PRIVACY PAPERS FOR POLICYMAKERS

2018

This material is based upon work supported by the National Science Foundation under Grant No. 1837413.

FUTURE OF PRIVACY FORUM

February 6, 2019

We are pleased to introduce FPF's ninth annual Privacy Papers for Policymakers. Each year, we invite privacy scholars and authors to submit scholarship for consideration by a committee of reviewers and judges from the FPF Advisory Board. The selected papers are those judged to contain practical analyses of emerging issues that policymakers in Congress, in federal agencies, at the state level and internationally should find useful.

This year's winning papers examine a variety of topical privacy issues:

- One paper focuses on sexual privacy abuses (Citron). The paper argues for the removal of some platform immunity and implementation of federal and state penalties to combat sexual privacy violations.
- Another paper grapples with how privacy is implemented during the design stage of technology and introduces a framework for incentivizing companies to bring privacy to the forefront of their business (Waldman).
- A third paper suggests filling gaps in federal and state privacy laws regarding government surveillance and fair information practices by looking to local statutes, while arguing that certain local laws should prevail against federal and state preemption (Rubinstein).
- Other papers focus on European privacy law and data subject rights. One paper investigates the results of an empirical study of data access requests, and finds that while access rights usually are not adequately accommodated, there are other potential solutions for controllers to improve the efficacy of access rights requests (Ausloos & Dewitte).
- Another paper argues that the right to an explanation under GDPR is unlikely to remedy harms stemming from machine learning algorithms (Edwards & Veale). Instead, the authors suggest that other elements of GDPR, including the right to erasure, the right to portability, and privacy by design principles, could better address these concerns.

For the third year in a row, we are proud to continue highlighting student work by honoring another excellent article. The winning paper (Bashir & Wilson) offers a novel approach to understanding the advertising and analytics landscape.

We thank the scholars, advocates, and Advisory Board members who are engaged with us to explore the future of privacy.

Sincerely,

Christopher Wolf
Senior 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's Heinz College

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

Sharon Anolik
President
Privacy Panacea

Annie Antón
Professor of Computer Science
Georgia Institute of Technology

Justin Antonipillai
Chief Executive Officer
WireWheel

Jocelyn Aqua
Principal, Regulatory Privacy & Cybersecurity
PricewaterhouseCoopers LLP

Vivienne Artz
Chief Privacy Officer
Refinitiv

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

Inna Barmash
General Counsel
Amplify Education, Inc.

Alisa Bergman
Vice President, 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,
Treasurer, FPF Education & Innovation Foundation Board of Directors

Andrew Bloom
Chief Privacy Officer
McGraw-Hill Education

Michael Blum
Senior Vice President, Business and Legal Affairs
Quantcast

Bruce Boyden
Assistant Professor of Law
Marquette University Law School

Anne Bradley
Chief Privacy Officer
Nike, Inc.

Tarryn Brennon
Chief Privacy Officer, Senior Vice President, Associate General Counsel
Pearson

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

Jill Bronfman
Privacy Counsel
Common Sense Media

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 and Chief Information Security Officer
Houghton Mifflin Harcourt

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

Andrew Burt
Chief Privacy Officer & Legal Engineer
Immuta

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

Sam Castic
Senior Director Privacy & Associate General Counsel
Nordstrom Inc.

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

Mary Chapin
Vice President & Chief Legal Officer
National Student Clearinghouse

Kerry Childe
Senior Corporate Counsel
Best Buy

Danielle Keats Citron
Morton & Sophia Macht Professor of Law
University of Maryland
FPF Senior Fellow
Member, FPF Education & Innovation Foundation Board of Directors

Sheila Colclasure
Global Privacy and Public Policy Executive
LiveRamp, Inc.

Maureen Cooney
Head of Privacy
Sprint

Barbara Cosgrove
Vice President, Chief Privacy Officer
Workday

Lorrie Cranor
Professor of Computer Science and of Engineering and Public Policy
Carnegie Mellon University's Heinz College

Mark Crosbie
Head of International Trust & Security
Dropbox

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

Simon Davies
Founder
Privacy International

Alyssa Harvey Dawson
General Counsel
Sidewalk Labs, LLC

Laurie Dechery
Associate General Counsel
Lifetouch, Inc.

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

Carol DiBattiste
General Counsel & Chief Privacy and People Officer
comscore

Erin Egan
Senior Policy Advisor and DIrector, Privacy
Facebook, Inc.

