PRIVACY PAPERS FOR POLICYMAKERS

2016

Privacy Papers for Policymakers is supported in part by the National Science Foundation under Grant No. 1654085.

January 11th, 2017

We are pleased to introduce FPF's seventh annual Privacy Papers for Policymakers. Each year, we invite privacy scholars and authors with an interest in privacy issues to submit scholarship 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 data protection authorities abroad.

This year, each of the selected papers explores an issue of critical importance for the years ahead. Several authors provide policymakers with immediate and specific policy recommendations, stemming from nuanced analyses of the role of Congress in laying the groundwork for cross-border data sharing by law enforcement (Daskal); respect for privacy of "public" records about individuals (Martin & Nissenbaum); and design of decision-making algorithms such that they align with basic objectives of fairness and non-discrimination (Kroll, et al). Each paper eschews conventional wisdoms or status quos, and instead provides policymakers with concrete, intelligent paths forward.

Other authors have provided in-depth reviews of subjects of growing importance, which we believe policymakers will find valuable. A comprehensive framework for how courts should recognize privacy and data security harms will have fundamental importance for any privacy-related legislation in years ahead (Solove & Citron). Relatedly, policymakers should read the first in-depth exploration of the role of state attorneys general as privacy enforcers (Citron), which will be increasingly important as states become laboratories of privacy norm-setting.

Finally, for the first time, we are proud to highlight a winning Student Paper. A computer science review of third-party tracking online will help policymakers understand the realities of Internet data sharing today, an issue of growing concern (Englehardt & Narayanan). As we engage with the challenges ahead, it will be more important than ever to engage students in the work of bridging the gaps between law, technology, and policy.

We want to thank the National Science Foundation for their 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,

Christopher Wolf
Founder and Board President

Jules Polonetsky
CEO and Executive Director

Future of Privacy Forum Advisory Board

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

Nicholas Ahrens
Vice President of Privacy and Cybersecurity
Retail Industry Leaders Association

Sharon A. Anolik
President
Privacy Panacea

Annie I. Antón
Professor and Chair, School of Interactive Computing
Georgia Institute of Technology

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

Stephen Balkam
Chief Executive Officer
Family Online Safety Institute

Kenneth A. Bamberger
Professor of Law
Co-Director of the Berkeley Center for Law and Technology
University of California Berkeley School of Law

Kabir Barday
Chief Executive Officer
OneTrust

Malita Barkataki
Privacy Compliance Director
Yahoo! Inc.

Inna Barmash
General Counsel
Amplify Education, Inc.

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
FPF Executive Board Treasurer

Jodie Z. Bernstein
Counsel
Kelley Drye & Warren, LLP

Andrew Bloom
Chief Privacy Officer
McGraw-Hill Education

Bill Bowman
Vice President, Cyber Security
Houghton Mifflin Harcourt

Bruce Boyden
Associate Professor of Law
Marquette University Law School

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

Julie Brill
Partner
Hogan Lovells LLP

Jill Bronfman
Adjunct Professor of Law
Director of the Privacy and Technology Project at the Institute for Innovation Law
University of California, Hastings College of the Law

Stuart N. Brotman
Howard Distinguished Endowed Professor of Media Management and Law & Beaman Professor of Communication and Information
University of Tennessee, Knoxville

Stephanie J. Bryson
Senior Public Policy Associate
Uber Technologies

J. Beckwith Burr
Deputy General Counsel & Chief Privacy Officer
Neustar

James M. Byrne
Chief Privacy Officer
Lockheed Martin Corporation

Ryan Calo
Assistant Professor of Law
Co-Director of the Tech Policy Lab
University of Washington School of Law

Sam Castic
Sr. Counsel and Director, Privacy
Nordstrom, Inc.

Ann Cavoukian, Ph.D
Executive Director
Privacy and Big Data Institute
Ryerson University

Mary Chapin
Chief Legal Officer
National Student Clearinghouse

Danielle Keats Citron
Morton & Sophia Macht Professor of Law
University of Maryland Francis King Carey School of Law
FPF Senior Fellow

Allison Cohen
Managing Counsel
Toyota Motor Sales, USA, Inc.

Maureen Cooney
Head of Privacy
Sprint Corporation

Mary Culnan
Professor Emeritus
Bentley University
FPF Executive Board Vice President
FPF Senior Fellow

Simon Davies
Founder
Privacy International

Laurie Dechery
Associate General Counsel
Lifetouch, Inc.

Michelle Finneran Dennedy
Chief Privacy Officer
Cisco Systems, Inc.

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

Benjamin Edelman
Associate Professor of Business Administration
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

H. Leigh Feldman
Managing Director, Global Chief Privacy Officer and Head of Privacy and Information Compliance
Citigroup

Lori Fink
Senior Vice President-Assistant General Counsel & Chief Privacy Officer
AT&T Services, Inc.

Dona Fraser
Vice President
Privacy Certified Program
Entertainment Software Rating Board

Leigh M. Freund
President & Chief Executive Officer
Network Advertising Initiative

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

Arkadi Gerney
Senior Fellow
Center for American Progress

Deborah Gertsen
Lead Privacy Counsel
Ford Motor Company

Jennifer Barrett Glasgow
Chief Privacy Officer
Acxiom Corporation

Ben Golden
Director of Legal Affairs
TUNE, Inc.

Eric Goldman
Professor of Law
Co-Director of the High Tech Law Institute
Santa Clara University School of Law

Scott Goss
Senior Privacy Counsel
Qualcomm, Inc.

