PRIVACY PAPERS FOR POLICYMAKERS

2019

FUTURE OF PRIVACY FORUM

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

FUTURE OF
PRIVACY
FORUM

February 6, 2020

We are pleased to introduce FPF's tenth 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 offers a framework for regulating personal information to reduce discrimination against vulnerable populations. (Cofone) The framework determines when information should flow, or not flow, based on key use cases of gender discrimination in orchestra auditions and discrimination against convicts in job applications.
- Another paper presents a case for federal privacy legislation that goes beyond data protection and fair information processing, arguing that privacy faces a "constitutional moment" that presents an opportunity to define the structure of our emerging digital society. (Hartzog & Richards)
- A third paper examines how Data Protection Impact Assessments (DPIAs) address, or fail to address, the EU's General Data Protection Regulation (GDPR) approach to algorithmic accountability. (Kaminski & Malgieri) The authors call for a multi-layered process for algorithmic accountability, better aligning with GDPR's transparency goals.
- Another paper tackles the problem of dark patterns—interface design choices intended to coerce users into purchasing or sharing information they otherwise would not—by conducting a study of 11,000 shopping websites. (Mathur et al.) The authors provide the results of the study and suggestions for further research and methods for regulators to mitigate deceptive practices.
- The fifth winning paper provides a detailed assessment of the 2018 Supreme Court opinion in *Carpenter v. United States,* requiring law enforcement to obtain a warrant to access an individual's historical whereabouts from the records of a cell phone provider. (Ohm) The author argues that this landmark case will guide the future of constitutional privacy in the United States for generations to come.

For the fourth year in a row, we are proud to continue highlighting student work by honoring another excellent paper. The winning paper (Malkin et al.) offers a novel approach to measuring the privacy perceptions and attitudes of smart speaker users.

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

Jules Polonetsky

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, Innovation
Retail Industry Leaders Association

Sharon Anolik
Founder & President
Privacy Panacea

Annie Antón
Professor of Computer Science
Georgia Institute of Technology

Justin Antonipillai
Founder & Chief Executive Officer
WireWheel

Jocelyn Aqua
Principal, Regulatory Privacy & Cybersecurity
PricewaterhouseCoopers LLP

Vivienne Artz
Chief Privacy Officer
Refinitiv

Joe Ashkouti
Senior Managing Counsel, Enterprise Functions & Chief Privacy Officer
Change Healthcare

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

Stephen Balkam
Founder & Chief Executive Officer
Family Online Safety Institute

Kenneth Bamberger
The Rosalinde and Arthur Gilbert Foundation Professor of Law
Co-Director of the Berkeley Center for Law & Technology
University of California, Berkeley School of Law

Kabir Barday
Founder, President & Chief Executive Officer
OneTrust

Inna Barmash
Senior Vice President, General Counsel & Chief of Staff
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
Vice President & Chief Privacy Officer
McGraw-Hill Education

Jamie Boone
Vice President, Government Affairs
Consumer Technology Association

Axel du Boucher
Group Data Protection Officer
Criteo

Bruce Boyden
Assistant Professor of Law
Marquette University Law School

Anne Bradley
Vice President, Chief Privacy Officer & Global Counsel Nike Direct
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

Julie Brill
Corporate Vice President, Deputy General Counsel Global Privacy and Regulatory Affairs, and Chief Privacy Officer
Microsoft Corporation

Jill Bronfman
Privacy Counsel
Common Sense Media

Stuart Brotman
Fellow
Woodrow Wilson International Center for Scholars

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

Andres Castrillon
Senior Manager, Federal Government Affairs
Fiat Chrysler Automobiles (FCA)

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

Mary Chapin
Vice President & Chief Legal Officer
National Student Clearinghouse

Danielle Keats Citron
Professor of Law
Boston University School of Law
FPF Senior Fellow
Member, FPF Education & Innovation Foundation Board of Directors

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
Data Protection Officer
Dropbox

Dan Crowley
Head of Trust & Safety and Data Protection Officer
Quizlet

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

Rachel Cummings
Assistant Professor of School of Industrial and Systems Engineering
Georgia Institute of Technology

Alyssa Harvey Dawson
General Counsel and Head of Legal, Privacy and Data Governance
Sidewalk Labs, LLC

Laurie Dechery
Associate General Counsel
Shutterfly, Inc.