Keith Enright
Director, Global Privacy Legal
Google

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
Professor of Law
Washington & Lee University

Debra Farber
Senior Director, Privacy Strategy
BigID

Ann Fealey
Global Head of Privacy Compliance
Citigroup

Lindsey Finch
Senior Vice President, Global Privacy & Product
Salesforce

Dona Fraser
Director
Children's Advertising Review Unit

Leigh Parsons 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.

John Godfrey
Senior Vice President, Public Policy
Samsung Electronics America

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

Melissa Goldstein
Associate Professor
George Washington University Law School

Scott Goss
Vice President and Legal Counsel
Qualcomm

Justine Gottshall
Chief Privacy Officer
Signal

John Grant
Civil Liberties Engineer
Palantir Technologies

Meredith Grauer
Chief Privacy Officer
The Nielsen Company

Kimberly Gray
Deputy General Counsel, Chief Privacy Officer
IQVIA

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

Eric Heath
Chief Privacy Officer
Ancestry

Rita Heimes
Research Director, 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, Faculty Director, Program on Data and Governance
Ohio State University

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
University of California Berkeley School of Law

Jane Horvath
Senior Director, 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,
Secretary, FPF Education & Innovation Foundation Board of Directors

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

Brian Huseman
Vice President, Public Policy
Amazon.com Services, Inc.

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

Damien Kieran
Data Protection Officer, Legal
Twitter

Stephen Kline
Vice President - Independent Privacy Risk and Chief Privacy Officer
American Express National Bank

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

Fernando Laguarda
Faculty Director, Program on Law and Government
American University Washington College of Law
Member, FPF Education & Innovation Foundation Board of Directors

Michael Lamb
Global Chief Privacy Officer
RELX Group

Barbara Lawler
Vice President, Chief Privacy and Data Ethics Officer
Looker Data Services

Peter Lefkowitz
Chief Privacy & Digital Risk Officer
Citrix Systems

Yafit Lev-Aretz
Assistant Professor of Law, Zicklin Business School, Baruch College
City University of New York

Ari Levenfeld
Chief Privacy Officer
Sizmek

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

David Longford
Chief Executive Officer
DataGuidance

Caroline Louveaux
Chief Privacy Officer
MasterCard

Brendon Lynch
Chief Privacy Officer
Microsoft Corporation

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

Knut Mager
Head Global Data Privacy
Novartis International

Larry Magid
President and Chief Executive Officer
Connect Safely

Guillaume Marcerou
Senior Counsel
Criteo SA

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

Lisa Martinelli
Vice President, Chief Privacy & Data Ethics Officer
Highmark Health

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

William McGeveran
Associate Professor
University of Minnesota Law School

Christin McMeley
Senior Vice President , Chief Privacy and Legal Information Security Officer
Comcast Cable

David Medine
Consultant
Consultative Group to Assist the Poor

Carlos Melvin
Managing Director, Global Privacy
Starbucks

Douglas Miller
Vice President, Global Privacy Leader
Verizon Media

Tom Moore
Chief Privacy Officer
AT&T Services, Inc.

Keith Murphy
Senior Vice President Government Relations & Regulatory Counsel
Viacom

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Kirsten Mycroft
Global Chief Privacy Officer
BNY Mellon

Vivek Narayanadas
Associate General Counsel, Privacy
Shopify

Ashley Narsutis
Head of Legal
AdRoll, Inc.

Jill Nissen
Founder
Nissen Consulting

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

Eleonore Pauwels
Director of the AI Lab
Wilson Center

Harriet Pearson
Partner
Hogan Lovells LLP

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 Ratte
Associate General Counsel - Privacy
The Walt Disney Company

Future of Privacy Forum Advisory Board (continued)

Alan Raul
Partner
Sidley Austin LLP
Member, FPF Board of Directors,
Member, FPF Education & Innovation Foundation Board of Directors

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

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

Michelle Richardson
Director, Privacy and Data Protection
Center for Democracy & Technology

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

Shirley Rooker
President
Call for Action, Inc.

Michelle Rosenthal
Principal Corporate Counsel
T-Mobile

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

Norman Sadeh
Professor
Carnegie Mellon University's Heinz College

Neal Schroeder
Senior Vice President Internal Audit and Corporate Privacy Officer
Enterprise Holdings, Inc.