Justine Gottshall
Chief Privacy Officer
Signal

Kimberly Gray
Chief Privacy Officer
QuintilesIMS

Pamela Jones Harbour
Partner
Fulbright & Jaworski LLP

Ghita Harris-Newton
Assistant General Counsel, Head of Global Privacy Law & Privacy Policy
Quantcast Corporation

Woodrow Hartzog
Assistant Professor
Cumberland School of Law,
Samford University

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

Megan Hertzler
Director of Enterprise Information Governance
PG&E

Beth Hill
General Counsel & Chief Compliance Officer
Ford Direct

Dennis D. Hirsch
Professor of Law
Director of the Program on Data and Governance
The Ohio State University Moritz College of Law

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 of Law
Faculty Director, Berkeley Center for Law & Technology
University of California Berkeley School of Law

Jestlan Hopkins
Privacy Manager
Inflection

Jane Horvath
Director of Global Privacy
Apple, Inc.

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

Sandra R. Hughes
President & Chief Executive Officer
Sandra Hughes Strategies
FPF Executive Board Secretary

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

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

Jeff Jarvis
Professor & Director of the Tow-Knight Center for Entrepreneurial Journalism
The City University of New York Graduate School of Journalism

Michael Kaiser
Chief Executive Director
National Cyber Security Alliance

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 School of Law

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

Barbara Lawler
Chief Privacy Officer
Intuit, Inc.

Virginia Lee
Director, Global Privacy
Starbucks Coffee Company

Peter M. Lefkowitz
Chief Privacy Officer
GE Digital

Sagi Leizerov, Ph.D
Global Privacy Leader - Advisory Services
Ernst & Young, LLP

Yoomi Lee
Vice President - Global Privacy
American Express

Gerard Lewis
Senior Vice President & Deputy General Counsel
Comcast Corporation

Harry Lightsey
Executive Director, Federal Affairs
General Motors Company

Chris Lin
Executive Vice President, General Counsel, & 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
President & CEO
ConnectSafely

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

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

David Medine
Consultant
Consultative Group to Assist the Poor

Scott Meyer
Chief Executive Officer
Ghostery, Inc.

Doug Miller
Global Privacy Leader
AOL, Inc.

John S. Miller
Vice President for Global Policy and Law, Cybersecurity and Privacy
Information Technology Industry Council

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

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Jill L. Nissen, Esq.
Founder & Principal
Nissen Consulting

Harriet Pearson
Partner
Hogan Lovells LLP

Future of Privacy Forum Advisory Board (continued)

Christina Peters
Senior Counsel, Security and Privacy
IBM Corporation

Bilyana Petkova
Postdoctoral Research Fellow
Information Law Institute
New York University

Peter Petros
General Counsel & Global Privacy Officer
Edelman

John Plunkett
Vice President, Policy & Advocacy
Hobsons

Kalinda Raina
Head of Global Privacy, Senior Director
LinkedIn Corporation

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

Alan Raul
Partner
Sidley Austin, LLP
FPF Board Member

Joel R. Reidenberg
Stanley D. and Nikki Waxberg Chair and Professor of Law
Director of the Center on Law and Information Policy
Fordham University School of Law

Neil Richards
Thomas and Karole Green Professor of Law
Washington University Law School

Susan Rohol
Global IP and Privacy Policy Director
NIKE, Inc.

Mila Romanoff
Privacy & Data Protection Legal Officer
United Nations 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

Paul Schwartz
Jefferson E. Peyser Professor of Law
Co-Director of the Berkeley Center for Law & Technology
University of California Berkeley School of Law

Evan Selinger, Ph.D
Professor of Philosophy
Head of Research Communications, Community & Ethics at the Center for Media, Arts, Games, Interaction, and Creativity (MAGIC)
Rochester Institute of Technology
FPF Senior Fellow

Wade Sherman
Acting Chief Privacy Officer
Adobe Systems, Inc.

Linda Sherry
Director, National Priorities
Consumer Action

Meredith Sidewater
Senior Vice President & General Counsel
LexisNexis Risk Solutions

Dale Skivington
Chief Privacy Officer
Dell, Inc.

Will Smith
Chief Executive Officer
Euclid, Inc.

Kim Smouter-Umans
Head of Public Affairs and Professional Standards
ESOMAR

Daniel Solove
John Marshall Harlan Research Professor of Law
The George Washington University Law School

Barbara Sondag
Senior Vice President, Head of Privacy
Westfield

Cindy Southworth
Executive Vice President
National Network to End Domestic Violence

JoAnn Stonier
EVP, Chief Information Governance & Privacy Officer
MasterCard

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 of Law and Ethics
Scheller College of Business
Georgia Institute of Technology
FPF Senior Fellow

Scott M. Taylor
Associate Vice President & Chief Privacy Officer
Merck & Co., Inc.

