PRIVACY PAPERS FOR POLICYMAKERS

2015

FUTURE OF PRIVACY FORUM

This publication of *Privacy Papers for Policymakers* is supported by AT&T, Microsoft, and TUNE.

FUTURE OF
PRIVACY
FORUM

January 13th, 2016

We are pleased to introduce FPF's sixth annual *Privacy Papers for Policymakers*. Each year, we invite privacy scholars and authors with an interest in privacy issues to submit papers to be considered by members of our Advisory Board. The Board then selects the scholarship they feel best analyzes emerging privacy issues and is most useful for policymakers in Congress and at government agencies, as well as for data protection authorities abroad.

In a year in which privacy made headlines across a variety of contexts, from international data transfers to internet- connected consumer appliances, it isn't a surprise that the papers selected this year examine a broad spectrum of privacy issues. The authors have explored wide-ranging topics, including the design of effective privacy notices, data release policies in light of the challenges of anonymization and re-identification, the relationship between privacy and markets, and the role of trust in data transfers. We hope this collection of scholarship can help to inform policymakers in Congress, at the FTC, and in other federal and state agencies as they work to explore new privacy issues.

We want to thank AT&T, Microsoft, and TUNE for their special support of this project. And as always, we thank the scholars, advocates, and Advisory Board members that are engaged with us to explore the future of privacy.

Sincerely,

Chris Wolf

Christopher Wolf
Founder and Board President

Jules Polonetsky

Jules Polonetsky
CEO and Executive Director

Future of Privacy Forum Advisory Board

Alessandro Acquisti
Associate Professor of Information
Technology and Public Policy
Heinz College
Carnegie Mellon University

Harvey Anderson
Chief Legal Officer
AVG Technologies USA, Inc.

Sharon A. Anolik
President
Privacy Panacea

Annie I. Antón
Professor of Computer Science and
Chair of the School of Interactive Computing
College of Computing
Georgia Institute of Technology

Stefanie Ash
Chief Privacy Officer, US
American Express

Jonathan Avila
Chief Privacy Officer
Wal-Mart Stores, Inc.

Chris Babel
Chief Executive Officer
TRUSTe

Stephen Balkam
Chief Executive Officer
Family Online Safety Institute

Kenneth A. Bamberger
Professor of Law
University of California
Berkeley School of Law

Nancy Bell
Senior Manager, External Affairs
FCA US LLC

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

Andrew Bloom
Chief Privacy Officer
McGraw-Hill Education

Michael Blum
Senior Vice President
Business and Legal Affairs
Quantcast

Bill Bowman
Vice President, Cyber Security
Houghton Mifflin Harcourt

Bruce Boyden
Assistant Professor of Law
Marquette University Law School

John Breyault
Vice President, Public Policy
Telecommunications and Fraud
National Consumers League

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

Ann Cavoukian, Ph.D.
Executive Director
Privacy and Data Institute
Faculty of Science
Ryerson University

Brian Chase
General Counsel
Foursquare Labs, Inc.

Danielle Citron
Professor of Law
University of Maryland School of Law

Allison Cohen
Managing Counsel
Toyota Motor North America, Inc.

Maureen Cooney
Head of Privacy
Sprint Corporation

Mary Culnan
Professor Emeritus
Bentley University

Simon Davies
Founder
Privacy International

Kim Dawson
Senior Director of Privacy
Nordstrom, Inc.
Michelle De Mooy
Deputy Director, Consumer Privacy
Center for Democracy & Technology

Laurie Dechery
Associate General Counsel
Lifetouch, Inc.

Elizabeth Denham
Information and Privacy Commissioner
British Columbia

Jeff Donaldson
Senior Vice President
GameStop Technology Institute

Brian Dunphy
Senior Vice President of Business
Development and Partner Relations
Gimbal, Inc.

Benjamin Edelman
Assistant Professor
Harvard Business School

Erin Egan
Chief Privacy Officer, Policy
Facebook, Inc.

Keith Enright
Senior Corporate Counsel
Google, Inc.

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
Professor of Law
Washington and Lee University
School of Law

Leigh Freund
President and CEO
Network Advertising Initiative

Eric Friedberg
Co-President
Stroz Friedberg

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

Michelle Garcia
General Counsel
Yext

Deborah Gertsen
Counsel, Global Privacy
Ford Motor Company

Julie Gibson
Global Privacy Program Leader
The Procter & Gamble Company

Jennifer Barrett Glasgow
Chief Privacy Officer, Emeritus
Acxiom Corporation

Eric Goldman
Professor, Santa Clara University
School of Law
Director, High Tech Law Institute

Scott Goss
Senior Privacy Counsel
Qualcomm, Inc.

Justine Gottshall
Chief Privacy Officer
Signal

Kimberly Gray
Chief Privacy Officer
IMS Health, Inc.