Corinna Schulze
Director, EU Government Relations, Global Corporate
SAP

Paul Schwartz
Jefferson E. Peyser Professor of Law
University of California Berkeley School of Law

Evan Selinger
Professor of Philosophy
Rochester Institute of Technology
FPF Senior Fellow

Kara Selke
Vice President - Privacy & Strategic Partners
StreetLight Data, Inc.

Urvashi Sen
Acting Chief Privacy Officer and Privacy Officer for Americas
HCL America Inc.

Linda Sherry
Director, National Priorities
Consumer Action

Scott Shipman
Vice President, Chief Privacy Officer
Intuit

Julia Shullman
Deputy General Counsel, Commercial & Privacy
AppNexus

Meredith Sidewater
Senior Vice President and General Counsel
LexisNexis Risk Solutions

James Simatacolos
Managing Counsel, Data Privacy and Cybersecurity
Toyota Motor North America, Inc.

Dale Skivington
Privacy Consultant and Adjunct Professor of Law
University of Colorado Law School
Member, FPF Education & Innovation Foundation Board Directors

Will Smith
Executive Chairman and Chief Strategy Officer
Euclid Analytics

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

Daniel Solove
John Marshall Harland Research Professor of Law
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

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

Zoe Strickland
Global Chief Privacy Officer
J.P. Morgan Chase

Greg Stuart
Chief Executive Officer
Mobile Marketing Association

Peter Swire
Elizabeth and Tommy Holder Chair of Law and Ethics, Scheller College of Business
Georgia Institute of Technology
FPF Senior Fellow

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

Adam Thierer
Senior Research Fellow
George Mason University

Melanie Tiano
Director, Cybersecurity and Privacy
CTIA-The Wireless Association

Anne Toth
Head of Data Policy
World Economic Forum

Teresa Troester-Falk
Chief Global Privacy Strategist
Nymity Inc.

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

David Vladeck
A.B. Chettle Chair 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

Rachel Welch
Senior Vice President of Policy and External Affairs
Charter Communications

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

Shane Wiley
Vice President, Privacy
cuebiq

Christopher Wolf
Senior Counsel
Hogan Lovells LLP
President, FPF Board of Directors
President, FPF Education & Innovation Foundation Board of Directors

Nicole Wong
Principal
Nwong Strategies

Christopher Wood
Executive Director
LGBT Technology Partnership

Heng Xu
Professor, Department of Information Technology and Analytics Director, Kogod Cybersecurity Governance Center
American University

Karen Zacharia
Chief Privacy Officer
Verizon

Ruby Zefo
Chief Privacy Officer
Uber Technologies, Inc.

Elana Zeide
PULSE Fellow in Artificial Intelligence, Law & Policy
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 2019. Please send all updates about this list to cpickeral@fpf.org.

Table of Contents

Awarded Papers

Awarded 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.

Shattering One-Way Mirrors: Data Subject Access Rights in Practice

Jef Ausloos and Pierre Dewitte

International Data Privacy Law, Vol. 8, Issue 1 (2018)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106632

Executive Summary

The right of access occupies a central role in EU data protection law's arsenal of data subject empowerment measures. It can be seen as a necessary enabler for most other data subject rights as well as an important role in monitoring operations and (en)forcing compliance. Despite some high-profile revelations regarding unsavoury data processing practices over the past few years, access rights still appear to be underused and not properly accommodated. It is especially this last hypothesis we tried to investigate and substantiate through a legal empirical study. During the first half of 2017, around sixty information society service providers were contacted with data subject access requests. Eventually, the study confirmed the general suspicion that access rights are by and large not adequately accommodated. The systematic approach did allow for a more granular identification of key issues and broader problematic trends. Notably, it uncovered an often-flagrant lack of awareness; organization; motivation; and harmonization. Despite the poor results of the empirical study, we still believe there to be an important role for data subject empowerment tools in a hyper-complex, automated and ubiquitous data-processing ecosystem. Even if only used marginally, they provide a checks and balances infrastructure overseeing controllers' processing operations, both on an individual basis as well as collectively. The empirical findings also allow identifying concrete suggestions aimed at controllers, such as relatively easy fixes in privacy policies and access rights templates.