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

Adam Thierer
Senior Research Fellow, Mercatus Center
George Mason University

Catherine Tucker
Sloan Distinguished Professor of Management & Professor of Marketing
Sloan School of Management
Massachusetts Institute of Technology

Friederike van der Jagt
Senior Legal Counsel Privacy
Avast

David C. Vladeck
Professor of Law
Georgetown University Law Center

Hilary M. Wandall
General Counsel & Chief Data Governance Officer
TRUSTe

Daniel J. Weitzner
Co-Director, Internet Policy Research Initiative
Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Estelle Werth
Vice President, Global Privacy Officer
Criteo

Heather West
Senior Policy Manager
Mozilla

Christopher Wolf
Partner
Hogan Lovells LLP
FPF Executive Board Chair

Nicole Wong
Principal
NWong Strategies

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
Associate Research Scholar
Center for Information Technology Policy
Princeton University

Michael Zimmer
Associate Professor
Director of the Center for Information Policy Research
School of Information Studies
University of Wisconsin, Milwaukee

as of December 31, 2016

Table of Contents

Awarded Papers

Student Paper

Honorable Mentions

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.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The Privacy Policymaking of State Attorneys General

Danielle Keats Citron

Notre Dame Law Review, Forthcoming (2017)
University of Maryland Legal Studies Research Paper No. 2016-08
Available at SSRN: https://ssrn.com/abstract=2733297

Executive Summary

Accounts of privacy law have focused on legislation, federal agencies, and the self-regulation of privacy professionals. Crucial agents of regulatory change, however, have been ignored: the state attorneys general. This article is the first in-depth study of the privacy norm entrepreneurship of state attorneys general. Because so little has been written about this phenomenon, I engaged with primary sources — first interviewing state attorneys general and current and former career staff, and then examining documentary evidence received through FOIA requests submitted to AG offices around the country.

Much as Justice Louis Brandeis imagined states as laboratories of the law, offices of state attorneys general have been laboratories of privacy enforcement. State attorneys general have been nimble privacy enforcement pioneers where federal agencies have been more conservative or constrained by politics. Their local knowledge, specialization, multi-state coordination, and broad legal authority have allowed them to experiment in ways that federal agencies cannot. These characteristics have enabled them to establish baseline fair information protections; expand the frontiers of privacy law to cover sexual intimacy and youth; and pursue enforcement actions that have harmonized privacy policy.

Although certain systemic practices enhance AG privacy policy making, others blunt its impact, including an over reliance on informal agreements that lack law's influence and a reluctance to issue closing letters identifying data practices that comply with the law. This article offers ways state attorneys general can function more effectively through informal and formal proceedings. It addresses concerns about the potential pile-up of enforcement activity, federal preemption, and the dormant Commerce Clause. It urges state enforcers to act more boldly in the face of certain shadowy data practices.

Author

Danielle Keats Citron is the Morton & Sophia Macht Professor of Law at the University of Maryland Francis King Carey School of Law. Her work focuses on information privacy, cyber law, automated systems, and civil rights. She received the 2005 "Teacher of the Year" award.

Professor Citron is the author of Hate Crimes in Cyberspace (Harvard University Press 2014). Cosmopolitan and Harper's Bazaar nominated her book as one of the "Top 20 Best Moments for Women" in 2014; Boston University Law Review held an online symposium on her book in 2015. Her current work focuses on the privacy policymaking of state attorneys general. Professor Citron's scholarship has appeared, or is forthcoming, in Boston University Law Review (twice), California Law Review, George Washington Law Review, Hastings Law Journal, Michigan Law Review (twice), Minnesota Law Review, Notre Dame Law Review, Southern California Law Review, Washington University Law Review, Washington Law Review (twice), Washington & Lee Law Review, U.C. Davis Law Review, and others. Her opinion pieces have been featured in The Atlantic, New York Times, TIME, CNN, Guardian UK, New Scientist, and Slate. She has appeared on National Public Radio, HBO's John Oliver Show and the New York Times video series. She is a technology contributor at Forbes.com and a member of Concurring Opinions.

Law Enforcement Access to Data Across Borders: The Evolving Security and Human Rights Issues

Jennifer Daskal

Journal of National Security Law & Policy, Vol. 8, No. 3 (2016)
Available at: http://jnslp.com/wp-content/uploads/2016/11/Law_Enforcement_Access_to_Data_Across_Borders_2.pdf

Executive Summary

A revolution is underway with respect to law enforcement access to data across borders. Frustrated by delays in accessing sought-after data located across territorial borders, several nations are taking action, often unilaterally, and often in concerning ways. Several nations are considering — or have passed — mandatory data localization requirements, pursuant to which companies doing business in their jurisdiction are required to store certain data, or copies of such data, locally. Such measures facilitate domestic surveillance, increase the cost of doing business, and undercut the growth potential of the Internet by restricting the otherwise free and most efficient movement of data. Meanwhile, a range of nations — including the United Kingdom, Brazil, and others — are asserting that they can unilaterally compel Internet Service Providers (ISPs) that operate in their jurisdiction to produce the emails and other private communications that are stored in other nation's jurisdictions, without regard to the location or nationality of the target. ISPs are increasingly caught in the middle — being forced to choose between the laws of a nation that seeks production of data and the laws of another nation that prohibits such production. In 2015, for example, Brazilian authorities detained a Microsoft employee for failing to turn over data sought by Brazil; U.S. law prohibited Microsoft from complying with the data request. Governments also are increasingly incentivized to seek other means of accessing otherwise inaccessible data, via, for example, use of malware or other surreptitious forms of surveillance.

While this is a problem of international scope, the United States has an outsized role to play, given a combination of the U.S.-based provider dominance of the market, blocking provisions in U.S. law that prohibit the production of the content of emails and other electronic communications to foreign-based law enforcement, and the particular ways that companies are interpreting and applying their legal obligations. It also means that the United States is uniquely situated to lay the groundwork for an alternative approach that better reflects the normative and practical concerns at stake — and do so in a privacy-protective way. This article analyzes the current state of affairs, highlights the urgent need for a new approach, and suggests a way forward, pursuant to which nations would be able to directly access data from U.S.-based providers when specified procedural and substantive standards are met. The alternative is a Balkanized Internet and a race to the bottom, with every nation unilaterally seeking to access sought-after data, companies increasingly caught between conflicting laws, and privacy rights minimally protected, if at all.