Janine Greenwood
Chief Legal Officer
Vice President
National Student Clearinghouse

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

Ghita Harris-Newton
Assistant General Counsel
Head of Global Privacy Law & Privacy Policy
Yahoo! Inc.

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

Megan Hertzler
Director of Enterprise Information
Governance
PG&E

David Hoffman
Associate General Counsel and Global
Privacy Officer
Intel Corporation

Lara Kehoe Hoffman
Global Director, Data Privacy and Security
Netflix

Bo Holland
Founder & CEO
AllClearID

Chris Hoofnagle
Adjunct Professor
Berkeley School of Information
Faculty Director,
Berkeley Center for Law & Technology

Jane Horvath
Director of Global Privacy
Apple, Inc.

Margaret Hu
Assistant Professor of Law
Washington and Lee University
School of Law

Sandra R. Hughes
Chief Executive Officer and President
Sandra Hughes Strategies

Trevor Hughes
President & Chief Executive Officer
International Association of
Privacy Professionals

Brian Huseman
Director, Public Policy
Amazon.com, Inc.

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

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

Cameron F. Kerry
Senior Counsel, Sidley Austin LLP

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

Dan Koslofsky
Chief Privacy & Compliance Officer
AARP

Michael C. Lamb, Esq.
Chief Counsel, Privacy and Information
Governance
RELX Group

Barbara Lawler
Chief Privacy Officer
Intuit, Inc.

Peter M. Lefkowitz
Chief Privacy Officer
Chief Privacy & Data Protection Counsel
GE Corporate Legal
General Electric Company

Sagi Leizerov, Ph.D
Americas Practice Leader, Privacy & Data
Protection Advisory Services
Ernst & Young, LLP

Gerard Lewis
Senior Counsel and Chief Privacy Officer
Comcast Corporation

Harry Lightsey
Executive Director, Federal Affairs
General Motors Company

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

David Liu
Chief Operating Officer
Knewton, Inc.

Brendon Lynch
Chief Privacy Officer
Microsoft Corporation

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

Larry Magid
Co-Founder and Co-Director
Connect Safely

Danan Margason
General Counsel
TUNE, Inc.

Kirsten Martin, Ph.D.
Assistant Professor
Strategic Management and Public Policy
George Washington University School of
Business

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
Ghostery, Inc.

Doug Miller
Global Privacy Leader
AOL, Inc.

Tiffany L. Morris
Vice President and General Counsel
Lotame Solutions, Inc.

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Jill Nissen
Principal and Founder
Nissen Consulting

Harriet Pearson
Partner
Hogan Lovells LLP

Future of Privacy Forum Advisory Board (continued)

Christina Peters
Senior Counsel, Security and Privacy
IBM Corporation

John Plunkett
Vice President, Policy & Advocacy
Hobsons

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

MeMe Rasmussen
Vice President, Chief Privacy Officer
Associate General Counsel
Adobe Systems, Inc.

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

Emma Redmond
Data Protection and Privacy Counsel
LinkedIn, Inc.

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

Neil Richards
Professor of Law
Washington University Law School

Susan Rohol
Global IP/Privacy Policy Director
Government & Public Affairs
NIKE, Inc.

Mila Romanoff
Legal Specialist
Partnerships
Privacy & Data Protection
UN Global Pulse

Shirley Rooker
President
Call for Action

Michelle Rosenthal
Corporate Counsel
T-Mobile, Inc.

Alexandra Ross
Senior Global Privacy and Data Security
Counsel
Autodesk

Patrick Salyer
Chief Executive Officer
Gigya, Inc.

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

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

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

Dale Skivington
Chief Privacy Officer
Dell, Inc.

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
Senior Vice President
and Global Privacy & Data Protection Officer
MasterCard Incorporated

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

Zoe Strickland
Managing Director
Global Chief Privacy Officer
JPMorgan Chase Bank NA

Greg Stuart
Chief Executive Officer
Mobile Marketing Association

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

Omer Tene
Vice President of Research
and Education
International Association
of Privacy Professionals

Adam Thierer
Senior Research Fellow
Mercatus Center
George Mason University

Catherine Tucker
Mark Hyman, Jr. Career Development
Professor and Associate Professor of
Management Science
Sloan School of Management
Massachusetts Institute of Technology (MIT)

David C. Vladeck
Professor of Law
Georgetown University Law Center

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

Daniel J. Weitzner
Co-Director, MIT CSAIL
Decentralized Information Group
W3C Technology and Society Policy Director

Estelle Werth
Global Privacy Officer
Criteo

Heather West
Senior Policy Manager
Mozilla

Christopher Wood
Executive Director & Co-Founder
LGBT Technology Partnership

Jack Yang
Associate General Counsel
Global Privacy Office
and Enterprise Risk Legal
Visa, Inc.

Karen Zacharia
Chief Privacy Officer
Verizon Communications, Inc.