Authors

Jef Ausloos is a postdoctoral researcher at the University of Amsterdam's Institute for Information law (IViR). His research centers around data-driven power asymmetries and the normative underpinnings of individual control empowerment and autonomy in today's largely privatized information ecosystem. Before joining IViR in December 2018 Jef was a doctoral researcher at the University of Leuven's Center for IT & IP Law (CiTiP), where he worked on a variety of projects in media and data protection law. In October 2018, he obtained his PhD entitled 'The right to erasure: safeguard for informational self-determination in a digital society?'. Jef holds degrees in law from the Universities of Namur Leuven and Hong Kong. He has worked as an International Fellow at the Center for Democracy & Technology and the Electronic Frontier Foundation and has been on research stays at the Berkman Center for Internet & Society (Harvard University) in 2012, the Institute for Information Law (University of Amsterdam) in 2015 and the Centre for Intellectual Property and Information Law (Cambridge University) in 2017.

Pierre Dewitte obtained his Bachelor and Master degree of Laws with a specialization in Corporate and Intellectual Property law from the Université Catholique de Louvain in 2016. As part of his Master program, he spent six months in the University of Helsinki where he strengthened his knowledge in European law. In 2017, he then completed the advanced Master of Intellectual Property and ICT law at the KU Leuven with a special focus on privacy, data protection and electronic communications law.

Pierre joined the KU Leuven Centre for IT & IP in October 2017 where he conducts interdisciplinary research on privacy engineering, smart cities and algorithmic transparency. Among other initiatives, his main research track seeks to bridge the gap between software engineering practices and data protection regulations by creating a common conceptual framework for both disciplines and providing decision and trade-off support for technical and organizational mitigation strategies in the software development life-cycle.

Sexual Privacy

Danielle Keats Citron

Yale Law Journal (Forthcoming 2019)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233805##

Executive Summary

Those who wish to control, expose, and damage the identities of individuals routinely do so by invading their privacy. People are secretly recorded in bedrooms and public bathrooms, and "up their skirts." They are coerced into sharing nude photographs and filming sex acts under the threat of public disclosure of their nude images. People's nude images are posted online without permission. Machine-learning technology is used to create digitally manipulated "deep fake" sex videos that swap people's faces into pornography.

At the heart of these abuses is an invasion of sexual privacy—the behaviors and expectations that manage access to, and information about, the human body; intimate activities; and personal choices about the body and intimate information. More often, women, nonwhites, sexual minorities, and minors shoulder the abuse.

Sexual privacy is a distinct privacy interest that warrants recognition and protection. It serves as a cornerstone for sexual autonomy and consent. It is foundational to intimacy. Its denial results in the subordination of marginalized communities. Traditional privacy law's efficacy, however, is eroding just as digital technologies magnify the scale and scope of the harm. This Article suggests an approach to sexual privacy that focuses on law and markets. Law should provide federal and state penalties for privacy invaders, remove the statutory immunity from liability for certain content platforms, and work in tandem with hate crime laws. Market efforts should be pursued if they enhance the overall privacy interests of all involved.

Author

Danielle Keats Citron is the Morton & Sophia Macht Professor of Law at the University of Maryland Carey School of Law where she teaches and writes about privacy, civil rights, and free speech. Her book Hate Crimes in Cyberspace (Harvard University Press) was named one of the "20 Best Moments for Women in 2014" by Cosmopolitan magazine. Her law review articles have appeared or are forthcoming in Yale Law Journal, California Law Review (twice), Michigan Law Review (twice), Texas Law Review, Boston University Law Review (three times), Notre Dame Law Review (twice), Washington University Law Review (three times), Southern California Law Review, Minnesota Law Review, Washington Law Review (twice), UC Davis Law Review, Fordham Law Review, and Hastings Law Journal. She is a frequent opinion writer for major media outlets including the New York Times, Slate, the Atlantic, and the Guardian. Danielle is an Affiliate Scholar at the Stanford Center on Internet and Society, Affiliate Fellow at the Yale Information Society Project, a Tech Fellow at NYU's Policing Project, and a member of the Principals Group for the Harvard-MIT AI Fund. Danielle works closely with tech companies such as Twitter and Facebook and federal and state lawmakers on issues of online safety, privacy, and free speech. She is the Chair of the Electronic Privacy Information Center's Board of Directors. Danielle will be joining the faculty of Boston University School of Law as a Professor of Law in the fall of 2019.

Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For

Lilian Edwards and Michael Veale

Duke Technology Review, Vol. 16, Issue 1 (2017)
Available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1315&context=dltr

Executive Summary

Algorithms, particularly machine learning (ML) algorithms, are increasingly important to individuals' lives, but have caused a range of concerns revolving mainly around unfairness, discrimination and opacity. Transparency in the form of a "right to an explanation" has emerged as a compellingly attractive remedy since it intuitively promises to open the algorithmic "black box" to promote challenge, redress, and hopefully heightened accountability. Amidst the general furore over algorithmic bias we describe, any remedy in a storm has looked attractive.