Author

Jennifer Daskal is is an Associate Professor at American University Washington College of Law. She teaches and writes in the fields of criminal law, national security law, and constitutional law, and is on academic leave from 2016-2017, working as an Open Society Institute Fellow on a project related to cross-border data flows and privacy.

From 2009-2011, Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice and, among other things, served on the Secretary of Defense and Attorney General-led Detention Policy Task Force. Prior to joining DOJ, she was the senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff. She spent two years before joining WCL's faculty as a national security law fellow and adjunct professor at Georgetown Law Center.

Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar. Recent publications include The Un-Territoriality of Data, 326 Yale L.J. 326 (2015); Pre-Crime Restraints: The Explosion of Targeted, Non-Custodial Prevention, 99 Cornell L. Rev. 327 (2014); After the AUMF, 5 Harvard Nat'l Sec. L. J. 115 (2014) (co-authored with Steve Vladeck); and The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone, 171 Penn. L. Rev. 1165 (2013). Daskal has published op-eds in the New York Times, Washington Post, International Herald Tribune, L.A. Times, and Salon.com, and she has appeared on BBC, C-Span, CNN, MSNBC, and NPR, among other media outlets. She is an Executive Editor of and regular contributor to the Just Security blog.

Accountable Algorithms

Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu

University of Pennsylvania Law Review, Vol. 165, Forthcoming (2017)
Fordham Law Legal Studies Research Paper No. 2765268
Available at SSRN: https://ssrn.com/abstract=2765268

Executive Summary

Many important decisions historically made by people are now made by computers. Algorithms count votes, approve loan and credit card applications, target citizens or neighborhoods for police scrutiny, select taxpayers for an IRS audit, grant or deny immigration visas, and more.

The accountability mechanisms and legal standards that govern such decision processes have not kept pace with technology. The tools currently available to policymakers, legislators, and courts were developed to oversee human decision-makers and often fail when applied to computers instead: for example, how do you judge the intent of a piece of software? Additional approaches are needed to make automated decision systems — with their potentially incorrect, unjustified or unfair results — accountable and governable. This Article reveals a new technological toolkit to verify that automated decisions comply with key standards of legal fairness.

We challenge the dominant position in the legal literature that transparency will solve these problems. Disclosure of source code is often neither necessary (because of alternative techniques from computer science) nor sufficient (because of issues analyzing code) to demonstrate the fairness of a process. Furthermore, transparency may be undesirable, such as when it permits tax cheats or terrorists to game the systems determining audits or security screening, or when it discloses private or protected information.

The central issue is how to assure the interests of citizens, and society as a whole, in making these processes more accountable. This Article argues that technology is creating new opportunities — more subtle and flexible than total transparency — to design decision-making algorithms so that they better align with legal and policy objectives. Doing so will improve not only the current governance of algorithms, but also — in certain cases — the governance of decision-making in general. The implicit (or explicit) biases of human decision-makers can be difficult to find and root out, but we can peer into the "brain" of an algorithm: computational processes and purpose specifications can be declared prior to use and verified afterwards.

The technological tools introduced in this Article apply widely. They can be used in designing decision-making processes from both the private and public sectors, and they can be tailored to verify different characteristics as desired by decision-makers, regulators, or the public. By forcing a more careful consideration of the effects of decision rules, they also engender policy discussions and closer looks at legal standards. As such, these tools have far-reaching implications throughout law and society.

Authors

Joshua A. Kroll is an Engineer working on cryptography and Internet security at the web performance and security company Cloudflare. He is also an affiliate of the Center for Information Technology Policy at Princeton University, where he studies the relationship between computer systems and human governance of those systems, with a special focus on accountability. His previous work spans cryptography, software security, formal methods, Bitcoin, and cybersecurity policy. He holds a PhD in Computer Science from Princeton University, where he received the National Science Foundation Graduate Research Fellowship in 2011.

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.*

Solon Barocas is a Post Doc Researcher in the New York City Lab of Microsoft Research. He focuses on the ethics of machine learning, particularly applications that affect people's life chances and their everyday experiences on online platforms. His research explores issues of fairness in machine learning, methods for bringing accountability to automated decision-making, the privacy implications of inference, and the role that privacy plays in mitigating economic inequality. Solon was previously a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. He completed his doctorate in the Department of Media, Culture, and Communication at New York University, where he remains a Visiting Scholar at the Center for Urban Science + Progress and an affiliate of the Information Law Institute. Solon also routinely works with the Data & Society Research Institute, where he is an affiliate as well.

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.

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 PoParis. 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.

David G. Robinson is Principal and co-founder of Upturn, based in Washington DC. Upturn works to give people a meaningful voice in how digital technology shapes their lives, so that technology can promote the dignity and well-being of all people. David leads Upturn's efforts on the civil rights impact of automated predictions in criminal justice. David is also Adjunct Professor of Law at Georgetown University Law Center, where in the spring 2017 semester he will teach a seminar he proposed and designed on the subject of "Governing Automated Decisions.

