PRIVACY PAPERS FOR POLICYMAKERS

2017

This material is based upon work supported by the National Science Foundation under Grant No. 1654085.

FUTURE OF PRIVACY FORUM

February 27, 2018

We are pleased to introduce FPF's eighth 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. A committee of Reviewers and Judges from 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 international data protection officials.

This year's winning papers grapple with a range of issues critical to regulators. Some of the papers analyze broader conceptions of how regulators, markets, and society at large consider different conceptions of privacy, prompting the reader to think critically about assumed paradigms. One paper argues that the definition of "public information" is unsettled and hazy, meriting a more rigorous analysis of the definition in legal determinations and policy discourse (Hartzog); another argues for a coalesced understanding of how privacy is conceptualized between the rights-based model in Europe and the marketplace-based model in the United States (Schwartz & Peifer).

Other papers offer key recommendations for how to best attack precise concerns in privacy law and policy. One paper argues that the role of technology surveillance companies must be curtailed to facilitate meaningful transparency over how that technology is used by police departments (Joh). Others propose mechanisms to prevent the disproportionate effects of secondary health data usage on vulnerable populations (Konnoth), and taxonomize design and policy strategies for diminishing discriminatory mechanisms in online platforms (Levy & Barocas). Striking the balancing between foundational analysis and narrower proposals, another paper contextualizes the role of artificial intelligence in law and policy, and proposes how relevant governance strategies should develop (Calo).

Following the introduction of our Student Paper Award last year, we are proud to continue highlighting student work by honoring another stellar article. The winning paper (Gupta) offers an insightful approach to the marketplace forces that shape the adoption of privacy and security standards, highlighting the role of individual actors in driving trends. As novel issues in law and technology continue to present new challenges to policymakers, we want to support the students who will one day shape important debates.

We thank the National Science Foundation for their support of this project. And as always, we thank the scholars, advocates, and Advisory Board members who are engaged with us to explore the future of privacy.

Sincerely,

Christopher Wolf
Of Counsel, Hogan Lovells LLP
Chairman, FPF Board of Directors

Jules Polonetsky
CEO

Future of Privacy Forum Advisory Board

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

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

Sharon Anolik
President
Privacy Panacea

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

Justin Antonipillai
Chief Executive Officer
WireWheel

Jocelyn Aqua
Principal, Regulatory Privacy & Cybersecurity
PricewaterhouseCoopers LLP

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

Stephen Balkam
Chief Executive Officer
Family Online Safety Institute

Kenneth Bamberger
The Rosalinde and Arthur Gilbert Foundation Professor of Law
University of California, Berkeley School of Law

Kabir Barday
Chief Executive Officer
OneTrust

Malita Barkataki
Privacy Compliance Director
Oath

Inna Barmash
General Counsel
Amplify Education, Inc.

Nancy Bell
Senior Manager, External Affairs
Fiat Chrysler Automobiles

Lael Bellamy
Chief Privacy Officer
The Weather Company/IBM Corporation

Alisa Bergman
Chief Privacy Officer
Adobe Systems Inc.

Elise Berkower (1957-2017)
Associate General Counsel
The Nielsen Company

Debra Berlyn
President
Consumer Policy Solutions
Treasurer, FPF Board of Directors

Andrew Bloom
Chief Privacy Officer
McGraw-Hill Education

Bruce Boyden
Assistant Professor of Law
Marquette University Law School

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

Phyllis Turner-Brim
Vice President, Assistant General Counsel
IP and Technology
Starbucks

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

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

Bill Brown
Senior Vice President & Chief Information Security Officer
Houghton Mifflin Harcourt

Stephanie Bryson
Senior Public Policy Associate
Uber Technologies, Inc.

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

Ryan Calo
Associate Professor of Law
University of Washington School of Law

Sam Castic
Senior Counsel & Director, Privacy
Nordstrom Inc.

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

Darlene Cedres
Chief Privacy Officer
Samsung Electronics America

Mary Chapin
Chief Legal Officer
National Student Clearinghouse

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

Allison Cohen
Managing Counsel
Toyota Motor North America, Inc.

Sheila Colclasure
Global Chief Data Ethics Officer
Acxiom Corporation

Maureen Cooney
Head of Privacy
Sprint

Barbara Cosgrove
Chief Privacy Officer
Workday

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

Mary Culnan
Professor Emeritus
Bentley University
Vice Chairman, FPF Board of Directors
Board President, FPF Education & Innovation Foundation
FPF Senior Fellow

Simon Davies
Founder
Privacy International

Alyssa Harvey Dawson
General Counsel
Sidewalk Labs

Laurie Dechery
Associate General Counsel
Lifetouch, Inc.

