of embedding privacy into the design specifications of various technologies." However, these promising solutions have left the full potential of design untapped. With respect to online communication technologies, design-based solutions for privacy remain incomplete because they have yet to successfully address the trickiest aspect of the Internet—social interaction. This Article posits that privacy-protection strategies such as "Privacy by Design" face unique challenges with regard to social software and social technology due to their interactional nature.

This Article proposes that design-based solutions for social technologies benefit from increased attention to user interaction, with a focus on the principles of "obscurity" rather than the expansive and vague concept of "privacy." The main thesis of this Article is that obscurity is the optimal protection for most online social interactions and, as such, is a natural locus for design-based privacy solutions for social technologies. To that end, this Article develops a model of "obscurity by design" as a means to address the privacy problems inherent in social technologies and the Internet.

Where the pursuit of "privacy" in design often seems like a quest for near-perfect protection, the goal of designing for obscurity is that it be "good enough" for most contexts or to accommodate a user's specific needs. As the natural state for many online social communications, obscurity is the logical locus for the front end design of social technologies. Obscurity by design utilizes the full potential of design-based solutions to protect privacy and serve as a roadmap for organizations and regulators who seek to confront the vexing problems and contradictions inherent in social technologies.

**Authors:**

**Woodrow Hartzog** is an Assistant Professor at the Cumberland School of Law at Samford University. He is also an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research focuses on privacy, human-computer interaction, contracts, and robotics. His work has been or is scheduled to be published in numerous scholarly publications such as the *Columbia Law Review, California Law Review*, and *Michigan Law Review* and popular publications such as *The Atlantic* and *The Nation*. He has been quoted or referenced in numerous articles and broadcasts, including *NPR, the New York Times, the Los Angeles Times, USA Today,* and *Bloomberg*. He previously worked as a trademark attorney at the United States Patent and Trademark Office and in private practice.

He has also served as a clerk for the Electronic Privacy Information Center.

**Fred Stutzman** is founder of Eighty Percent Solutions, a LAUNCH Incubator company which builds the innovative productivity software Freedom and Anti-Social. Previously, he was co-founder of ClaimID.com and technology researcher at UNC-Chapel Hill and Carnegie Mellon University. He holds a Ph.D. in Information Science, a graduate certificate in quantitative research, and a B.A. in Economics. Currently, he is adjunct professor at UNC's School of Information and Library Science, where he teaches courses about privacy and social media.

# A Primer on Metadata: Separating Fact from Fiction

Ann Cavoukian

Full paper available at:
http://www.realprivacy.ca/index.php/paper/primer-metadata-separating-fact-fiction/

**Executive Summary:**

Since the June 2013 revelations of the NSA's sweeping surveillance of the public's metadata, the term "metadata" has been regularly used in the media, frequently without any explanation of its meaning. In an effort to educate the public and draw importance to this issue, Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, set out in this paper to provide a clear understanding of metadata and how revealing its content can be.

Metadata's reach can be extensive – including information that reveals the time and duration of a communication, the particular devices used, email addresses, numbers contacted, which kinds of communications services were used, and at what geolocations. And since virtually every device we use has a unique identifying number, our communications and Internet activities may be linked and traced with relative ease, ultimately back to the individuals involved.

All this metadata is collected and retained by communications service providers for varying periods of time and, for legitimate business purposes. Key questions arise, however, including who else may have access to all this information, and for what purposes? Senior U.S. government officials have been defending their sweeping and systemic seizure of the public's communications data on the basis that it is "only metadata." They say it is neither sensitive nor privacy-invasive since it does not access the actual content contained in the associated communications.

*A Primer on Metadata: Separating Fact from Fiction*, explains that metadata can be far more revealing than accessing the content of our communications. The paper disputes popular claims that the information being captured is neither sensitive, nor privacy-invasive, since it does not access any content. Given the implications for privacy and freedom, it is critical that we all question the dated but ever-so prevalent either/or, zero-sum mindset of privacy vs. security. Instead, what is needed are proactive measures designed to provide for both security and privacy, in an accountable and transparent manner.