Harlan Yu is a principal at Upturn, based in Washington DC. Upturn works alongside social justice leaders to shape the impact of new technologies on people's lives. Recently, Harlan has been working closely with major civil rights organizations to examine law enforcement's use of body-worn cameras and other emerging police technologies. Harlan holds a Ph.D. in computer science from Princeton University and has extensive experience working at the intersection of technology and policy. He is a Non-Residential Fellow at the Center for Internet and Society at Stanford Law School. He has worked at Google in both engineering and public policy roles, at the Electronic Frontier Foundation as a technologist, and at the U.S. Department of Labor.

Privacy of Public Data

Kirsten Martin and Helen Nissenbaum

Available at SSRN: https://ssrn.com/abstract=2875720

Executive Summary

The construct of an information dichotomy has played a defining role in regulating privacy: information deemed private or sensitive typically earns high levels of protection, while lower levels of protection are accorded to information deemed public or non-sensitive. Challenging this dichotomy, the theory of contextual integrity associates privacy with complex typologies of information, each connected with respective social contexts. Moreover, it contends that information type is merely one among several variables that shape people's privacy expectations and underpin privacy's normative foundations. Other contextual variables include key actors — information subjects, senders, and recipients — as well as the principles under which information is transmitted, such as whether with subjects' consent, as bought and sold, as required by law, and so forth. Prior work revealed the systematic impact of these other variables on privacy assessments, thereby debunking the defining effects of so-called private information.

In this paper, we shine a light on the opposite effect, challenging conventional assumptions about public information. The paper reports on a series of studies, which probe attitudes and expectations regarding information that has been deemed public. Public records established through the historical practice of federal, state, and local agencies, as a case in point, are afforded little privacy protection, or possibly none at all. Motivated by progressive digitization and creation of online portals through which these records have been made publicly accessible our work underscores the need for more concentrated and nuanced privacy assessments, even more urgent in the face of vigorous open data initiatives, which call on federal, state, and local agencies to provide access to government records in both human and machine readable forms. Within a stream of research suggesting possible guard rails for open data initiatives, our work, guided by the theory of contextual integrity, provides insight into the factors systematically shaping individuals' expectations and normative judgments concerning appropriate uses of and terms of access to information.

Using a factorial vignette survey, we asked respondents to rate the appropriateness of a series of scenarios in which contextual elements were systematically varied; these elements included the data recipient (e.g. bank, employer, friend,.), the data subject, and the source, or sender, of the information (e.g. individual, government, data broker). Because the object of this study was to highlight the complexity of people's privacy expectations regarding so-called public information, information types were drawn from data fields frequently held in public government records (e.g. voter registration, marital status, criminal standing, and real property ownership).

Our findings are noteworthy on both theoretical and practical grounds. In the first place, they reinforce key assertions of contextual integrity about the simultaneous relevance to privacy of other factors beyond information types. In the second place, they reveal discordance between truisms that have frequently shaped public policy relevant to privacy. For example,

- Ease of accessibility does not drive judgments of appropriateness. Thus, even when respondents deemed information easy to access (marital status) they nevertheless judged it inappropriate ("Not OK") to access this information under certain circumstances.
- Even when it is possible to find certain information in public records, respondents cared about the immediate source of that information in judging whether given data flows were appropriate. In particular, no matter that information in question was known to be available in public records, respondents deemed inappropriate all circumstances in which data brokers were the immediate source of information.
- Younger respondents (under 35 years old) were more critical of using data brokers and online government records as compared with the null condition of asking data subjects directly, debunking conventional wisdom that "digital natives" are uninterested in privacy.

One immediate application to public policy is in the sphere of access to records that include information about identifiable or reachable individuals. This study has shown that individuals have quite strong normative expectations concerning appropriate access and use of information in public records that do not comport with the maxim, "anything goes." Furthermore, these expectations are far from idiosyncratic and arbitrary. Our work calls for approaches to providing access that are more judicious than a simple on/off spigot. Complex information ontologies, credentials of key actors (i.e. sender and recipients in relation to data subject), and terms of access – even lightweight ones – such as, identity or role authentication, varying privilege levels, or a commitment to limited purposes may all be used to adjust public access to align better with legitimate privacy expectations. Such expectations should be systematically considered when crafting policies around public records and open data initiatives.

Authors

Kirsten Martin is an assistant professor of strategic management & public policy at the George Washington University's School of Business. She is the principle investigator on a three-year grant from the National Science Foundation to study online privacy. Martin is also a member of the advisory board of the Future Privacy Forum and the Census Bureau's National Advisory Committee for her work on privacy and the ethics of "big data." Martin has published academic papers in Journal of Business Ethics, First Monday, Business and Professional Ethics Journal, and Ethics and Information Technology and is co-author of the textbook Business Ethics: A managerial approach. She has written teaching cases for the Business Roundtable Institute for Corporate Ethics including cases on Google in China as well as Bailouts and Bonuses on the financial crisis. She is regularly asked to speak on privacy and the ethics of big data.

Martin earned her BS in engineering from the University of Michigan and her MBA and PhD from the University of Virginia's Darden Graduate School of Business. Her research interests center on online privacy, corporate responsibility, and stakeholder theory.

Before beginning her academic career, Martin worked at Sprint Telecommunications developing corporate strategy and Internet solutions. She also provided information system consulting services for Anderson Consulting (currently Accenture) to clients in the coal, pharmaceutical, telecommunication, and oil and gas industries.