However, we argue that a right to an explanation in the EU General Data Protection Regulation (GDPR) is unlikely to present a complete remedy to algorithmic harms, particularly in some of the core "algorithmic war stories" that have shaped recent attitudes in this domain. Firstly, the law is restrictive, unclear, or even paradoxical concerning when any explanation-related right can be triggered. Secondly, even navigating this, the legal conception of explanations as "meaningful information about the logic of processing" may not be provided by the kind of ML "explanations" computer scientists have developed, partially in response. ML explanations are restricted both by the type of explanation sought, the dimensionality of the domain and the type of user seeking an explanation. However, "subject-centric" explanations (SCEs) focussing on particular regions of a model around a query show promise for interactive exploration, as do explanation systems based on learning a model from outside rather than taking it apart (pedagogical versus decompositional explanations) in dodging developers' worries of intellectual property or trade secrets disclosure.

Based on our analysis, we fear that the search for a "right to an explanation" in the GDPR may be at best distracting, and at worst nurture a new kind of "transparency fallacy." But all is not lost. We argue that other parts of the GDPR related (i) to the right to erasure ("right to be forgotten") and the right to data portability; and (ii) to privacy by design, Data Protection Impact Assessments and certification and privacy seals, may have the seeds we can use to make algorithms more responsible, explicable, and human centered.

Authors

Lilian Edwards is a leading UK-based academic and frequent speaker on issues of Internet law, intellectual property and artificial intelligence. She is on the Advisory Board of the Open Rights Group and the Foundation for Internet Privacy Research and is the Professor of Law, Innovation and Society at Newcastle Law School at Newcastle University, having previously held chairs at Southampton, Sheffield and Strathclyde. She has taught information technology law, e-commerce law, privacy law and Internet law at the undergraduate and postgraduate level since 1996 and been involved with law and artificial intelligence (AI) since 1985.

She has co-edited (both with Charlotte Waelde and alone) three editions of a bestselling textbook, Law and the Internet (later Law, Policy and the Internet); a new sole-edited collection, Law, Policy and the Internet appeared in 2018. She won the Barbara Wellberry Memorial Prize in 2004 for work on online privacy and data trusts. A collection of her essays, The New Legal Framework for E-Commerce in Europe, was published in 2005. She is Deputy Director, and was co-founder, of the Arts and Humanities Research Council (AHRC) Centre for IP and Technology Law (now SCRIPT). Edwards has consulted inter alia for the EU Commission, the OECD, and WIPO. Edwards co-chairs GikII, an annual series of international workshops on the intersections between law, technology and popular culture.

Michael Veale is a researcher in responsible public sector machine learning at University College London, specializing in the fairness and accountability of data-driven tools in the public sector, the interplay between advanced technologies, data protection law, and human-computer interaction. His research has been cited by national and international governments and regulators, discussed in the media, as well as debated in Parliament. Michael has acted as expert consultant on machine learning and society for the World Bank, United Nations, European Commission, the Royal Society and the British Academy, and a range of national governments. Michael is a Fellow at the Centre for Public Impact, an Honorary Research Fellow at Birmingham Law School, University of Birmingham, a Visiting Researcher at the BBC DataLab, and a member of the Advisory Council for the Open Rights Group. He previously worked on IoT and ageing policy at the European Commission, and holds degrees from LSE (BSc) and Maastricht University (MSc). A full list of publications can be found at https://michae.lv. He tweets at @mikarv.

Privacy Localism

Ira Rubinstein

NYU School of Law, Public Law Research Paper No. 18-18 (2018)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124697

Executive Summary

Privacy law scholarship often focuses on domain-specific federal privacy laws and state efforts to broaden them. This Article provides the first comprehensive analysis of privacy regulation at the local level (which it dubs "privacy localism"), using recently enacted privacy laws in Seattle and New York City as principle examples. It attributes the rise of privacy localism to a combination of federal and state legislative failures and three emerging urban trends: the role of local police in federal counter-terrorism efforts; smart city and open data initiatives; and demands for local police reform in the wake of widely reported abusive police practices.