Elana Zeide
Privacy Research Fellow
Information Law Institute
New York University

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

Table of Contents

Honorable Mention

Out of respect for copyright law and for ease of reference, this compilation is a digest of the papers selected by the Future of Privacy Forum Advisory Board and does not contain full text. The selected papers in full text are available through the referenced links.

A Design Space for Effective Privacy Notices

Florian Schaub, Rebecca Balebako, Adam L. Durity & Lorrie Faith Cranor

Published in the Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS 2015).
Full paper available at: https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

Executive Summary:

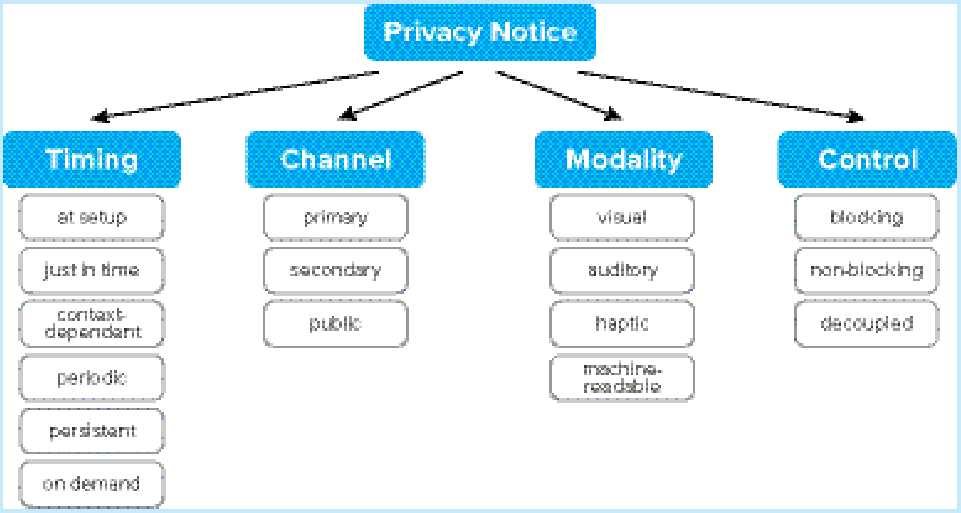
The goal of privacy notices is to make a company's data practices involving personal information transparent. Notifying consumers about a system's data practices is supposed to enable them to make informed privacy decisions. Yet, current notice and choice mechanisms, such as privacy policies, are often ineffective because they are too complex and lack meaningful choices. They are neither usable nor useful, and are therefore ignored by users. The increasing adoption of mobile devices, smartphones, wearables, and Internet of Things technology exacerbates the issue. Such devices are highly connected with each other and the cloud, but small screens and limited interaction capabilities constrain how users can be given notice about and control over data practices.

Much research has studied usability issues of privacy notices and many proposals for more usable privacy notices, transparency tools and privacy mechanisms exist. Yet, so far there has been little guidance for system designers and developers on the design aspects that can impact the effectiveness of privacy notices. As a result, privacy notices are often hastily bolted on rather than integrated into a system's interaction design.

In this paper, we survey the existing literature on privacy notices and identify challenges, requirements, and best practices for the design of usable and effective privacy notices. The goal is to help developers embed privacy notices and choice options into their system design where relevant, with minimal disruption to the interaction with the system. We emphasize the importance of understanding a system's information flows and different user groups, as well as the system's constraints and opportunities for providing notice, in order to develop layered and contextualized privacy notices that provide information that is relevant and actionable.

We further identify relevant aspects of privacy notices that need to be considered in their design. The main dimensions of this design space are the timing of a notice, the channel used to deliver the notice, the modality used to communicate with the user, and how control and choice options are integrated. For each dimension, we discuss multiple alternatives

Figure 1. The privacy notice design space.



The four main dimensions offer multiple options and alternatives for designing notices.

and their implications for a notice's effectiveness. Our design space provides a taxonomy and consistent terminology of notice approaches to foster understanding and reasoning about notice options available in the context of specific systems.

A key aspect of effective notice design is the realization that a privacy policy, which may be necessary for regulatory compliance, is insufficient and often unsuitable for informing users. Privacy policies need to be accompanied by a comprehensive user-oriented notice concept that leverages the options provided in the notice design space to provide targeted notices with information relevant to a specific audience and their interaction with the system and makes the given privacy information actionable by providing real choices.

Novel technologies and integrated devices, such as wearables or the Internet of Things, pose new challenges for the design of privacy notices and controls. Public policy, legislation, and technological approaches need to work together to enable users to manage their privacy in such systems. The identified best practices and the proposed design space provide the means to reason about meaningful design options for notice and control in such systems. For instance, by leveraging alternative channels or modalities, and providing notices and control options at different times in the information lifecycle.