Michelle DeMooy
Director, Privacy & Data Project
Center for Democracy & Technology

Michelle Dennedy
Vice President, Chief Privacy Officer
Cisco Systems Inc.

Carol DiBattiste
General Counsel & Chief Privacy and People Officer
comScore

Travis Dodd
Chief Privacy Officer and Associate General Counsel
AARP

Erin Egan
Vice President & Chief Privacy Officer, Policy,
Facebook, Inc.

Keith Enright
Director, Global Privacy Legal
Google

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
Professor of Law
Washington & Lee University

Denise Farnsworth
Chief Privacy Officer and Senior Corporate Counsel
Jazz Pharmaceuticals

Teresa Troester-Falk
Chief Global Privacy Strategist
Nymity Inc.

H. Leigh Feldman
Managing Director, Global Chief Privacy Officer
Citigroup

Lori Fink
Senior Vice President, Assistant General Counsel & Chief Privacy Officer
AT&T

Leigh Freund
President & CEO
Network Advertising Initiative

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

Deborah Gertsen
Lead Policy Counsel
Ford Motor Company

John Gevertz
Chief Privacy Officer
Visa Inc.

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

Scott Goss
Vice President and Privacy Counsel
Qualcomm

Justine Gottshall
Chief Privacy Officer
Signal

John Grant
Civil Liberties Engineer
Palantir Technologies

Kimberly Gray
Chief Privacy Officer, Global
IQVIA

Simon Hania
Vice President, Privacy & Security
TomTom International B.V.

Ghita Harris-Newton
Deputy General Counsel &
Chief Privacy Officer
Quantcast Corp

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University School of Law

Ben Hayes
Chief Privacy Officer
The Nielsen Company

Eric Heath
Chief Privacy Officer
Ancestry

Rita Heimes
Research Director and
Data Protection Officer
IAPP - International Association of Privacy Professionals

Eileen Hershenov
General Counsel
Wikimedia Foundation

Beth Hill
General Counsel, Chief Compliance Officer
Ford Direct

Dennis Hirsch
Professor of Law, Director,
Program on Data and Governance
Ohio State University

Alex Hoehn-Saric
Senior Vice President, Government Relations
Charter Communications

David Hoffman
Associate General Counsel and Global Privacy Officer
Intel Corporation

Lara Kehoe Hoffman
Global Director, Data Privacy and Security
Netflix, Inc.

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

Jane Horvath
Senior Director of Global Privacy
Apple, Inc.

Margaret Hu
Assistant Professor of Law
Washington & Lee University

Sandra Hughes
CEO and President
Sandra Hughes Strategies
Secretary, FPF Board of Directors

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

Brian Huseman
Director, Public Policy
Amazon.com

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

Michael Kaiser
Executive Director
National Cyber Security Alliance

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

Cameron Kerry
Senior Counsel
Sidley Austin LLP

Maria Kirby
Assistant Vice President of Regulatory Affairs and Associate General Counsel
CTIA-The Wireless Association

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

Michael Lamb
Global Chief Privacy Officer
RELX Group

Yoomi Lee
Vice President, Enterpise Data Strategy
American Express

Gerard Lewis
Senior Vice President & Deputy General Counsel
Comcast

Harry Lightsey
Executive Director, Global Connected Customer, Public Policy
General Motors Company

Brendon Lynch
Chief Privacy Officer
Microsoft

Mark MacCarthy
Senior Vice President, Public Policy
Software & Information Industry Association

Knut Mager
Head Data Global Privacy
Novartis International AG

Larry Magid
Chief Executive Officer
Connect Safely

Kirsten Martin
Assistant Professor, Strategic Management and Public Policy
The George Washington University - School of Business

Lisa Martinelli
Vice President & Chief Privacy Officer
Highmark Health

Michael McCullough
Chief Privacy Officer & Vice President, Enterprise Information Management & Privacy
Macy's Inc.

William McGeveran
Associate Professor
University of Minnesota Law School

David Medine
Consultant
Consultative Group to Assist the Poor

Scott Meyer
Chief Executive Officer & Founder
Evidon, Inc.

Douglas Miller
Vice President and Global Privacy Leader
Oath

John Miller
Vice President for Global Policy and Law, Privacy and Security
Information Technology Industry Council

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Jill Nissen
Founder & Principal
Nissen Consulting

Tiffany Morris Palazzo
General Counsel and Vice President of Global Privacy
Lotame Solutions, Inc.