Both Seattle and New York have enacted or proposed (1) a local surveillance ordinance regulating the purchase and use of surveillance equipment and technology by city departments (including the police) and (2) a law regulating city departments' collection, use, disclosure and retention of personal data. In adopting these local laws, both cities have sought to fill two significant gaps in federal and state privacy laws: the public surveillance gap (which refers to the weak constitutional and statutory protections against government surveillance in public places) and the fair information practices gap (which refers to the inapplicability of the federal and state Privacy Acts to government records held by local government agencies).

Filling these gaps is a significant accomplishment and one that exhibits all of the values typically associated with federalism (diversity, participation, experimentation, responsiveness, and accountability). This Article distinguishes federalism and localism and shows why privacy localism should prevail against the threat of federal and (more importantly) state preemption. The Article concludes by suggesting that privacy localism has the potential to help shape emerging privacy norms for an increasingly urban future, inspire more robust regulation at the federal and state levels, and inject more democratic control into city deployments of privacy-invasive technologies.

Author

Ira Rubinstein is a Senior Fellow at the Information Law Institute (ILI) of the New York University School of Law. His research interests include privacy by design, electronic surveillance law, big data, voters' privacy, and privacy regulation. Rubinstein lectures and publishes widely on issues of privacy and security and has testified before Congress on these topics on several occasions. Recent work includes papers on co-regulatory models of privacy regulation, anonymization and risk, voter privacy in the age of big data. Additionally, he co-authored a research report on Systematic Government Access to Personal Data: A Comparative Analysis, prepared for the Center for Democracy and Technology. Earlier papers include Big Data: The End of Privacy or a New Beginning published in International Data Privacy Law in 2013 and presented it at the 2013 Computer Privacy and Data Protection conference in Brussels; and Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, co-authored with Nathan Good, which won the IAPP Privacy Law Scholars Award at the 5th Annual Privacy Law Scholars Conference in 2012 and was published in the Berkeley Technology Law Journal.

Prior to joining the ILI, Rubinstein spent 17 years in Microsoft's Legal and Corporate Affairs department, most recently as Associate General Counsel in charge of the Regulatory Affairs and Public Policy group. Before coming to Microsoft, he was in private practice in Seattle, specializing in immigration law. From 2010-2016, he served on the Board of Directors of the Center for Democracy and Technology. He also served as Rapporteur, of the EU-US Privacy Bridges Project, which was presented at the 2015 International Conference of Privacy and Data Protection Commissioners in Amsterdam. He currently serves on the Board of Advisers of the American Law Institute for the Restatement Third, Information Privacy Principles and the Organizing Committee of the Privacy by Design Workshops sponsored by the Computing Research Association. Rubinstein graduated from Yale Law School in 1985.

Designing Without Privacy

Ari Ezra Waldman

Houston Law Review, Vol. 55, Issue 3 (2018)
Available at: https://houstonlawreview.org/article/3880-designing-without-privacy

Executive Summary

In *Privacy on the Ground,* the law and information scholars Kenneth Bamberger and Deirdre Mulligan showed that empowered chief privacy officers (CPOs) are pushing their companies to take consumer privacy seriously by integrating privacy into the designs of new technologies. Their work was just the beginning of a larger research agenda. CPOs may set policies at the top, but they alone cannot embed robust privacy norms into the corporate ethos, practice, and routine. As such, if we want the mobile apps, websites, robots, and smart devices we use to respect our privacy, we need to institutionalize privacy throughout the corporations that make them. In particular, privacy must be a priority among those actually doing the work of design on the ground—namely, engineers, computer programmers, and other technologists.

This Article presents the initial findings from an ethnographic study of how, if at all, those designing technology products think about privacy, integrate privacy into their work, and consider user needs in the design process. It also looks at how attorneys at private firms draft privacy notices for their clients and interact with designers. Based on these findings, this Article suggests that Bamberger's and Mulligan's narrative is not yet fully realized. The account among some engineers and lawyers, where privacy is narrow, limited, and barely factoring into design, may help explain why so many products seem to ignore our privacy expectations. The Article then proposes a framework for understanding how factors both exogenous (theory and law) and endogenous (corporate structure and individual cognitive frames and experience) to the corporation prevent the CPOs' robust privacy norms from diffusing throughout technology companies and the industry as a whole. This framework also helps suggest how specific reforms at every level—theory, law, organization, and individual experience—can incentivize companies to take privacy seriously, enhance organizational learning, and eliminate the cognitive biases that lead to discrimination in design.