Authors:

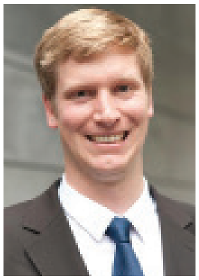


Photo © Elvira Eberhardt

Florian Schaub is a postdoctoral fellow in the School of Computer Science at Carnegie Mellon University. His research focuses on human factors of privacy, human-computer interaction, ubiquitous computing, and mobile security. He has a doctoral degree and Diplom in Computer Science from Ulm University, Germany, and a Bachelor in Information Technology (Multimedia Technology) from Deakin University, Australia. Dr. Schaub is an IAPP Certified Information Privacy Professional (CIPP/US) and Privacy Technologist (CIPT). His research has been featured in the *Wall Street Journal, The Guardian, Wired, New Scientist,* as well as on CNN and BBC.

Rebecca Balebako is an information scientist at RAND Corporation. Her research in usable privacy has included understanding and communicating the privacy and security risks of technology to consumers. Her work has also examined how user studies can inform policy-making for privacy. Her work is at the intersection of computer science, psychology, and behavioral economics. Before attending graduate school, she was a software engineer and product manager at startups and research universities for over a decade. She is particularly interested in the process of developing quality and ethical software, both through social engineering and improved programming tools.

Adam L. Durity is a privacy engineer on the Privacy & Security team at Google. Prior to Google, he completed the Privacy Engineering Master's program at Carnegie Mellon University, focusing on mapping the privacy notice design space, parent-teen privacy, and password research. Previously, Adam was a technology analyst in the financial services industry. Adam earned his Bachelor's degree in electrical and computer engineering and computer science from Duke University.

Lorrie Faith Cranor is serving as Chief Technologist at the US Federal Trade Commission while on leave from Carnegie Mellon University where she is a professor of Computer Science and of Engineering and Public Policy, director of the CyLab Usable Privacy and Security Laboratory (CUPS) and co-director of the MSIT-Privacy Engineering masters program. She is also a co-founder of Wombat Security Technologies, Inc. She is a fellow of the ACM and the IEEE. Dr. Cranor has authored over 150 research papers on online privacy, usable security, and other topics. She has played a key role in building the usable privacy and security research community, having co-edited the seminal book *Security and Usability* (O'Reilly 2005) and founded the Symposium On Usable Privacy and Security (SOUPS). She also chaired the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C and authored the book *Web Privacy with P3P* (O'Reilly 2002). She has served on a number of boards, including the Electronic Frontier Foundation Board of Directors, and on the editorial boards of several journals. She was previously a researcher at AT&T-Labs Research and taught in the Stern School of Business at New York University. In 2012-13 she spent her sabbatical year as a fellow in the Frank-Ratchye STUDIO for Creative Inquiry at Carnegie Mellon University where she worked on fiber arts projects that combined her interests in privacy and security, quilting, computers, and technology. She practices yoga, plays soccer, and runs after her three children.

Anonymization and Risk

Ira S. Rubinstein & Woodrow Hartzog

Forthcoming in the *Washington Law Review.*
Full paper available at: http://papers.ssrn.com/sol3/abstract_id=2646185

Executive Summary:

It turns out that "anonymization" is not foolproof. The possibility of correctly identifying people and attributes from anonymized data sets has sparked one of the most lively and important debates in privacy law. The credibility of anonymization, which anchors much of privacy law, is now open to attack. How should the law respond? Critics of anonymization argue that almost any data set is vulnerable to a reidentification attack given the inevitability of related data becoming publicly available over time, thereby setting the stage for a linkage attack. Defenders of anonymization counter that despite the theoretical and demonstrated ability to mount such attacks, the likelihood of reidentification for most data sets remains minimal. As a practical matter, they argue most data sets will remain anonymized using established techniques.

These divergent views might lead us to different regulatory approaches. Those that focus on the remote possibility of reidentification might prefer an approach that reserves punishment only in the rare instance of harm, such as a negligence or strict liability regime revolving around harm triggers. Critics of anonymization might suggest we abandon deidentification-based approaches altogether, in favor of different privacy protections focused on collection, use, and disclosure that draw from the Fair Information Practice Principles, often called the FIPPs.

There is a better focus for the data release law and policy: the process of minimizing risk. We argue that the best way to move data release policy past the alleged failures of anonymization is to focus on the process of minimizing risk, not preventing harm. We argue that focusing on process and risk can bridge the concerns of formalists (for whom mathematical proof is the touchstone of any meaningful policy) and pragmatists (for whom workable solutions should prevail over theoretical concerns). This change in focus reframes the debate away from the endpoint of perfect anonymity and toward the process of risk management. In order to develop a clear, flexible, and workable legal framework for data releases, we propose drawing from the related, more established area of data security.

The law of data security focuses on requiring reasonable processes that decrease the likelihood of harm, even if threats are remote. Because there is no such thing as perfect data protection, data security policy is focused on regular risk assessment, the implementation of technical, physical, and procedural safeguards, and the appropriate response once a system or data set has been compromised.