In this globally networked age, privacy knows no bounds – it is no longer simply a local issue – it transcends borders, demanding global attention. Accordingly, we urge governments to adopt a proactive approach to securing the rights affected by intrusive surveillance programs. To protect privacy and liberty, any power to seize communications metadata must come with strong safeguards directly embedded into programs and technologies,that are clearly expressed in the governing legal framework. More robust judicial oversight, parliamentary or congressional controls, and systems capable of providing for effective public accountability should be brought to bear. The need for operational secrecy must not stand in the way of public accountability. Our essential need for privacy and the preservation of our freedom and liberty are at stake.

# A Primer on Metadata: Separating Fact from Fiction

**Author:**

**Ann Cavoukian**, Ph.D., Information and Privacy Commissioner, Ontario, Canada.

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to proactively embed privacy into the design specifications of information technology and accountable business practices, thereby achieving the strongest protection possible. In October, 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection. This was followed by the U.S. Federal Trade Commission's inclusion of *Privacy by Design* as one of its three recommended practices for protecting online privacy – a major validation of its significance. This was later followed by the inclusion of *Privacy by Design* in the draft EU Data Protection Regulation.

An avowed believer in the role that technology can play in the protection of privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected globally. She has been involved in numerous international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening consumer confidence and trust in emerging technology applications.

Dr. Cavoukian serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. She is also a member of several Boards including, the *European Biometrics Forum, Future of Privacy Forum,* RIM Council, and has been conferred as a Distinguished Fellow of the Ponemon Institute. Dr. Cavoukian was honoured with the prestigious *Kristian Beckman Award* in 2011 for her pioneering work on *Privacy by Design* and privacy protection in modern international environments. In the same year, Dr. Cavoukian was also named by *Intelligent Utility* Magazine as one of the Top 11 Movers and Shakers for the Global Smart Grid industry, received the SC Canada Privacy Professional of the Year Award and was honoured by the University of Alberta for her positive contribution to the field of privacy.

# Privacy in Europe: Initial Data on Governance Choices and Corporate Practice

Kenneth Bamberger & Deirdre Mulligan

Paper published in the *George Washington Law Review*. Full paper available at: http://www.gwlr.org/2013/09/14/bamberger_mulligan/

**Executive Summary:**

As this Article goes to press, the European Union is embroiled in debates over the contours of a proposed new privacy regulation. These efforts, however, have lacked critical information necessary for reform. For, like privacy debates generally, they focus almost entirely on law "on the books"—legal texts enacted by legislatures or promulgated by agencies.

By contrast, they largely ignore privacy "on the ground"—the ways in which corporations in different countries have operationalized privacy protection in the light of divergent formal laws, different approaches taken by local administrative agencies, and other jurisdiction-specific social, cultural, and legal forces. Indeed, despite the new regulation's central goal of harmonizing privacy across Europe by preempting today's enormous variation in national approaches, policymakers have been hobbled by an absence of evidence as to which national choices about privacy governance have proven more or less resilient in the face of radical technological and social change. Information about the relative strengths and benefits of the alternate regulatory approaches that have flourished in the "living laboratories" of the European member states is largely undeveloped.

This Article begins to fill this gap—and at a critical juncture. Our "on the ground" project uses qualitative empirical inquiry—including interviews with, and questionnaires completed by, corporate privacy officers, regulators, and other actors within the privacy field in three European countries, France, Germany and Spain—to identify the ways in which privacy protection is implemented in different jurisdictions, and the combination of social, market, and regulatory forces that drive these choices. It thus offers a comparative "in-the-wild" assessment of the effects of the different regulatory approaches adopted by these three countries – as well as with similar research previously completed about privacy "on the ground" in the United States.