Harriet Pearson
Partner
Hogan Lovells LLP

Future of Privacy Forum Advisory Board (continued)

Bilyana Petkova
Assistant Professor,
International and European Law, Faculty of Law, Maastricht University

Peter Petros
General Counsel & Global Privacy Officer
Edelman

Kalinda Raina
Head of Global Privacy
LinkedIn Corporation

Katie Ratté
Associate General Counsel,
Privacy & Global Public Policy
The Walt Disney Company

Alan Raul
Partner
Sidley Austin LLP
FPF Board of Directors

Joel 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

Amy Reitz
General Manager
Hobsons

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

Susan Rohol
Global Intellectual Property and Privacy Policy Director
Nike, Inc.

Mila Romanoff
Privacy and Data Protection Legal Officer
United Nations Global Pulse

Shirley Rooker
President
Call for Action

Michelle Rosenthal
Senior Corporate Counsel
T-Mobile

Alexandra Ross
Senior Global Privacy and Data Security Counsel
Autodesk, Inc.

Neal Schroeder
Vice President Internal Audit, Corporate Business Ethics Officer
Enterprise Holdings

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
Professor of Philosophy
Rochester Institute of Technology
FPF Senior Fellow

Linda Sherry
Director, National Priorities
Consumer Action

Julia Shullman
Senior Director, Deputy General Counsel,
Commercial and Privacy
AppNexus

Meredith Sidewater
Senior Vice President and General Counsel
LexisNexis Risk Solutions

Dale Skivington
Vice President Global Compliance and Chief Privacy Officer
Dell, Inc.

Will Smith
Executive Chairman and Chief Strategy Officer
Euclid Analytics

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

Cindy Southworth
Executive Vice President
National Network to End Domestic Violence

Gerard Stegmaier
Adjunct Professor, Antonin Scalia Law School
George Mason University

Amie Stepanovich
U.S Policy Manager
Access Now

JoAnn Stonier
Executive Vice President, 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

Greg Stuart
Chief Executive Officer
Mobile Marketing Association

Lisa Sullivan
Vice President, Deputy General Counsel
Intuit

Peter Swire
Nancy J. & Lawrence P. Huang Professor of Law & Ethics, Scheller College of Business
Georgia Institute of Technology
FPF Senior Fellow

Scott Taylor
Vice President, Compliance, Privacy, Big Data and Global Services
Merck & Co., Inc.

Omer Tene
Vice President, Chief Knowledge Officer
IAPP - International Association of Privacy Professionals
FPF Senior Fellow

Adam Thierer
Senior Research Fellow at Mercatus Center
George Mason University

Anne Toth
Head of Data Policy, Center for the Fourth Industrial Revolution
World Economic Forum

Catherine Tucker
Mark Hyman, Jr. Career Development Professor and Associate Professor of Management Science
Massachusetts Institute of Technology

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

David Vladeck
Professor of Law in Civil Procedure
Georgetown University School of Law

Hilary Wandall
General Counsel & Chief Data Governance Officer
TrustArc

Daniel Weitzner
Director and Principal Research Scientist
MIT CSAIL Decentralized Information Group

Kevin Werbach
Associate Professor of Legal Studies & Business Ethics
Wharton School of the University of Pennsylvania

Heather West
Senior Policy Manager
Mozilla Corporation

Janice Whittington
Associate Professor,
Department of Urban Design and Planning
University of Washington

Christopher Wolf
Of Counsel
Hogan Lovells LLP
Chairman, FPF Board of Directors

Nicole Wong
Principal
Nwong Strategies

Christopher Wood
Executive Director & Co-Founder
LGBT Technology Partnership

Heng Xu
Associate Professor, College of Information Sciences and Technology
The Pennsylvania State University

Karen Zacharia
Chief Privacy Officer
Verizon

Elana Zeide
Visiting Assistant Professor, Seton Hall University School of Law

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

List as of January 2018, please send updates about this list to mwright@fpf.org

Table of Contents

Awarded Papers

Artificial Intelligence Policy: A Primer and Roadmap 6
Ryan Calo

Designing Against Discrimination in Online Markets 8
Karen Levy and Solon Barocas

Health Information Equity 10
Craig Konnoth

The Public Information Fallacy 12
Woodrow Hartzog

Transatlantic Data Privacy Law 14
Paul M. Schwartz and Karl-Nikolaus Peifer

The Undue Influence of Surveillance Technology Companies on Policing 16
Elizabeth Joh

Awarded Student Paper

The Market's Law of Privacy: Case Studies in Privacy/Security Adoption 18
Chetan Gupta

Honorable Mentions

Algorithmic Jim Crow 20
Margaret Hu

The Idea of 'Emergent Properties' In Data Privacy: Towards A Holistic Approach 20
Samson Y. Esayas

Public Values, Private Infrastructure and the Internet of Things: The Case of Automobiles 21
Deirdre K. Mulligan and Kenneth A. Bamberger

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.