Data security policy also largely refrains from overly specific rules, deferring instead to a reasonable adherence to industry standards. As the motivation for a consistent approach to releasing personal data increases, industry standards will inevitably develop in coordination with public policy and consumer protection goals. In short, the law of data release should look more like the law of data security: process-based, contextual, and tolerant of harm, so long as procedures to minimize risk are implemented ex ante.

We advocate a system where perfect anonymization is not the enemy of sound data release policy. However, we do not fully embrace the pragmatism advocated by defenders of anonymization. The lessons learned from the criticism and defense of anonymization can be used to develop a policy-driven and comprehensive process-based framework for minimizing the risk of reidentification and sensitive attribute disclosure. By identifying risk factors, mitigating techniques, and shifting from output to process, we can move past the anonymization stalemate between the formalists and the pragmatists driving this debate. For example, policy makers should look specific risk vectors such as data volume, data sensitivity, type of data recipient, data use, data treatment technique, data access controls, and consent and consumer expectations.

A risk-based approach recognizes that there is no perfect anonymity. It focuses on process rather than output. Yet effective risk-based data release policy also avoids a ruthless pragmatism by acknowledging the limits of current risk projection models and building in important protections for individual privacy. This policy-driven, integrated, and comprehensive approach will help us better protect data while preserving its utility.

Authors:

Ira Rubinstein is a Senior Fellow at the Information Law Institute of the New York University School of Law. His research interests include Internet privacy, electronic surveillance law, big data, and voters' privacy. Rubinstein lectures and publishes widely on issues of privacy and security and has testified before Congress on these topics on several occasions. Recent papers include a research report on *Systematic Government Access to Personal Data: A Comparative Analysis,* prepared for the Center for Democracy and Technology and co-authored with Ron Lee and Greg Nojeim; *Big Data: The End of Privacy or a New Beginning*, published in International Data Privacy Law in 2013 and presented at the 2013 Computer Privacy and Data Protection conference in Brussels; *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, co-authored with Nathan Good, published in the Berkeley Technology Law Journal in 2013 and which won the IAPP Privacy Law Scholars Award at the 5th Annual Privacy Law Scholars Conference in 2012; and *Regulating Privacy by Design*, 26 BERKELEY TECH L.J. 1409 (2012). Rubinstein has also completed a work in progress entitled *Voter Privacy in the Age of Big Data*. Prior to joining the ILI, Rubinstein spent 17 years in Microsoft's Legal and Corporate Affairs department, most recently as Associate General Counsel in charge of the Regulatory Affairs and Public Policy group. Before coming to Microsoft, he was in private practice in Seattle, specializing in immigration law. Rubinstein graduated from Yale Law School in 1985. From 1998-2001, he served on the President's Export Council, Subcommittee on Encryption. He has also served on the Editorial Board of the IEEE Security and Privacy Magazine. In 2010, he joined the Board of Directors of the Center for Democracy and Technology.

Woodrow Hartzog is an Associate Professor at Samford University's Cumberland School of Law. He is also an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research focuses on privacy, media, contracts, and robotics. His work has been published in numerous scholarly publications such as the *Columbia Law Review, California Law Review,* and *Michigan Law Review* and popular publications such as BBC, CNN, *The Guardian, Wired, Bloomberg, New Scientist, 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,* and *USA Today.* His book, P*rivacy's Blueprint: The Battle to Control the Design of New Technologies,* is under contract with Harvard University Press.

A Precautionary Approach to Big Data Privacy

Arvind Narayanan, Joanna Huey & Edward W. Felten

Presented at Computers, Privacy & Data Protection 2015.
Full paper available at: http://randomwalker.info/publications/precautionary.pdf

Executive Summary:

Once released to the public, data cannot be taken back. As time passes, data analytic techniques improve and additional datasets become public that can reveal information about the original data. It follows that released data will get increasingly vulnerable to re-identification—unless methods with provable privacy properties are used for the data release.

We review and draw lessons from the history of re-identification demonstrations; explain why the privacy risk of data that is protected by ad hoc de-identification is not just unknown, but unknowable; and contrast this situation with provable privacy techniques like differential privacy. We then offer recommendations for practitioners and policymakers. Because ad hoc de-identification methods make the probability of a privacy violation in the future essentially unknowable, we argue for a weak version of the precautionary approach, in which the idea that the burden of proof falls on data releasers guides policies that incentivize them not to default to full, public releases of datasets using ad hoc de-identification methods. We discuss the levers that policymakers can use to influence data access and the options for narrower releases of data. Finally, we present advice for six of the most common use cases for sharing data. Our thesis is that the problem of "what to do about re-identification" unravels once we stop looking for a one-size-fits-all solution, and in each of the six cases we consider a solution that is tailored, yet principled.