Helen Nissenbaum is Professor of Media, Culture, and Communication, and Computer Science, at New York University, where she is also Director of the Information Law Institute. Her eight books include Obfuscation: A User's Guide for Privacy and Protest, with Finn Brunton (MIT Press, 2015), Values at Play in Digital Games, with Mary Flanagan (MIT Press, 2014), and Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford, 2010). Her research has been published in journals of philosophy, politics, law, media studies, information studies, and computer science. Grants from the National Science Foundation, Air Force Office of Scientific Research, and the U.S. Department of Health and Human Services Office of the National Coordinator have supported her work on privacy, trust online, and security, as well as studies of values embodied in design, search engines, digital games, facial recognition technology, and health information systems.

Recipient of the 2014 Barwise Prize of the American Philosophical Association, Prof. Nissenbaum has contributed to privacy-enhancing software, including TrackMeNot (for protecting against profiling based on Web search) and AdNauseam (protecting against profiling based on ad clicks). Both are free and freely available.

Nissenbaum holds a Ph.D. in philosophy from Stanford University and a B.A. (Hons) from the University of the Witwatersrand. Before joining the faculty at NYU, she served as Associate Director of the Center for Human Values at Princeton University.

Risk and Anxiety: A Theory of Data Breach Harms

Daniel J. Solove and Danielle Keats Citron

Available at SSRN: http://ssrn.com/abstract=2885638

Executive Summary

In lawsuits about data breaches, the issue of harm has confounded courts. Harm is central to whether plaintiffs have standing to sue in federal court and whether plaintiffs have viable claims in tort or contract. Plaintiffs have argued that data breaches create a risk of future injury from identity theft or fraud and that breaches cause them to experience anxiety about this risk. Courts have been reaching wildly inconsistent conclusions on the issue of harm, with most courts dismissing data breach lawsuits for failure to allege harm. A sound and compelling approach to harm has yet to emerge, resulting in a lack of consensus among courts and a rather incoherent jurisprudence.

Two U.S. Supreme Court cases within the past five years have contributed significantly to this tortured state of affairs. In 2013, the Court in *Clapper v. Amnesty International* concluded that fear and anxiety about surveillance — and the cost of taking measures to protect against it — were too speculative to constitute "injury in fact" for standing. The Court emphasized that injury must be "certainly impending" to be recognized. This past term, the U.S. Supreme Court in *Spokeo v. Robins* issued an opinion aimed at clarifying the harm required for standing in a case involving personal data. But far from providing guidance, the opinion fostered greater confusion. What the Court made clear, however, was that "intangible" injury, including the "risk" of injury, could be sufficient to establish harm.

Little progress has been made to harmonize this troubled body of law, and there is no coherent theory or approach. In this Article, we examine why courts have struggled when dealing with harms caused by data breaches. We contend that the struggle stems from the fact that data breach harms there are intangible, risk-oriented, and diffuse. Although these characteristics have been challenging to courts in the past, courts have, in fact, been recognizing harms with these characteristics in other areas of law.

We argue that many courts are far too dismissive of certain forms of data breach harm. In many instances, courts should be holding that data breaches cause cognizable harm. We explore why courts struggle to recognize data breach harms and how existing foundations in the law should be used by courts to recognize such harm. We demonstrate how courts can assess risk and anxiety in a concrete and coherent way.

Authors

Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also the founder of TeachPrivacy, a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations. An internationally-known expert in privacy law, Solove has been interviewed and quoted by the media in several hundred articles and broadcasts, including the New York Times, Washington Post, Wall Street Journal, USA Today, Chicago Tribune, the Associated Press, ABC, CBS, NBC, CNN, and NPR.

He has written numerous books including Nothing to Hide: The False Tradeoff Between Privacy and Security (Yale 2011), Understanding Privacy (2008), The Future of Reputation: Gossip, Rumor, and Privacy on the Internet (Yale 2007), and The Digital Person: Technology and Privacy in the Information Age (NYU 2004). He has also written several textbooks including Information Privacy Law (Aspen, 5th ed. 2015), Privacy Law Fundamentals (IAPP, 3d ed. 2015), Privacy and the Media (Aspen, 2d ed. 2015), Privacy, Law Enforcement, and National Security (Aspen, 1st ed. 2015), Consumer Privacy and Data Protection (Aspen, 1st ed. 2015), and Privacy, Information, and Technology (Aspen Publishing, 3rd ed. 2012). All of these books were co-authored with Paul M. Schwartz.

Additionally, Professor Solove has written more than 50 law review articles in the Harvard Law Review, Yale Law Journal, Stanford Law Review, Columbia Law Review, NYU Law Review, Michigan Law Review, U. Pennsylvania Law Review, U. Chicago Law Review, California Law Review, Duke Law Journal, and many others. He has also written shorter works for Wired, Scientific American, the Washington Post, and several other magazines and periodicals.

Danielle Keats Citron is the Morton & Sophia Macht Professor of Law at the University of Maryland Francis King Carey School of Law. Her work focuses on information privacy, cyber law, automated systems, and civil rights. She received the 2005 "Teacher of the Year" award.