Jolynn Dellinger
Special Counsel for Privacy Policy & Litigation, NC DOJ
Privacy Law, Duke and UNC

Sara DePaul
Senior Director, Technology Policy
Software & Information Industry Association

Michael Dolan
Senior Director, Head of Enterprise Privacy
Best Buy

Megan Duffy
Head of Privacy
Atlassian

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

Jill Elliot
Vice President & Associate General Counsel
Houghton Mifflin Harcourt

Keith Enright
Chief Privacy Officer
Google

Kristen Erbes
Chief Privacy Officer
Cambia Health Solutions

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
Professor of Law
Washington and Lee University

Anne Fealey
Global Chief Privacy Officer
Citi

Heather Federman
Vice President of Privacy & Policy
BigID

Lindsey Finch
Executive Vice President, Global Privacy & Product Legal
Salesforce

Leo Fitzsimon
Government Relations – Americas
HERE

Renard Francois
Managing Director – Global Chief Privacy Officer
JPMorgan Chase & Co.

Dona Fraser
Director
Children's Advertising Review Unit

Leigh Parsons Freund
President & Chief Executive Officer
Network Advertising Initiative

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

Deborah Gertsen
Counsel - Corporate Compliance Office - Privacy
Ford Motor Company

John Gevertz
Chief Privacy Officer
Visa

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, Department of Health Policy and Management
George Washington University Law School

Scott Goss
Vice President and Privacy Counsel
Qualcomm

John Grant
Civil Liberties Engineer
Palantir Technologies

Meredith Grauer
Chief Privacy Officer
The Nielsen Company

Kimberly Gray

Chief Privacy Officer, Global
IQVIA

Cathleen Hartge
Head of Legal
Branch

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

Ben Hayes
Chief Privacy Officer
Zeta Global

Cate Haywood
Senior Director & Global Head of Privacy
Sony

Eric Heath
Chief Privacy Officer
Ancestry

Rita Heimes
Research Director & Data Protection Officer
International Association of Privacy Professionals

Becky Heironimus
Managing Vice President Enterprise Customer
Products and Data Ethics and Privacy
Capital One

Beth Hill
General Counsel, Chief Compliance Officer
and Privacy Leader
Ford Direct

Dennis Hirsch
Professor of Law; 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

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

Jane Horvath
Senior Director of Global Privacy
Apple, Inc.

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

Sandra Hughes
Chief Executive Officer 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.

Harvey Jang
Vice President, Chief Privacy Officer
Cisco Systems, Inc.

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

Audrey Jean
Vice President, Privacy Officer & Associate
General Counsel
AARP

Meg Leta Jones
Associate Professor
Georgetown University

Mark Kahn
General Counsel and Vice President of Policy
Segment

Damien Kieran
Global Data Protection Officer, Legal Director,
and Associate General Counsel
Twitter

Stephen Kline
Vice President – Independent Privacy Risk
& Chief Privacy Officer
American Express National Bank

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

Karen Kornbluh
Senior Fellow and Director, Digital Innovation
& Democracy Initiative
The German Marshall Fund of the United States

Mihir Kshirsagar
Clinic Director of the Center for Information
Technology Policy
Princeton University

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-Artez
Assistant Professor of Law,
Zicklin Business School, Baurch College
City University of New York

Ari Levenfield
Chief Privacy Officer
Quantcast

Matt Levine
General Counsel and Chief Privacy Officer
CLEAR

Lara Liss
Vice President, Global Chief Privacy Officer
Walgreens Boots Alliance

David Longford
Chief Executive Officer
DataGuidance

Douglas Longhitano
Manager – Connected & Automated
Vehicle Policy
American Honda Motor Co.

Caroline Louveaux
Chief Privacy Officer
MasterCard

Mark MacCarthy
Senior Fellow and Adjunct Professor
Georgetown University

Knut Mager
Head Global Data Privacy
Novartis Pharmaceuticals Corporation

Larry Magid
President & Chief Executive Officer
Connect Safely

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

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

Winston Maxwell
Director of Law & Digital Technology
Telecom ParisTech

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

William McGeveran
Associate Dean for Academic Affairs Julius E. Davis
Professor of Law
University of Minnesota Law School

Zoe McMahon
Chief Privacy and Data Protection Officer
HP Inc.

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

Terry McQuay
President & Founder
Nymity

David Medine
Senior Financial Sector Specialist
Consultative Group to Assist the Poor

Carlos Melvin
Managing Director, Global Privacy
Starbucks

Douglas Miller
Vice President of Global Privacy and Trust
Verizon Media

Christina Montgomery
Vice President & Chief Privacy Officer
IBM

Tom Moore
Chief Privacy Officer & Senior Vice President
Compliance
AT&T Services, Inc.