Artificial Intelligence Policy: A Primer and Roadmap

Ryan Calo
University of California, Davis Law Review, Vol. 51, No.2 (2017)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350

Executive Summary

Talk of artificial intelligence is everywhere. People marvel at the capacity of machines to translate any language and master any game. Others condemn the use of secret algorithms to sentence criminal defendants or recoil at the prospect of machines gunning for blue, pink, and white-collar jobs. Some worry aloud that artificial intelligence will be humankind's "final invention."

This essay, prepared in connection with UC Davis Law Review's 50th anniversary symposium, explains why AI is suddenly on everyone's mind and provides a roadmap to the major policy questions AI raises. The essay is designed to help policymakers, investors, technologists, scholars, and students understand the contemporary policy environment around AI at least well enough to initiate their own exploration. Topics covered include justice and equity, use of force, safety and certification, privacy, taxation, and displacement of labor. The essay also touches briefly on broader systemic questions, such as institutional configuration and expertise, investment and procurement, removing hurdles to accountability, and correcting mental models of AI.

Author

Ryan Calo is the Lane Powell and D. Wayne Gittinger Associate Professor at the University of Washington School of Law. 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 Paul G. Allen School of Computer Science and Engineering. Professor Calo's research on law and emerging technology appears in leading law reviews (California Law Review, University of Chicago Law Review, and Columbia Law Review) and technical publications (MIT Press, Nature, Artificial Intelligence) and is frequently referenced by the mainstream media (NPR, New York Times, Wall Street Journal). Professor Calo serves as an advisor to many organizations, including the AI Now Institute, and is a member of the R Street Institute's board.

Designing Against Discrimination in Online Markets

Karen Levy and Solon Barocas
Berkeley Technology Law Journal, Vol. 32 (Forthcoming 2018)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084502

Executive Summary

Platforms that connect users to one another have flourished online in domains as diverse as transportation, employment, dating, and housing. When users interact on these platforms, their behavior may be influenced by preexisting biases, including tendencies to discriminate along the lines of race, gender, and other protected characteristics. In aggregate, such user behavior may result in systematic inequities in the treatment of different groups. While there is uncertainty about whether platforms bear legal liability for the discriminatory conduct of their users, platforms necessarily exercise a great deal of control over how users' encounters are structured—including who is matched with whom for various forms of exchange, what information users have about one another during their interactions, and how indicators of reliability and reputation are made salient, among many other features. Platforms cannot divest themselves of this power; even choices made without explicit regard for discrimination can affect how vulnerable users are to bias. This article analyzes ten categories of design and policy choices through which platforms may make themselves more or less conducive to discrimination by users. In so doing, it offers a comprehensive account of the complex ways platforms' design choices might perpetuate, exacerbate, or alleviate discrimination in the contemporary economy.

Authors

Karen Levy is an Assistant Professor in the Department of Information Science at Cornell University and associated faculty at Cornell Law School. She researches how law and technology interact to regulate social life, with particular focus on social and organizational aspects of surveillance. Dr. Levy's research analyzes the uses of data collection for social control in various contexts, from long-haul trucking to intimate relationships, with emphasis on inequality and marginalization. She holds a Ph.D. in Sociology from Princeton University and a J.D. from Indiana University Maurer School of Law. Before joining Cornell, she was a postdoctoral fellow at NYU's Information Law Institute and at the Data & Society Research Institute.

Solon Barocas is an Assistant Professor in the Department of Information Science at Cornell University. His current research explores ethical and policy issues in artificial intelligence, particularly fairness in machine learning, methods for bringing accountability to automated decision-making, and the privacy implications of inference. He was previously a Postdoctoral Researcher at Microsoft Research, where he worked with the Fairness, Accountability, Transparency, and Ethics in AI group, as well as a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. Solon 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.