Professor Citron is the author of Hate Crimes in Cyberspace (Harvard University Press 2014). Cosmopolitan and Harper's Bazaar nominated her book as one of the "Top 20 Best Moments for Women" in 2014; Boston University Law Review held an online symposium on her book in 2015. Her current work focuses on the privacy policymaking of state attorneys general. Professor Citron's scholarship has appeared, or is forthcoming, in Boston University Law Review (twice), California Law Review, George Washington Law Review, Hastings Law Journal, Michigan Law Review (twice), Minnesota Law Review, Notre Dame Law Review, Southern California Law Review, Washington University Law Review, Washington Law Review (twice), Washington & Lee Law Review, U.C. Davis Law Review, and others. Her opinion pieces have been featured in The Atlantic, New York Times, TIME, CNN, Guardian UK, New Scientist, and Slate. She has appeared on National Public Radio, HBO's John Oliver Show and the New York Times video series. She is a technology contributor at Forbes.com and a member of Concurring Opinions.

Student Paper

Online Tracking: A 1-million-site Measurement and Analysis

Steven Englehardt and Arvind Narayanan

Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security
Available at SSRN: http://dl.acm.org/citation.cfm?id=2976749.2978313

Executive Summary

We present the largest and most detailed measurement of online tracking conducted to date, based on a crawl of the top 1 million websites. On each site we measure 15 types of tracking, ranging from traditional cookie-based tracking to newer techniques such as fingerprinting. We show how trackers are readily adopting new browser features to make tracking more persistent, examine the exchange of identifiers between trackers (i.e. cookie syncing), and show how well privacy tools protect consumers.

Cookie-based tracking has been well-studied and is known to be pervasive on the modern web. Browser vendors, privacy advocates, and industry self-regulatory bodies have developed a set of norms and advice to help give users control over tracking with cookies, i.e. by allowing users to clear cookies, use opt-out cookies, or outright block third-party cookies.

Trackers are adopting and developing techniques to track users which don't rely on cookies, we present several of such techniques which were never before measured in the wild. Rather than identifying users with a file on their computer, trackers can identify users by the "fingerprint", or set of properties, of the user's browser. Unlike cookies, users do not have the ability to effectively control their browser's fingerprint. Browser features often thought of as privacy-preserving by consumers, such as incognito or private browsing mode, are ineffective at preventing fingerprinting. In our paper we enumerate several fingerprinting techniques and quantify their adoption on the web.

We show that, despite a large number of trackers, relatively few companies have a tracking presence on a meaningful fraction of the web. The tracking practices of these companies are likely to affect nearly all internet users, and can help set norms for acceptable and unacceptable tracking practices. On the other hand, we also show that the top trackers share their identifiers frequently, amplifying the effects of bad practices, even if carried out by third-parties with a relatively small tracking presence. We show how news sites contain significantly more trackers than many other categories of sites, including adult, reference, and science websites.

Many consumers have turned to third-party privacy tools to prevent tracking, primarily choosing those which block third-party trackers from loading on a site. Examples include AdBlock Plus, Ghostery, Disconnect, and Privacy Badger. In our paper we show how these tools are effective at preventing traditional cookie-based blocking but fail to block many of the fingerprinting scripts we discovered on the web. This further shows that consumers have less control of fingerprinting-based tracking, even when they take steps to protect their privacy.

This measurement is made possible by our open-source web privacy measurement tool, OpenWPM, which uses automated Firefox browsers to crawl the web. Both our work, and the measurement work of others, has repeatedly uncovered the misuse of tracking and consumer privacy violations on the web. We envision an ecosystem that incentivizes trackers to be transparent to their users in techniques used to track and readily supports auditing by privacy researchers and regulators alike.

Authors

Steven Englehardt is a computer science PhD candidate at Princeton University and a graduate research fellow at the Center for Information Technology Policy. His area of research is web privacy and security, with a focus on online tracking measurement. Mr. Englehardt has published numerous studies of the online tracking ecosystem at top computer science conferences, and has worked with regulators, non-profits, standards groups, and companies to improve the state of privacy online. Mr. Englehardt is the primary maintainer of OpenWPM, an open web privacy measurement platform. He previously worked on the security engineering team at Mozilla and received his B.Sc. in Physics from Stevens Institute of Technology.

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

Honorable Mentions

Biometric Cyberintelligence and the Posse Comitatus Act

by Professor Margaret Hu, Washington & Lee University School of Law

Emory Law Journal, Forthcoming (2017)
Available at SSRN: https://ssrn.com/abstract=2886575

Executive Summary

This Article addresses the rapid growth of what the military and intelligence community refer to as "biometric-enabled intelligence." This newly emerging intelligence system is reliant upon biometric databases — for example, digitalized collections of scanned fingerprints and irises, digital photographs for facial recognition technology, and DNA. This Article introduces the term "biometric cyberintelligence" to describe more accurately the manner in which this new tool is dependent upon cybersurveillance and big data's mass-integrative systems. This Article argues that the Posse Comitatus Act of 1878, designed to limit the deployment of federal military resources in the service of domestic policies, may be impotent in light of the growth of cybersurveillance. Maintaining strict separation of data between military and intelligence operations on the one hand, and civilian, homeland security, and domestic law enforcement agencies on the other hand, is increasingly difficult as cooperative data sharing increases. The Posse Comitatus Act and constitutional protections such as the Fourth Amendment's privacy jurisprudence, therefore, must be reinforced in the digital age in order to appropriately protect citizens from militarized cyberpolicing, i.e., the blending of military/foreign intelligence tools and operations and homeland security/domestic law enforcement tools and operations. The Article concludes that, as of yet, neither statutory nor constitutional protections have evolved sufficiently to cover the unprecedented surveillance harms posed by the migration of biometric cyberintelligence from foreign to domestic use.