Authors:

Arvind Narayanan is an Assistant Professor of Computer Science at Princeton. He studies information privacy and security and has a side-interest in technology policy. His research has shown that data anonymization is broken in fundamental ways, for which he jointly received the 2008 Privacy Enhancing Technologies Award. Narayanan leads the Princeton Web Transparency and Accountability Project, which aims to uncover how companies are collecting and using our personal information. He also studies the security and stability of Bitcoin and cryptocurrencies. Narayanan is an affiliated faculty member at the Center for Information Technology Policy at Princeton and an affiliate scholar at Stanford Law School's Center for Internet and Society. You can follow him on Twitter at @random_walker.

Joanna Huey is the associate director of Princeton's Center for Information Technology Policy, which takes an interdisciplinary approach to addressing the interaction of digital technologies and society. Prior to joining CITP, she clerked for the Honorable Michael Boudin, worked as a business associate at Goodwin Procter, and co-founded Casetext, a Y Combinator-backed startup. She holds an A.B. in physics and math from Harvard College, an M.P.P. in science and technology policy from the Harvard Kennedy School, and a J.D. from Harvard Law School, where she was president of the *Harvard Law Review*.

Edward W. Felten is Deputy U.S. Chief Technology Officer at the White House. He is on leave from Princeton University, where he is the Robert E. Kahn Professor of Computer Science and Public Affairs, and the founding Director of Princeton's Center for Information Technology Policy. In 2011-12 he served as the first Chief Technologist at the U.S. Federal Trade Commission. His research interests include computer security and privacy, and technology law and policy. He has published more than 100 papers in the research literature, and two books. His research on topics such as Internet security, privacy, copyright and copy protection, and electronic voting has been covered extensively in the popular press. He is a member of the National Academy of Engineering and the American Academy of Arts and Sciences, and is a Fellow of the ACM. He has testified before the House and Senate committee hearings on privacy, electronic voting, and digital television. In 2004, *Scientific American* magazine named him to its list of fifty worldwide science and technology leaders.

Privacy and Markets: A Love Story

Ryan Calo

Forthcoming in the *Notre Dame Law Review*.
Full paper available at: http://papers.ssrn.com/sol3/abstract_id=2640607

Executive Summary:

Imagine a market without privacy. What if price and quality were only small considerations among a large amount of extraneous information about market participants? Would such a marketplace, where consumers and businesses knew everything about one another, actually work? Would it be efficient? Would it be desirable?

This article finds that privacy and markets turn out to be interdependent and fundamentally sympathetic—each allows the other to function in a more efficient and desirable way. The law and economics critique of privacy, and the hostility toward markets displayed by many privacy scholars, fail to tell us much about the deeper relationship between the two concepts. Setting aside such mutual skepticism, this article develops a novel account of privacy and markets as opposites that attract.

Markets assume and rely upon privacy for a number of important functions. While information is crucial to the proper functioning of the marketplace, privacy supports the basic market mechanism by preventing an inundation of extraneous, value-laden information. Privacy helps to hide distracting information from market participants by focusing on the traditionally relevant market considerations, such as quality and price, over potentially distorting and balkanizing information, like personal or political commitments.

Privacy facilitates stable and trustworthy business partnerships by creating the conditions for market intimacy, enabling parties to disclose desired details over time. And privacy helps keep information asymmetry between people and firms in check. In today's markets, firms can process new information much faster than consumers can, and will increasingly have the potential to use dynamic price discrimination to exploit consumers. The market relies upon privacy, which in effect, saves the market from itself.

The reverse is true as well: privacy assumes and relies upon markets. In thinking through how privacy is necessary for human self-actualization, we should not lose sight that privacy is not a sufficient condition for human flourishing. People must not only have a means by which to withdraw, but also a means by which to connect. Markets help support human flourishing by connecting people to the basic needs, cultural resources, ideas, and materials necessary for self-determination. With both competitive and collective functions, markets provide a relatively anonymous means by which society can distribute these resources. A world without markets would alternatively depend on highly detailed information about all individuals, and therefore would not be a very privacy-friendly one.

This article builds the case for protecting privacy within the market context, including through the force of law. A framework where privacy and markets function together symbiotically helps resolve certain institutional puzzles, such as why the Federal Trade Commission arose as the de facto privacy authority for the United States, and how other agencies like the Consumer Financial Protection Bureau are likely to become increasingly involved in privacy enforcement. The normative case for certain laws and policies keeping personal information out of markets is presented. The enforcement of such laws can allow parties to focus on the efficient exchange of goods and services, duly separated from their roles as real people living in a complex world.