Health Information Equity

Craig Konnoth
University of Pennsylvania Law Review, Vol. 165, Issue 6 (2017)
Available at: http://scholar.law.colorado.edu/articles/701

Executive Summary

In the last few years, numerous Americans' health information has been collected and used for follow-on, secondary research. This research examines correlations between medical conditions, genetic or behavioral profiles, and treatments, to customize medical care to specific individuals. Recent federal legislation and regulations make it easier to collect and use the data of the low-income, unwell, and elderly for this purpose. This would impose disproportionate security and autonomy burdens on these individuals. Those who are well-off and pay out of pocket could effectively exempt their data from the publicly available information pot. This presents a problem which modern research ethics is not well equipped to address. Where it considers equity at all, it emphasizes underinclusion and the disproportionate distribution of research benefits, rather than overinclusion and disproportionate distribution of burdens.

I rely on basic intuitions of reciprocity and fair play as well as broader accounts of social and political equity to show that equity in burden distribution is a key aspect of the ethics of secondary research. To satisfy its demands, we can use three sets of regulatory and policy levers. First, information collection for public research should expand beyond groups having the lowest welfare. Next, data analyses and queries should draw on data pools more equitably. Finally, we must create an entity to coordinate these solutions using existing statutory authority if possible. Considering health information collection at a systematic level—rather than that of individual clinical encounters—gives us insight into the broader role that health information plays in forming personhood, citizenship, and community.

Author

Professor Craig Konnoth's work lies at the intersection of health law and policy, bioethics, civil rights, and technology. His papers consider how health privacy burdens are created and distributed, how medical discourse is used both to enable and harm civil rights and autonomy, and how technology can be used to improve health outcomes. He has examined these issues in in contexts as diverse as religion and biblical counseling, consumer rights and transparency, FDA regulation, and collection of individual data.

Professor Konnoth's publications have appeared in the Yale Law Journal, the Hastings Law Journal, the Penn Law Review, the Iowa Law Review, the online companions to the Penn Law Review & the Washington & Lee Law Review, and as chapters in edited volumes.

Before arriving at the University of Colorado, Craig was a Sharswood and Rudin Fellow at Penn Law School and NYU Medical School, where he taught health information law, health law, and LGBT health law and bioethics. Before that he was the Deputy Solicitor General and the Inaugural Earl Warren Fellow at the California Department of Justice where he litigated primarily before the United States Supreme Court, and also before the California Supreme Court and the Ninth Circuit Court of Appeals. Cases involved the contraceptive mandate in the Affordable Care Act, Sexual Orientation Change Efforts, Facebook privacy policies, and cellphone searches. Before moving into government, Craig was the R. Scott Hitt Fellow in Law & Policy at the Williams Institute at UCLA Law School, where he focused on issues affecting same-sex partners, long term care, and Medicaid coverage issues, and drafted HIV rights legislation. He holds a J.D. from Yale, and an M.Phil. from the University of Cambridge. He clerked for Judge Margaret McKeown of the Ninth Circuit Court of Appeals.

The Public Information Fallacy

Woodrow Hartzog

Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084102

Executive Summary

The concept of privacy in "public" information or acts is a perennial topic for debate. It has given privacy law fits. People struggle to reconcile the notion of protecting information that has been made public with traditional accounts of privacy. As a result, successfully labeling information as public often functions as a permission slip for surveillance and personal data practices. It has also given birth to a significant and persistent misconception — that public information is an established and objective concept.

In this article, I argue that the "no privacy in public" justification is misguided because nobody knows what "public" even means. It has no set definition in law or policy. This means that appeals to the public nature of information and contexts in order to justify data and surveillance practices is often just guesswork. There are at least three different ways to conceptualize public information: descriptively, negatively, or by designation. For example, is the criteria for determining publicness whether it was hypothetically accessible to anyone? Or is public information anything that's controlled, designated, or released by state actors? Or maybe what's public is simply everything that's "not private?"

If the concept of "public" is going to shape people's social and legal obligations, its meaning should not be assumed. Law and society must recognize that labeling something as public is both consequential and value-laden. To move forward, we should focus the values we want to serve, the relationships and outcomes we want to foster, and the problems we want to avoid.

Author

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University, where he teaches privacy and data protection law, policy, and ethics. He holds a joint appointment with the School of Law and the College of Computer and Information Science. Professor Hartzog's work has been published in numerous scholarly publications such as the Yale Law Journal, Columbia Law Review, California Law Review, and Michigan Law Review and popular national publications such as The Guardian, Wired, BBC, CNN, Bloomberg, New Scientist, Slate, The Atlantic, and The Nation. He has testified twice before Congress on data protection issues. His book, Privacy's Blueprint: The Battle to Control the Design of New Technologies, is forthcoming in Spring 2018 from Harvard University Press.