Our comparative analysis indicates fundamental flaws in the dominant narratives regarding the regulation of privacy in the United States and Europe—accounts that have dominated privacy scholarship and advocacy for over a decade. Those narratives have portrayed the U.S. regulatory regime as a weak one that fails to provide across-the-board procedures that empower individuals to control the use and dissemination of their personal information. By contrast, those accounts promote a "European" model of privacy governance—typified by rigorous privacy principles embodied in law or binding codes, mandating processes to protect individual "choice" about the use of personal data, and interpreted and monitored by an independent and dedicated privacy agency—as the sort of privacy regime to which the United States must aspire.

Our research, offers evidence to the contrary. First it demonstrates that there is not one single "European" approach, but rather that the implementation of privacy

varies widely among European jurisdictions, reflecting different governance choices and regulatory approaches. Second, it suggests that a variety of "new governance" approaches to privacy resonant in both German and U.S. privacy governance contribute to regulatory frameworks that can both foster adaptability in the face of rapid technological change, and encourage development of the type of privacy expertise within corporations that can respond new privacy threat models raised by new products, services, and business models. Third, it indicates the shortcomings of a traditional "European" rights-based model of privacy protection focused on the protection of individual "choice," and the strengths of a model intended to promote the "operationalization" of privacy within corporate structures, such that privacy expertise informs business decisions about technology, products, and services from the start of the development process to its completion.

In the face of novel challenges to privacy, leveraging the adaptability of distinct regulatory approaches and institutions has never been more important. As technological and social change has altered the generation and use of data, the definition of privacy that has prevailed in the political sphere—individual control over the disclosure and use of personal information—has increasingly lost its salience. In particular, the common instruments of protection generated by this definition—procedural mechanisms to protect individual "choice"—have offered an inapt paradigm for privacy protection in the face of data ubiquity and computing capacity. In developing new metrics for protecting privacy, policymakers must take into account a far more granular and bottom-up analysis of both differences in national practice and the forces on the ground that result in the diffusion—or lack thereof—of corporate structures and institutions that research suggests are most adaptive in protecting privacy in the face of change.

**Authors:**

**Kenneth A. Bamberger** is Professor of Law at the University of California, Berkeley, and Faculty Director of the Berkeley Center for Law and Technology. His research focuses on institutional design and decisionmaking, the governance of technology, and corporate regulation. In particular, his recent 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. At Berkeley, Bamberger teaches Administrative Law, The First Amendment, and Technology and Governance.

**Deirdre K. Mulligan** is an Assistant Professor in the School of Information at UC Berkeley, and a Director of the Berkeley Center for Law & Technology. Prior to joining the School of Information in 2008, she was a Clinical Professor of Law, founding Director of the Samuelson Law, Technology & Public Policy Clinic, and

Director of Clinical Programs at the UC Berkeley School of Law (Boalt Hall). Mulligan is the Policy lead for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University. Mulligan's current research agenda focuses on information privacy and security. Current projects include comparative, qualitative research to explore the conceptualization and management of privacy within corporations based in different jurisdictions, and policy approaches to improving cybersecurity. She is Chair of the Board of Directors of the Center for Democracy and Technology, and a Fellow at the Electronic Frontier Foundation. She is co-chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises technology and policy experts who meet periodically to advise Microsoft about products and strategy. Prior to Berkeley, she served as staff counsel at the Center for Democracy & Technology in Washington, D.C.

# Reconciling Personal Information in the U.S. and EU

Paul M. Schwartz & Daniel J. Solove

Forthcoming in the *California Law Review*. Full paper available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442

**Executive Summary:**

U.S. and EU privacy law can greatly diverge. Even at the threshold level—determining what information is covered by the regulation—the United States and European Union differ significantly. The existence of personal information—commonly referred to as "personally identifiable information" (PII)—is the trigger for when privacy laws apply.

PII is defined quite differently in U.S. and EU privacy law. The U.S. approach involves multiple and inconsistent definitions of PII that are often quite narrow. The EU approach defines PII to encompass all information identifiable to a person, which is a definition that can be quite broad and vague. This divergence is so basic that it threatens the current status quo built around second-order mechanisms for allowing international data transfers, including the presently contentious Safe Harbor. It also raises compliance costs for companies who do business in both areas of the world. But since both the United States and the European Union are deeply committed to their respective approaches, attempts to harmonize U.S. and EU privacy law by turning EU privacy law into a U.S.-style approach, or vice versa, are unlikely to succeed.