Author:

Ryan Calo is an assistant professor at the University of Washington School of Law and an assistant professor (by courtesy) at the Information School. He is a faculty co-director (with Batya Friedman and Tadayoshi Kohno) of the University of Washington Tech Policy Lab, a unique, interdisciplinary research unit that spans the School of Law, Information School, and Department of Computer Science and Engineering. Professor Calo has testified about privacy before the full Judiciary Committee of the United States Senate and spoken at the Aspen Ideas Festival and NPR's Weekend in Washington. Prior to academia he worked as an associate in the D.C. offices of Covington & Burling, LLP.

Taking Trust Seriously in Privacy Law

Neil Richards & Woodrow Hartzog

Forthcoming in the *Stanford Technology Law Review.*
Full paper available at: http://papers.ssrn.com/sol3/abstract_id=2655719

Executive Summary:

Trust is beautiful. The willingness to accept vulnerability to the actions of others is the essential ingredient for friendship, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow. Trust is everywhere, but particularly at the core of the information relationships that have come to characterize our modern, digital lives. Relationships between people and their ISPs, social networks, and hired professionals are typically understood in terms of privacy. But the way we have talked about privacy has a pessimism problem – privacy is conceptualized in negative terms, which leads us to mistakenly look for "creepy" new practices, focus excessively on harms from invasions of privacy, and place too much weight on the ability of individuals to opt out of harmful or offensive data practices.

But there is another way to think about privacy and shape our laws. Instead of trying to protect us against bad things, privacy rules can also be used to create good things, like trust. In this paper, we argue that privacy can and should be thought of as enabling trust in our essential information relationships. This vision of privacy creates value for all parties to an information transaction and enables the kind of sustainable information relationships on which our digital economy must depend.

Drawing by analogy on the law of fiduciary duties, we argue that privacy laws and practices centered on trust would enrich our understanding of the existing privacy principles of confidentiality, transparency, and data protection. Reconsidering these principles in terms of trust would move them from procedural means of compliance for data extraction towards substantive principles to build trusted, sustainable information relationships. Thinking about privacy in terms of trust also reveals a principle that we argue should become a new bedrock tenet of privacy law: the Loyalty that data holders must give to data subjects. Rejuvenating privacy law by getting past Privacy Pessimism is essential if we are to build the kind of digital society that is sustainable and ultimately beneficial to all – users, governments, and companies. There is a better way forward for privacy. Trust us.

Authors:

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, an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, and a consultant and expert in privacy cases. He serves on the boards of the Future of Privacy Forum, the Right to Read Foundation, and is a member of the American Law Institute. Professor Richards graduated in 1997 with degrees in law and history from the University of Virginia, and served as a law clerk to William H. Rehnquist, Chief Justice of the United States. Professor Richards is the author of *Intellectual Privacy* (Oxford Press 2015). His many writings on privacy and civil liberties have appeared in a variety of academic journals including 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 *Time, Slate, Salon, Wired,* CNN.com, *Forbes,* the *Boston Review,* and the *Chronicle of Higher Education.*

Woodrow Hartzog is an Associate Professor at Samford University's Cumberland School of Law. He is also an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research focuses on privacy, media, contracts, and robotics. His work has been published in numerous scholarly publications such as the *Columbia Law Review, California Law Review,* and *Michigan Law Review* and popular publications such as BBC, CNN, *The Guardian, Wired, Bloomberg, New Scientist, 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,* and *USA Today.* His book, *Privacy's Blueprint: The Battle to Control the Design of New Technologies,* is under contract with Harvard University Press.

Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Peter Swire

Testimony, Senate Judiciary Committee Hearing, July 8, 2015
Full paper available at: http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf

Executive Summary:

This testimony was submitted as a part of the Senate Judiciary Committee's Hearing on "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy" on July 8, 2015. This testimony argues why providing exceptions for law enforcement and intelligence agencies to access encrypted data would be harmful, rather than helpful, to national security. Despite concerns of "going dark," the steady increase of electronic communications worldwide provides these agencies with an ever-growing amount of valuable data and meta-data to use in identifying and pursuing targets of investigations. The inability to directly access the content of a small fraction of these communications does not warrant the subsequent damage that would result to privacy and to U.S. economic, diplomatic, and security interests.

In Part I, this testimony describes the conclusions of the President's Review Group on Intelligence and Communications Technology issued in the wake of the Snowden revelations. The Review Group unanimously and clearly recommended that the U.S. Government vigorously encourage the use of strong encryption. With full awareness of the "going dark" concerns, it sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny. Based on the top-secret briefings and the Group's experience, it found these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

In Part II, this testimony argues that it is more accurate to say we are in a "Golden Age of Surveillance" than for law enforcement to assert that it is "Going Dark." While law enforcement and intelligence agencies do lose some specific previous surveillance capabilities due to changing encryption technologies, these specific losses are more than offset by massive gains, including location information, information about contacts and confederates, and an array of new databases that create digital dossiers about individuals' lives. The testimony demonstrates the gains to law enforcement through the growth of smartphones and text messages, specifically noting that the predominant share of all text messages sent are unencrypted, and therefore available from the provider. Even for the small subset of messages that are encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs. With over six trillion SMS messages sent in 2010, text messages are a prime example of a golden age of surveillance, and not of going dark.