Transatlantic Data Privacy Law

Paul M. Schwartz and Karl-Nikolaus Peifer

Georgetown Law Journal, Vol. 106, Issue 1 (2017)

Available at: https://georgetownlawjournal.org/articles/249/transatlantic-data-privacy-law/pdf

Executive Summary

International flows of personal information are more significant than ever, but differences in transatlantic data privacy law imperil this data trade. The resulting policy debate has led the EU to set strict limits on transfers of personal data to any non-EU country—including the United States—that lacks sufficient privacy protections. Bridging the transatlantic data divide is therefore a matter of the greatest significance.

In exploring this issue, this article analyzes the respective legal identities constructed around data privacy in the EU and the United States. It identifies profound differences in the two systems' images of the individual as bearer of legal interests. The EU has created a privacy culture around "rights talk" that protects its "data subjects." In the EU, moreover, rights talk forms a critical part of the postwar European project of creating the identity of a European citizen. In the United States, in contrast, the focus is on a "marketplace discourse" about personal information and the safeguarding of "privacy consumers." In the United States, data privacy law focuses on protecting consumers in a data marketplace.

This article uses its models of rights talk and marketplace discourse to analyze how the EU and United States protect their respective data subjects and privacy consumers. Although the differences are great, there is a path forward. A new set of institutions and processes can play a central role in developing mutually acceptable standards of data privacy. The key documents in this regard are the General Data Protection Regulation, an EU-wide standard that becomes binding in 2018, and the Privacy Shield, an EU–U.S. treaty signed in 2016. These legal standards require regular interactions between the EU and United States and create numerous points for harmonization, coordination, and cooperation. The GDPR and Privacy Shield also establish new kinds of governmental networks to resolve conflicts. The future of international data privacy law rests on the development of new understandings of privacy within these innovative structures.

Authors

Paul M. Schwartz is a leading international expert on information privacy law. He is Jefferson E. Peyser Professor at the University of California, Berkeley Law School and a director of the Berkeley Center for Law and Technology. Professor Schwarz is the author of many books, including the leading casebook, "Information Privacy Law," and the distilled guide, "Privacy Law Fundamentals," each with Daniel Solove. Schwartz's over fifty articles have appeared in journals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, University of Chicago Law Review and California Law Review.

Professor Schwartz is co-reporter of the American Law Institute's Principles of the Law, Data Privacy. He is a past recipient of the Berlin Prize Fellowship at the American Academy in Berlin and a Research Fellowship at the German Marshall Fund in Brussels. Schwartz is also a recipient of grants from the Alexander von Humboldt Foundation, Fulbright Foundation, and the German Academic Exchange. He is a member of the organizing committee of the Privacy + Security Forum, International Privacy + Security Forum, and Privacy Law Salon. Schwartz publishes on a wide array of privacy and technology topics including cloud computing, financial privacy, European data privacy law, and comparative privacy law.

Karl-Nikolaus Peifer is the Director of the Institute for Media Law and Communications Law of the University of Cologne and Director of the Institute for Broadcasting Law at the University of Cologne. He studied law, economics and romanic languages at the of Universities of Trier, Bonn, Hamburg and Kiel. In 2003 he was appointed to be a judge at the Court of Appeals in Hamm/Germany, and in 2013 at the Court of Appeals in Cologne. He was a Visiting Professor at the University of Illinois in 2009 and at the University of California at Berkeley from 2009 to 2012. In 2011 he was among the experts heard during the sessions of the Parliamentary Commission "Internet und Digital Society." His main fields of research are Intellectual Property and Media Law.

The Undue Influence of Surveillance Technology Companies on Policing

Elizabeth Joh

New York University Law Review Online, Vol. 92 (2017)
Available at: http://www.nyulawreview.org/sites/default/files/Joh-FINAL_0.pdf

Executive Summary

Conventional wisdom assumes that the police are in control of their investigative tools. But with surveillance technologies, this is not always the case. Increasingly, police departments are consumers of surveillance technologies that are created, sold, and controlled by private companies. These surveillance technology companies exercise an undue influence over the police today in ways that aren't widely acknowledged, but that have enormous consequences for civil liberties and police oversight. Three seemingly unrelated examples—stingray cellphone surveillance, body cameras, and big data software—demonstrate varieties of this undue influence. The companies that provide these technologies act out of private self-interest, but their decisions have considerable public impact. The harms of this private influence include the distortion of Fourth Amendment law, the undermining of accountability by design, and the erosion of transparency norms. This essay demonstrates the increasing degree to which surveillance technology vendors can guide, shape, and limit policing in ways that are not widely recognized. Any vision of increased police accountability today cannot be complete without consideration of the role surveillance technology companies play.