Author

Ari Ezra Waldman is a Professor of Law and the Founding Director of the Innovation Center for Law and Technology at New York Law School. Professor Waldman's work is forthcoming or has been published in numerous leading scholarly journals, including Law & Social Inquiry (peer reviewed), the Washington University Law Review, the UC Irvine Law Review, and the Cornell Law Review, among many others. His first book, Privacy As Trust: Information Law for an Information Age (Cambridge University Press, 2018), reorients privacy law around sociological principles of trust and argues that privacy law should protect information disclosed in contexts of trust. In 2018, Professor Waldman was honored as the Deirdre G. Martin Memorial Lecturer on Privacy at the University of Ottawa. In 2017, he received the highest award in privacy law, the Best Paper Award at the Privacy Law Scholars Conference in Berkeley, CA. And in 2016, his scholarship was awarded the Otto L. Walter Distinguished Writing Award. Professor Waldman has testified before the U.S. House of Representatives on issues relating to privacy and online social networks. His opinion pieces have appeared in the New York Times, the New York Daily News, The Advocate, among other popular press. He has appeared on Nightline, Good Morning America, MSNBC's "The Docket," and appeared as an expert on Syfy's miniseries, The Internet Ruined My Life. He holds a Ph.D. from Columbia University, a J.D. from Harvard Law School, and a B.A. from Harvard College. He also really loves dogs.

Awarded Student Paper

Diffusion of User Tracking Data in the Online Advertising Ecosystem

Muhammad Ahmad Bashir and Christo Wilson

Sciendo, Vol. 2018, Issue 4 (2018)
Available at: https://pdfs.semanticscholar.org/73c2/7fb99c4959c0409818c9c90c3961da0f4775.pdf

Executive Summary

There are two trends that are currently reshaping the online display advertising industry. First, the amount and precision of data that is being collected by Advertising and Analytics (A&A) companies about users as they browse the web is increasing. Second, there is a transition underway from "ad networks" to "ad exchanges", where advertisers bid on "impressions" (empty advertising slots on websites) being sold in Real Time Bidding (RTB) auctions. The rise of RTB has forced A&A companies to collaborate with one another, in order to exchange data about users and facilitate bidding on impressions.

These trends have fundamental implications for users' online privacy. It is no longer sufficient to view each A&A company, and the data it collects, in isolation. Instead, when a given user is observed by a single A&A company, that observation may be shared, in real time, with hundreds of other A&A companies within RTB auctions.

To understand the impact of RTB on users' privacy, we propose a new model of the online advertising ecosystem called an Interaction Graph. This graph captures the business relationships between A&A companies, and allows us to model how tracking data is shared between companies. Using our Interaction Graph model, we simulate browsing behavior to understand how much of a typical web user's browsing history can be tracked by A&A companies. We find that 52 A&A companies are each able to observe 91% of an average user's browsing history, under modest assumptions about data sharing in RTB auctions. 636 A&A companies are able to observe at least 50% of an average user's browsing history. Even under very strict simulation assumptions, the top 10 A&A companies still observe 89-99% of an average user's browsing history.

Additionally, we investigate the effectiveness of several tracker-blocking strategies, including those implemented by popular privacy-enhancing browser extensions. We find that AdBlock Plus (the world's most popular ad blocking browser extension), is ineffective at protecting users' privacy because major ad exchanges are whitelisted under the Acceptable Ads program. In contrast, Disconnect blocks the most information flows to A&A companies of the extensions we evaluated. However, even with strong blocking, major A&A companies still observe 40-80% of an average users' browsing history.

Authors

Muhammad Ahmad Bashir is a PhD candidate at Northeastern University's College of Computer and Information Science, where he is advised by Professor Christo Wilson. Ahmad is broadly interested in web security and privacy. His current research focuses on understanding the online advertising ecosystem with an emphasis on privacy implications for end users. Ahmad earned his Bachelor of Science degree in Computer Science from Lahore University of Management Sciences in Pakistan. Before starting his PhD, Ahmad collaborated with Krishna Gummadi's group at Max Planck Institute (SWS) for 2 years, where his research focused on studying trustworthiness and reputation of identities in Online Social Networks.