In Part III, this testimony argues that government-mandated vulnerabilities would threaten severe harm to cybersecurity, privacy, human rights, and U.S. technological leadership, while not preventing effective encryption by adversaries. Concerns around government-mandated encryption vulnerabilities include: (1) technology companies, even before Snowden, had multiple reasons to deploy strong encryption to enhance cybersecurity and customer trust; (2) overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption; (3) U.S. government support for encryption vulnerabilities increases cybersecurity problems in the "least trusted countries" and globally, and undermines U.S. human rights policies; and (4) mandated vulnerabilities are bad industrial policy and threaten U.S. technological leadership without preventing bad actors from using strong encryption.

Author:

Peter P. Swire has been a leading privacy and cyberlaw scholar, government leader, and practitioner since the rise of the Internet in the 1990's. In 2013, he became the Nancy J. and Lawrence P. Huang Professor of Law and Ethics at the Georgia institute of Technology. Swire teaches in the Scheller College of Business, with appointments by courtesy with the College of Computing and School of Public Policy. He is senior counsel with the law firm of Alston & Bird LLP. Swire served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Prior to that, he was co-chair of the global Do Not Track process for the World Wide Web Consortium. He is a Senior Fellow with the Future of Privacy Forum, and a Policy Fellow with the Center for Democracy and Technology.

Swire has been a recognized leader in privacy, cybersecurity, and the law of cyberspace for well over a decade, as a scholar, government official, and participant in numerous policy, public interest, and business settings. From 2009 to 2010 Professor Swire was Special Assistant to the President for Economic Policy, serving in the National Economic Council under Lawrence Summers. From 1999 to early 2001 Professor Swire served as the Clinton Administration's Chief Counselor for Privacy, in the U.S. Office of Management and Budget, as the only person to date to have government-wide responsibility for privacy issues. Among his other activities when at OMB, Swire was the White House coordinator for the HIPAA Medical Privacy Rule and chaired a White House Working Group on how to update wiretap laws for the Internet age. Professor Swire is lead author of the official texts for the Foundations and U.S. Law examinations for Certified Information Privacy Professionals. Many of his writings appear at www.peterswire.net.

The Transparent Citizen

Joel R. Reidenberg

Forthcoming in the *Loyola University Chicago Law Journal*.
Full paper available at: http://papers.ssrn.com/sol3/abstract_id=2674313

Executive Summary:

This article shows that the transparency of personal information online through ubiquitous data collection and surveillance challenges the rule of law both domestically and internationally. The article makes three arguments. First, the transparency created by individuals' interactions online erodes the boundary between public and private information and creates a "transparent citizen." Second, the transparent citizen phenomenon undermines the state's faithfulness to the ideals of the rule of law and to citizens' respect for the rule of law. Transparency enables government to collect and use personal information from the private sector in ways that circumvent traditional political and legal checks and balances. Transparency encourages the development of anonymity tools that empower wrong-doers to evade legal responsibility and the rule of law. And, transparency puts national security, public safety and legal institutions at risk in ways that will jeopardize and corrode the public's faith in the rule of law. Third and lastly, transparency challenges international norms and data flows. National data privacy law is anchored in local constitutional culture and the transparency of personal information across borders creates deep-seated political instability that will only be resolved through political treaties.

Author:

Joel R. Reidenberg is the Stanley D. and Nikki Waxberg Chair and Professor of Law at Fordham University where he directs the Center on Law and Information Policy. He was the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton and has also taught as a visiting professor at the University of Paris-Sorbonne and Sciences Po-Paris. Reidenberg publishes regularly on both information privacy and on information technology law and policy. He is a member of the American Law Institute and an Advisor to the ALI's Restatement (Third) on Privacy Principles. Reidenberg has served as an expert adviser to the U.S. Congress, the Federal Trade Commission, the European Commission and the World Intellectual Property Organization. At Fordham, Reidenberg previously served as the University's Associate Vice President for Academic Affairs and, prior to his academic career, he was an associate at the law firm Debevoise & Plimpton.

Reidenberg is a graduate of Dartmouth College, earned a J.D. from Columbia University and a Ph.D. in law from the Université de Paris–Sorbonne. He is admitted to the Bars of New York and the District of Columbia.

FUTURE OF
PRIVACY
FORUM

The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. We facilitate discussions with privacy advocates, industry leaders, regulators, legislators (and their staff) and international representatives, to inform our Advisory Board and their organizations, and to exchange views. The annual publication of *Privacy Papers for Policymakers* brings the best academic ideas to the attention of government leaders.

1400 EYE STREET, NW | SUITE 450 | WASHINGTON, DC 20005 • FPF.ORG