Keith Murphy
Senior Vice President, Government Relations
& Regulatory Counsel
ViacomCBS

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Kirsten Mycroft
Global Chief Privacy Officer
BNY Mellon

Vivek Narayanadas
Associate General Counsel & Data Protection Officer
Shopify

Ashley Narsutis
Deputy General Counsel
NextRoll, Inc.

Jill Nissen
President & Founder
Nissen Consulting

Xinru Page
Assistant Professor, Computer Information Systems
Bentley University

Eleonore Pauwels
Director of the AI Lab
Wilson Center

Harriet Pearson
Partner
Hogan Lovells LLP

Bilyana Petkova
Assistant Professor
HBKU College of Law

Peter Petros
General Counsel & Global Privacy Officer
Edelman

Renee Phillips
Counsel Privacy and Cybersecurity
General Motors Company

Future of Privacy Forum Advisory Board (continued)

Andrew Powell
Data Protection Officer
Bank of England

Kalinda Raina
Vice President, Head of Global Privacy
LinkedIn Corporation

MeMe Rasmussen
Vice President of Legal Innovation
Splunk

Katie Ratté
Assistant General Counsel – Privacy
The Walt Disney Company

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
Director of the Center on Law and Information Policy
Fordham University School of Law

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

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

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

Shirley Rooker
President
Call for Action, Inc.

Michelle Rosenthal
Director, Privacy + Data Security, Federal Regulatory Affairs
T-Mobile, Inc.

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

Andy Roth
Chief Privacy Officer
Intuit

Norman Sadeh
Professor, School of Computer Science
Carnegie Mellon University

Neal Schroeder
Senior Vice President Internal Audit, 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

Matt Scutari
Privacy Director
Optimizely

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

Kara Selke
Vice President of Strategic Partners and Privacy
Streetlight Data, Inc.

Emily Sharpe
Director of Policy
World Wide Web Foundation

Linda Sherry
Director, National Priorities
Consumer Action

Kimberly Shur
Global Privacy Officer and Assistant General Counsel
Marriott International

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

Simeon Simeonov
Founder & Chief Technology Officer
Swoop

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

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

Amy Lee Stewart
Senior Vice President, General Counsel and Global Chief Data Ethics Officer
LiveRamp

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
Executive Director
Silicon Flatirons

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

Stephanie Strelau
Associate General Counsel, Product
Magic Leap

Zoe Strickland
Vice President, Global Privacy and U.S. Commercial Compliance
Cigna

Greg Stuart
Chief Executive Officer & President
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

Katherine Tassi
Deputy General Counsel for Privacy and Product
Snap Inc.

Omer Tene
Vice President, Chief Knowledge Officer
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

Ann Toth
Technology Policy Consultant
World Economic Forum

Linda Trickey
Assistant General Counsel, Privacy & Security
Cox Communications

Catherine Tucker
Sloan Distinguished Professor of Management, Professor of Marketing
MIT Sloan

David Vladeck
A.B. Chettle Chair in Civil Procedure
Georgetown University School of Law

Hilary Wandall
Senior Vice President, Privacy Intelligence and General Counsel
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, Inc.

Kevin Werbach
Professor of Legal Studies & Business Ethics
The Wharton School, The University of Pennsylvania

Heather West
Head of Policy, Americas
Mozilla

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

Shane Wiley
Chief Privacy Officer
Cuebiq

Travis Witteveen
Chief Executive Officer
Avira

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 & Co-Founder
LGBT Technology Partnership

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

Dennis Yeoh
VP, Deputy Counsel
VIZIO

Amy Yeung
General Counsel and Chief Privacy Officer
Lotame Solutions, Inc.

Karen Zacharia
Chief Privacy Officer
Verizon Communications, Inc.

Farah Zaman
Vice President, Chief Privacy Officer
Meredith

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, Ph.D.
Associate Professor of Computer Science
Marquette University

List as of January 2020. Please send all updates about this list to Judy Gawczynski at jgawczynski@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.

Antidiscriminatory Privacy

Ignacio N. Cofone

SMU Law Review, Vol. 72 (2019)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3154518

Executive Summary

Law often regulates the flow of information to prevent discrimination. It does so, however, without a theory or framework to determine when doing so is warranted. As a result, these measures produce mixed results. This article offers a framework for determining, with a view of preventing discrimination, when personal information should flow and when it should not. It examines the relationship between precluded personal information, such as race, and the proxies for precluded information, such as names and zip codes. It proposes that the success of these measures depends on what types of proxies exist for the information blocked and it explores in which situations those proxies should also be blocked. This framework predicts the effectiveness of antidiscriminatory privacy rules and offers the potential of a wider protection to minorities.