Author

Elizabeth E. Joh is a Professor of Law at the University of California, Davis School of Law, and is the recipient of the 2017 Distinguished Teaching Award. Professor Joh has written widely about policing, technology, and surveillance. Her scholarship has appeared in the Stanford Law Review, the California Law Review, the Northwestern University Law Review, the Harvard Law Review Forum, and the University of Pennsylvania Law Review Online. She has also provided commentary for the Los Angeles Times, Slate, and the New York Times.

Awarded Student Paper

The Market's Law of Privacy: Case Studies in Privacy/Security Adoption

Chetan Gupta

Washington & Lee Law Review Online Edition, Vol. 73 (2017)
Available at: http://lawreview.journals.wlu.io/the-markets-law-of-privacy-case-studies-in-privacysecurity-adoption/

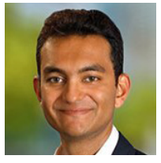
Executive Summary

This paper examines the hypothesis that it may be possible for individual actors in a marketplace to drive the adoption of particular privacy and security standards. It aims to explore the diffusion of privacy and security technologies in the marketplace. Using HTTPS, Two-Factor Authentication, and End-to-End Encryption as case studies, it tries to ascertain which factors are responsible for successful diffusion that improves the privacy of a large number of users. Lastly, it explores whether the FTC may view a widely-diffused standard as a necessary security feature for all actors in a particular industry.

Based on the case studies chosen, the paper concludes that while single actors/groups often do drive the adoption of a standard, they tend to be significant players in the industry or otherwise well positioned to drive adoption and diffusion. The openness of a new standard can also contribute significantly to its success. When a privacy standard becomes industry dominant on account of a major actor, the cost to other market participants appears not to affect its diffusion.

A further conclusion is that diffusion is easiest in consumer facing products when it involves little to no inconvenience to consumers, and is carried out at the back end, yet results in tangible and visible benefits to consumers, who can then question why other actors in that space are not implementing it. Actors who do not adopt the standard may also potentially face reputational risks on account of non-implementation, and lose out on market share.

Author



Chetan Gupta is an associate in Baker McKenzie's Employment Practice Group in Palo Alto. Chetan holds a Masters in Law (LLM) degree from the University of California, Berkeley, with a specialization in law and technology, and a Bachelors of Civil Law (BCL) degree from the University of Oxford, UK.

Chetan advises clients on a wide range of domestic and cross-border employment-related matters. He routinely assists US multinationals with employment aspects of entering and doing business in new jurisdictions across the globe, including data privacy compliance, whistleblower policy and hotline implementation, proprietary information and non-compete agreements.

Honorable Mentions

Algorithmic Jim Crow

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

Fordham Law Review, Vol. 86, Issue 2 (2017)
Available at: http://ir.lawnet.fordham.edu/flr/vol86/iss2/13/

Executive Summary

This article contends that current immigration- and security-related vetting protocols risk promulgating an algorithmically-driven form of Jim Crow. Under the "separate but equal" discrimination of a historic Jim Crow regime, state laws required mandatory separation and discrimination on the front end, while purportedly establishing equality on the back end. In contrast, an Algorithmic Jim Crow regime allows for "equal but separate" discrimination. Under Algorithmic Jim Crow, equal vetting and database screening of all citizens and noncitizens will make it appear that fairness and equality principles are preserved on the front end. Algorithmic Jim Crow, however, will enable discrimination on the back end in the form of designing, interpreting, and acting upon vetting and screening systems in ways that result in a disparate impact.

The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach

by Samson Y. Esayas, Faculty of Law, University of Oslo, Norwegian Research Center for Computers and Law

International Journal of Law and Information Technology, Vol. 25, Issue 2 (2017)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977786

Executive Summary

"The whole is more than the sum of its parts." This article applies lessons from the concept of 'emergent properties' in systems thinking to data privacy law. This concept, rooted in the Aristotelian dictum 'the whole is more than the sum of its parts', where the 'whole' represents the 'emergent property', allows systems engineers to look beyond the properties of individual components of a system and understand the system as a single complex. Applying this concept, the article argues that the current EU data privacy rules focus on individual processing activity based on a specific and legitimate purpose, with little or no attention to the totality of the processing activities—ie., the whole—based on separate purposes. This implies that when an entity processes personal data for multiple purposes, each processing must comply with the data privacy principles separately, in light of the specific purpose and the relevant legal basis.