Christo Wilson is an Associate Professor in the College of Computer and Information Science at Northeastern University. He is a founding member of the Cybersecurity and Privacy Institute at Northeastern, and serves as director of the BS in Cybersecurity program. Professor Wilson's research focuses on online security and privacy, with a specific interest in algorithmic auditing and fairness. Algorithmic auditing is an emerging, interdisciplinary area that uses experimental techniques to measure the black-box algorithmic systems that increasingly pervade daily life. His work has been covered extensively in the press, including the CBS Evening News, Good Morning America, The Wall Street Journal, The Boston Globe, and The Washington Post. He is supported by an NSF CAREER award, the Knight Foundation, the Democracy Fund, the Russel Sage Foundation, the Data Transparency Lab, and Verisign Labs.

Honorable Mentions

Regulating Bot Speech

Madeline Lamo, Law Clerk, United States Court of Federal Claims
Ryan Calo, Lane Powell and D. Wayne Gittinger Associate Professor of Law, University of Washington School of Law

UCLA Law Review (Forthcoming 2019)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3214572

Executive Summary

We live in a world of artificial speakers with real impact. Bots foment political strife, skew online discourse, and manipulate the marketplace. In response to concerns about the unique threats bots pose, legislators have begun to pass laws that require online bots to clearly indicate that they are not human. This work is the first to consider how such efforts to regulate bots might raise concerns about free speech and privacy.

While requiring a bot to self-disclose does not censor speech as such, it may nonetheless infringe upon the right to speak—including the right to speak anonymously—in the digital sphere. Specifically, complexities in the enforcement process threaten to unmask anonymous speakers, and requiring self-disclosure creates a scaffolding for censorship by private actors and other governments.

Ultimately, bots represent a diverse and emerging medium of speech. Their use for mischief should not overshadow their novel capacity to inform, entertain, and critique. We conclude by providing policymakers with a series of principles to bear in mind when regulating bots, so as not to inadvertently curtail an emerging form of expression or compromise anonymous speech.

The Intuitive Appeal of Explainable Machines

Andrew D. Selbst, Postdoctoral Scholar, Data & Society Research Institute
Solon Barocas, Assistant Professor, Cornell University

Fordham Law Review, Vol. 87, Issue 3 (2018)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126971

Executive Summary

Algorithmic decision-making has become synonymous with inexplicable decision-making, but what makes algorithms so difficult to explain? This Article examines what sets machine learning apart from other ways of developing rules for decision-making and the problem these properties pose for explanation. We show that machine learning models can be both inscrutable and nonintuitive and that these are related, but distinct, properties.

Calls for explanation have treated these problems as one and the same, but disentangling the two reveals that they demand very different responses. Dealing with inscrutability requires providing a sensible description of the rules; addressing nonintuitiveness requires providing a satisfying explanation for why the rules are what they are. Existing laws like the Fair Credit Reporting Act (FCRA), the Equal Credit Opportunity Act (ECOA), and the General Data Protection Regulation (GDPR), as well as techniques within machine learning, are focused almost entirely on the problem of inscrutability. While such techniques could allow a machine learning system to comply with existing law, doing so may not help if the goal is to assess whether the basis for decision-making is normatively defensible.

In most cases, intuition serves as the unacknowledged bridge between a descriptive account and a normative evaluation. But because machine learning is often valued for its ability to uncover statistical relationships that defy intuition, relying on intuition is not a satisfying approach. This Article thus argues for other mechanisms for normative evaluation. To know why the rules are what they are, one must seek explanations of the process behind a model's development, not just explanations of the model itself.

Thank you to our 2018 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
Senior Counsel
Hogan Lovells LLP
President, FPF Board of Directors
President, FPF Education & Innovation Foundation
Board of Directors

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

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

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

Advisory Board Reviewers

Eduard Bartholme
Call For Action

Monica Bulger
FPF

Maureen Cooney
Sprint

Philip Fabinger
HERE Technologies

Jonathan Fox
Cisco

Dona Fraser
CARU

Claire Gartland
Facebook

Lauren Gelman
BlurryEdge Strategies

Scott Goss
Qualcomm

John Grant
Palantir

Rita Heimes
IAPP

Joseph Jerome
CDT

Barbara Lawler
Looker Data Services

Knut Mager
Novartis

Magnolia Mobley
LegalMatters

Lisa Martinelli
Highmark Health

Estelle Massé
Access Now

Drew Mitnik
Access Now

Robyn Mohr
Loeb & Loeb

Vivek Narayanadas
Shopify

Kara Selke
StreetLight Data

Amie Stepanovich
Access Now

Thomas van der Valk
Facebook

Heather West
Mozilla

PRIVACY PAPERS FOR POLICYMAKERS 2018

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