Ambiguity in Privacy Policies and the Impact of Regulation

by Professors Joel R. Reidenberg, Fordham University School of Law, Jaspreet Bhatia, Carnegie Mellon University, Travis Breaux, Carnegie Mellon University, and Thomas B. Norton, Fordham University

Journal of Legal Studies, Forthcoming
Fordham Law Legal Studies Research Paper No. 2715164
Available at SSRN: https://ssrn.com/abstract=2715164

Executive Summary

Website privacy policies often contain ambiguous language that undermines the purpose and value of privacy notices for site users. This paper compares the impact of different regulatory models on the ambiguity of privacy policies in multiple online sectors. First, the paper develops a theory of vague and ambiguous terms. Next, the paper develops a scoring method to compare the relative vagueness of different privacy policies. Then, the theory and scoring are applied using natural language processing to rate a set of policies. The ratings are compared against two benchmarks to show whether government-mandated privacy disclosures result in notices less ambiguous than those emerging from the market. The methodology and technical tools can provide companies with mechanisms to improve drafting, enable regulators to easily identify poor privacy policies and empower regulators to more effectively target enforcement actions.

Data-Driven Discrimination at Work

by Professor Pauline Kim, Washington University in Saint Louis School of Law

William & Mary Law Review, Forthcoming (2017)
Washington University in St. Louis Legal Studies Research Paper No. 16-12-01
Available at SSRN: https://ssrn.com/abstract=2801251

Executive Summary

A data revolution is transforming the workplace. Employers are increasingly relying on algorithms to decide who gets interviewed, hired, or promoted. Although data algorithms can help to avoid biased human decision-making, they also risk introducing new sources of bias. Algorithms built on inaccurate, biased, or unrepresentative data can produce outcomes biased along lines of race, sex, or other protected characteristics. Data mining techniques may cause employment decisions to be based on correlations rather than causal relationships; they may obscure the basis on which employment decisions are made; and they may further exacerbate inequality because error detection is limited and feedback effects compound the bias. Given these risks, I argue for a legal response to classification bias—a term that describes the use of classification schemes, like data algorithms, to sort or score workers in ways that worsen inequality or disadvantage along the lines or race, sex, or other protected characteristics. Addressing classification bias requires fundamentally rethinking antidiscrimination doctrine. When decision-making algorithms produce biased outcomes, they may seem to resemble familiar disparate impact cases; however, mechanical application of existing doctrine will fail to address the real sources of bias when discrimination is data-driven. A close reading of the statutory text suggests that Title VII directly prohibits classification bias. Framing the problem in terms of classification bias leads to some quite different conclusions about how to apply the antidiscrimination norm to algorithms, suggesting both the possibilities and limits of Title VII's liability-focused model.

Friending the Privacy Regulators

by Professor William McGeveran, University of Minnesota Law School

58 Arizona Law Review 2016
Minnesota Legal Studies Research Paper No. 16-26
Available at SSRN: https://ssrn.com/abstract=2820683

Executive Summary

According to conventional wisdom, data privacy regulators in the European Union are unreasonably demanding, while their American counterparts are laughably lax. Many observers further assume that any privacy enforcement without monetary fines or other punishment is an ineffective "slap on the wrist." This Article demonstrates that both of these assumptions are wrong. It uses the simultaneous 2011 investigation of Facebook's privacy practices by regulators in the United States and Ireland as a case study. These two agencies reached broadly similar conclusions, and neither imposed a traditional penalty. Instead, they utilized "responsive regulation," where the government emphasizes less adversarial techniques and considers formal enforcement actions more of a last resort. When regulators in different jurisdictions employ this same responsive regulatory strategy, they blur the supposedly sharp distinctions between them, whatever may be written in their respective constitutional proclamations or statute books. Moreover, "regulatory friending" techniques work effectively in the privacy context. Responsive regulation encourages companies to improve their practices continually, it retains flexibility to deal with changing technology, and it discharges oversight duties cost-efficiently, thus improving real-world data practices.

Thank you to our 2016 Advisory Board Judges and Reviewers

Submissions received numeric rankings from a diverse team of academics, consumer advocates, and industry privacy professionals from the FPF Advisory Board, with each submission being evaluated for originality; overall quality of writing; and applicability to policy making. For more information, visit fpf.org/privacy-papers-for-policy-makers/.

Jules Polonetsky
CEO
Future of Privacy Forum

Christopher Wolf
Founder and Board Chair
Future of Privacy Forum

Mary Culnan
Professor Emeritus
Bentley University
FPF Board Vice President

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

Virginia Lee
Director, Privacy
Starbucks

Advisory Board Reviewers

Projjol Banerjea
zeotap

Eduard Bartholme
Call For Action

Allison Cohen
Toyota Motor Sales, USA, Inc.

Heather Federman
Macy's

Olga Garcia-Kaplan
Novitex Enterprise Solutions

Lauren Gelman
BlurryEdge Strategies

Rita Heimes
International Association of Privacy Professionals

Mike Hintze
Hintze Law

Sarah Holland
Google

Susan Israel
Loeb & Loeb, LLP

Manoj Lamba
ClassDojo

David Medine
Consultative Group to Assist the Poor

Catherine Tucker
MIT Sloan School of Management

Susannah Wesley
Edelman

Heather West
Mozilla

Michael Zimmer
University of Wisconsin, Milwaukee School of Information Studies

PRIVACY PAPERS FOR POLICYMAKERS 2016

Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms and workable business practices. This 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