Author

Ignacio N. Cofone is an Assistant Professor at McGill University's Faculty of Law, where he teaches about privacy law and artificial intelligence regulation, and an Affiliated Fellow at the Yale Law School Information Society Project. His research explores how law should adapt to technological and social change with a focus on information privacy and algorithmic decision-making. Before joining McGill, Ignacio was a research fellow at the NYU Information Law Institute, a resident fellow at the Yale Law School Information Society Project, and a legal advisor for the City of Buenos Aires. He obtained a joint PhD from Erasmus University Rotterdam and Hamburg University, where he was an Erasmus Mundus Fellow, and a JSD from Yale Law School. His full list of publications is available at www.ignaciocofone.com. He tweets from @IgnacioCofone.

Privacy's Constitutional Moment and the Limits of Data Protection

Woodrow Hartzog and Neil M. Richards

Boston College Law Review, Vol. 61 (Forthcoming 2020)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441502

Executive Summary

America's privacy bill has come due. Since the dawn of the Internet, Congress has repeatedly failed to build a robust identity for American privacy law. But now both California and the European Union have forced Congress's hand by passing the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These data protection frameworks, structured around principles for Fair Information Processing called the "FIPs," have industry and privacy advocates alike clamoring for a "U.S. GDPR." States seemed poised to blanket the country with FIP-based laws if Congress fails to act. The United States is thus in the midst of a "constitutional moment" for privacy, in which intense public deliberation and action may bring about constitutive and structural change. And the European data protection model of the GDPR is ascendant.

In this article we highlight the risks of U.S. lawmakers embracing a watered-down version of the European model as American privacy law enters its constitutional moment. European-style data protection rules have undeniable virtues, but they won't be enough. The FIPs assume data processing is always a worthy goal, but even fairly processed data can lead to oppression and abuse. Data protection is also myopic because it ignores how industry's appetite for data is wrecking our environment, our democracy, our attention spans, and our emotional health. Even if E.U.-style data protection were sufficient, the United States is too different from Europe to implement and enforce such a framework effectively on its European law terms. Any U.S. GDPR would in practice be what we call a "GDPR-Lite."

Our argument is simple: In the United States, a data protection model cannot do it all for privacy, though if current trends continue, we will likely entrench it as though it can. Drawing from constitutional theory and the traditions of privacy regulation in the United States, we propose instead a "comprehensive approach" to privacy that is better focused on power asymmetries, corporate structures, and a broader vision of human well-being. Settling for an American GDPR-lite would be a tragic ending to a real opportunity to tackle the critical problems of the information age. In this constitutional moment for privacy, we can and should demand more. This article offers a path forward to do just that.

Authors

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences. He is also a Resident Fellow at the Center for Law, Innovation and Creativity (CLIC) at Northeastern University, a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University, a Non-resident Fellow at The Cordell Institute for Policy in Medicine & Law at Washington University, and an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research on privacy, media, and robotics has been published in scholarly publications such as the *Yale Law Journal*, *Columbia Law Review*, and *California Law Review* and popular publications such as *The New York Times*, *The Washington Post*, and *The Guardian*. He has testified multiple times before Congress and has been quoted or referenced by numerous media outlets, including *NPR*, *BBC*, and *The Wall Street Journal.* He is the author of *Privacy's Blueprint*: *The Battle to Control the Design of New Technologies*, published in 2018 by Harvard University Press. His book with Daniel Solove, *Breached!*: *Why Data Security Law Fails and How to Improve It*, is under contract with Oxford University Press.

Neil M. Richards is one of the world's leading experts in privacy law, information law, and freedom of expression. He writes, teaches, and lectures about the regulation of the technologies powered by human information that are revolutionizing our society. Professor Richards holds the Koch Distinguished Professor in Law at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine & Law. He is also an affiliate scholar with the Stanford Center for Internet and Society and the Yale Information Society Project, a Fellow at the Center for Democracy and Technology, and a consultant and expert in privacy cases. Professor Richards serves on the board of the Future of Privacy Forum and is a member of the American Law Institute. Professor Richards graduated in 1997 with graduate degrees in law and history from the University of Virginia, and served as a law clerk to both William H. Rehnquist, Chief Justice of the United States and Paul V. Niemeyer, United States Court of Appeals for the Fourth Circuit.