This (atomized) approach is premised on two underlying assumptions:

(I) distinguishing among different processing activities and relating every piece of personal data to a particular processing if possible, and

(II) if each processing is compliant, the data privacy rights of individuals are not endangered.

However, these assumptions are untenable in an era where companies process personal data for a panoply of purposes, where almost all processing generates personal data and where data are combined across several processing activities. These practices blur the lines between different processing activities and complicate attributing every piece of data to a particular processing. Moreover, when entities engage in these practices, there are privacy interests independent of and/or in combination with the individual processing activities. Informed by the discussion about emergent properties, the article calls for a holistic approach with enhanced responsibility for certain actors based on the totality of the processing activities and data aggregation practices.

Public Values, Private Infrastructure and the Internet of Things: The Case of Automobiles

Deirdre K. Mulligan, Associate Professor in the School of Information at UC Berkeley, and Kenneth A. Bamberger, Professor of Law at the University of California, Berkeley, and Co-Director of the Berkeley Center for Law and Technology

Journal of Law and Economic Regulation, Vol. 9, No. 1 (2016)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914268

Executive Summary

In July 2015, two researchers gained control of a Jeep Cherokee by hacking wirelessly into its dashboard connectivity system. The resulting recall of more than 1.4 million Fiat Chrysler vehicles marked the first-ever security-related automobile recall. These incidents (and related vulnerability disclosures) reveal the critical security issues of modern automobiles, so-called "connected cars," and other Internet of Things (IoT) devices, and underscore the importance of regulatory structures that incentivize greater attention to security.

This paper sets forth principles that should inform the agenda of regulatory agencies such as the National Highway Traffic Safety Administration (NHTSA) that play an essential role in ensuring that the IoT, and specifically the OTA update functionality it requires, responds to relevant cybersecurity and safety risks while attending to other public values. It explains the importance of OTA security and safety update functionality in the automotive industry, and barriers to its development. It explores challenges posed by the interaction between OTA update functionality, consumer protections — including repair rights and privacy — and competition. It then proposes a set of principles to guide the regulatory approach to OTA updates and automobile cybersecurity in light of these challenges.

Thank you to our 2017 Reviewers and Finalist Judges:

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
Of Counsel, Hogan Lovells LLP
Chairman, FPF Board of Directors

Mary Culnan
Professor Emeritus, Bentley University
Vice President, FPF Board of Directors
Chair, FPF Education & Innovation Foundation
FPF Senior Fellow

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

John Verdi
Vice President of Policy,
Future of Privacy Forum

Advisory Board Reviewers

Projjol Banerjea
zeotap

Eduard Bartholme
Call For Action

Anomika Bedi
Halebury

Maureen Cooney
Sprint

Jonathan Fox
Cisco

Leigh Freund
Network Advertising Initiative

Olga Garcia-Kaplan
Novitex Enterprise Solutions

Lauren Gelman
BlurryEdge Strategies

Rita Heimes
IAAP

Sarah Holland
Google

Susan Israel
Loeb & Loeb

Cameron Kerry
Sidley Austin

Barbara Lawler
Digital Stewardship Strategies

Jennifer Mailander
Comscore

Lisa Martinelli
Highmark Health

Magnolia Mobley
PrivacyMatters

Robyn Mohr
Loeb & Loeb

Katie Ratté
Disney

Noga Rosenthal
Epsilon

Kara Selke
Streetlight Data

Amie Stepanovich
Access Now

Catherine Tucker
MIT Sloan School of Management

Hilary Wandall
TrustArc

Susannah Wesley
Edelman

Heather West
Mozilla

Shane Witnov
Facebook

PRIVACY PAPERS FOR POLICYMAKERS 2017

Future of Privacy Forum (FPF) is a nonprofit 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. FPF helps fill the void in the "space not occupied by law" which exists due to the speed of technology development. As "data optimists," we believe that the power of data for good is a net benefit to society, and that it can be well-managed to control risks and offer the best protections and empowerment to consumers and individuals.

1400 EYE STREET, NW | SUITE 450 | WASHINGTON, DC 20005 FPF.ORG | 202-768-8950