In this Essay, we argue that there is a way to bridge these differences regarding PII. We contend that a tiered approach to the concept of PII (which we call "PII 2.0") represents a superior way of defining PII than the current approaches in the United States and European Union. We also argue that PII 2.0 is consistent with the different underlying philosophies of the U.S. and EU privacy law regimes. Under PII 2.0, all of the Fair Information Practices (FIPs) should apply when data refers to an identified person or where there is a significant risk of the data being identified. Only some of the FIPs should apply when data is merely identifiable, and no FIPs should apply when there is a minimal risk that the data is identifiable. We demonstrate how PII 2.0 advances the goals of both U.S. and EU privacy law and how PII 2.0 is consistent with their different underlying philosophies. PII 2.0 thus advances the process of bridging the current gap between U.S. and EU privacy law.

**Authors:**

**Paul Schwartz** is a leading international expert on information privacy law. He is a professor at the University of California, Berkeley Law School and a director of the Berkeley Center for Law and Technology. He has testified before Congress and served as an advisor to international organizations, including Directorate Generals of the European

Union. He assists numerous corporations and organizations with regulatory, policy and governance issues relating to information privacy. Schwartz is a frequent speaker at technology conferences and corporate events in the United States and abroad. He is a Special Advisor to the privacy and data security practice of Paul Hastings LLP.

Professor Schwarz is the author of many books, including the leading casebook, "Information Privacy Law," and the distilled guide, "Privacy Law Fundamentals," each with Daniel Solove. "Information Privacy Law," now in its fourth edition, is used in courses at more than 20 law schools. Schwartz's over fifty articles have appeared in journals such as the *Harvard Law Review, Yale Law Journal, Stanford Law Review*, *University of Chicago Law Review* and *California Law Review*. He publishes on a wide array of privacy and technology topics including data analytics, cloud computing, telecommunications surveillance, data security breaches, health care privacy, privacy governance, data mining, financial privacy, European data privacy law, and comparative privacy law.

**Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also Senior Policy Advisor at Hogan Lovells. Additionally, he is the founder of TeachPrivacy, a company that provides privacy and security training. One of the world's leading experts in privacy law, Solove is the author of numerous books, including *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale 2011), *Privacy Law Fundamentals* (IAPP 2011),*Understanding Privacy* (Harvard 2008), and *The Future of Reputation: Gossip and Rumor in the Information Age* (Yale 2007). Additionally, he is also the author of a textbook, *Information Privacy Law,* as well as more than 40 articles. Solove has testified before Congress and has consulted in a number of high-profile privacy cases.

# Why Data Privacy Law Is (Mostly) Constitutional

Neil M. Richards

Excerpt from *Intellectual Privacy* (forthcoming). Full paper available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335196

**Executive Summary:**

A few kinds of privacy rights run into conflict with the First Amendment, most notably the old Warren and Brandeis argument for a tort by which the rich and famous could keep unflattering and embarrassing truths about them out of the newspapers. But privacy can mean many things, and most of these things are fully consistent with the American commitments to broad rights of free speech and free press. Specifically, we use the term "privacy" to refer to the many laws regulating personal data, including consumer credit and video rental information, and information given to doctors and lawyers. Despite calls from industry groups and a few isolated academics that these laws somehow menace free public debate, the vast majority of information privacy law is constitutional under ordinary settled understandings of the First Amendment. Policymakers can thus make information policy on the merits rather than being distracted by spurious free speech claims.

Throughout the world, democratic societies regulate personal data using laws that embody the "Fair Information Practices" or FIPs. The FIPs are a set of principles that regulate the relationships between business and government entities that collect, use, and disclose personal information about "data subjects," and which were developed by the United States Government in the 1970s. Over the past decade, some (but not all) industry groups and a handful of scholars have argued that the FIPs somehow offend the First Amendment, an argument seemingly strengthened by the Supreme Court's 2011 decision in *Sorrell v. IMS Health*, which struck down a Vermont law preventing drug reps (but no one else) from using data-based marketing to speak to physicians.

Before *Sorrell*, there was a settled understanding that general commercial regulation of the huge data trade wasn't censorship. It was seen on the contrary as part of the ordinary business of commercial regulation that fills thousands of pages of the United States Code and the Code of Federal Regulations. Nothing in the *Sorrell* opinion should lead policymakers to conclude that this settled understanding has changed. The poorly-drafted Vermont law in *Sorrell* discriminated against particular kinds of protected speech (in-person advertising), and particular kinds of protected speakers (advertisers but not their opponents). Such content- and viewpoint discrimination would doom even *unprotected speech* under well-settled First Amendment law. As the Court made clear, the real problem with the Vermont law at issue was that it didn't regulate *enough*, unlike the "more coherent policy" of the undoubtedly constitutional federal Health Insurance Portability and Accountability Act of 1996.

Notwithstanding the Court's clarity on this point, a few observers have suggested that data flows are somehow "speech" protected by the First Amendment. But the "data is speech" argument makes no sense from a First Amendment perspective. People do things every day that are more clearly "speech" than a data flow, from blogging and singing in the shower to insider trading, sexually harassing co-workers, verbally abusing children, and even hiring

assassins. Well-settled First Amendment allows us to separate out which of these activities cannot be regulated (the first two) from those which can (the rest). First Amendment lawyers don't ask whether something is "speech," because almost everything is expressive in some way. Instead, they ask which kinds of government regulation are particularly threatening to long-standing First Amendment values. And commercial regulation – of sexual harassment, unfair trade practices, and commercial data flows based on the FIPs —is rarely threatening to First Amendment values, properly understood by their settled meaning.

The ordinary understandings of First Amendment lawyers are supported by a more fundamental reason. During the New Deal, American society decided that, by and large, commercial regulation should be made on the basis of economic and social policy rather than blunt constitutional rules. This has become one of the basic principles of American Constitutional law. As we move into the digital age, in which more and more of our society is affected or constituted by data flows, we face a similar threat. If "data" were somehow "speech," virtually every economic law would become clouded by constitutional doubt. Economic or commercial policy affecting data flows (which is to say all economic or social policy) would become almost impossible. This might be a valid policy choice, but it is not one that the First Amendment commands. Any radical suggestions to the contrary are unsupported by our Constitutional law.

Privacy law is thus (mostly) constitutional. And when we're talking about the regulation of commercial data flows, it's entirely constitutional, except for a few poorly-drafted outliers like the law struck down in *Sorrell*. In a democratic society, the basic contours of information policy must ultimately be up to the people and their policymaking representatives, and not to unelected judges. We should decide policy on that basis, rather than on odd readings of the First Amendment.

**Author:**

**Neil Richards** is an internationally-recognized expert in privacy law, information law, and freedom of expression. He is a professor of law at Washington University School of Law, a member of the Advisory Board of the Future of Privacy Forum, and a consultant and expert in privacy cases. He graduated in 1997 from the University of Virginia School of Law, and served as a law clerk to Chief Justice William H. Rehnquist. His first book, Intellectual Privacy, will be published by Oxford University Press in 2014.

Professor Richards' many writings on privacy and civil liberties have appeared in prominent legal journals such as the Harvard Law Review, the Columbia Law Review, the Virginia Law Review, and the California Law Review. He has written for a more general audience in Wired Magazine UK, CNN.com, and the Chronicle of Higher Education.

Professor Richards appears frequently in the media, and he is a past winner of the Washington University School of Law's Professor of the Year award. At Washington University, he teaches courses on privacy, free speech, and constitutional law. He was born in England, educated in the United States, and lives with his family in St. Louis. He is an avid cyclist and a lifelong supporter of Liverpool Football Club.


**About the Future Privacy Forum**

Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leading figures from industry, academia, law and advocacy groups.

To learn more about FPF, please visit www.futureofprivacy.org