Professor Richards is the author of Intellectual Privacy (Oxford Press 2015). His many scholarly and popular writings on privacy and civil liberties have appeared in a wide variety of media, from the Harvard Law Review and the Yale Law Journal to The Guardian, WIRED, and Slate. His next book, Why Privacy Matters, will be published by Oxford Press in 2020. Professor Richards regularly speaks about privacy, big data, technology, and civil liberties throughout the world, and also appears frequently in the media. At Washington University, he teaches courses on privacy, technology, free speech, and constitutional law, and is a past winner of the Washington University School of Law's Professor of the Year award. He was born in England, educated in the United States, and lives with his family in St. Louis. He is an avid cyclist and a lifelong supporter of Liverpool Football Club.

Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations

Margot E. Kaminski and Gianclaudio Malgieri

University of Colorado Law Legal Studies Research Paper No. 19-28 (2019)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224

Executive Summary

Policy-makers, scholars, and commentators are increasingly concerned with the risks of using profiling algorithms and automated decision-making. The EU's General Data Protection Regulation (GDPR) has tried to address these concerns through an array of regulatory tools. As one of us has argued, the GDPR combines individual rights with systemic governance, towards algorithmic accountability. The individual tools are largely geared towards individual "legibility": making the decision-making system understandable to an individual invoking her rights. The systemic governance tools, instead, focus on bringing expertise and oversight into the system as a whole, and rely on the tactics of "collaborative governance," that is, use public-private partnerships towards these goals. How these two approaches to transparency and accountability interact remains a largely unexplored question, with much of the legal literature focusing instead on whether there is an individual right to explanation.

The GDPR contains an array of systemic accountability tools. Of these tools, impact assessments (Art. 35) have recently received particular attention on both sides of the Atlantic, as a means of implementing algorithmic accountability at early stages of design, development, and training. The aim of this paper is to address how a Data Protection Impact Assessment (DPIA) links the two faces of the GDPR's approach to algorithmic accountability: individual rights and systemic collaborative governance. We address the relationship between DPIAs and individual transparency rights. We propose, too, that impact assessments link the GDPR's two methods of governing algorithmic decision-making by both providing systemic governance and serving as an important "suitable safeguard" (Art. 22) of individual rights.

After noting the potential shortcomings of DPIAs, this paper closes with a call — and some suggestions — for a Model Algorithmic Impact Assessment in the context of the GDPR. Our examination of DPIAs suggests that the current focus on the right to explanation is too narrow. We call, instead, for data controllers to consciously use the required DPIA process to produce what we call "multi-layered explanations" of algorithmic systems. This concept of multi-layered explanations not only more accurately describes what the GDPR is attempting to do, but also normatively better fills potential gaps between the GDPR's two approaches to algorithmic accountability.

Authors

Margot E. Kaminski is an Associate Professor at the University of Colorado Law and the Director of the Privacy Initiative at Silicon Flatirons. She specializes in the law of new technologies, focusing on information governance, privacy, and freedom of expression. Recently, her work has examined autonomous systems, including AI, robots, and drones (UAS). In 2018, she researched comparative and transatlantic approaches to sensor privacy in the Netherlands and Italy as a recipient of the Fulbright-Schuman Innovation Grant. Her academic work has been published in UCLA Law Review, Minnesota Law Review, Boston University Law Review, and Southern California Law Review, among others, and she frequently writes for the popular press.

Prior to joining Colorado Law, Margot was an Assistant Professor at the Ohio State University Moritz College of Law (2014-2017), and served for three years as the Executive Director of the Information Society Project at Yale Law School, where she remains an affiliated fellow. She is a co-founder of the Media Freedom and Information Access (MFIA) Clinic at Yale Law School. She served as a law clerk to the Honorable Andrew J. Kleinfeld of the Ninth Circuit Court of Appeals in Fairbanks, Alaska.

Gianclaudio Malgieri is a doctoral researcher at the "Law, Science, Technology and Society" center of Vrije Universiteit Brussel, Attorney in Law and Training Coordinator of the Brussels Privacy Hub. He is Work Package Leader of the EU *Panelfit* Research Project, about Legal & Ethical issues of data processing in the research sector. He is also external expert of the EU Commission for the ethics and data protection assessment of EU research proposals. He has authored more than 40 publications in leading international law reviews and is deputy editor of *Computer, Law and Security Review* (Elsevier). He is lecturer of Data Protection Law and Intellectual Property for undergraduate and professional courses at the University of Pisa, Sant'Anna School of Advanced Studies and Strasbourg University. He got an LLM with honours at the University of Pisa and a JD with honours at Sant'Anna School of Advanced Studies of Pisa (Italy). He was visiting researcher at the Oxford University, London School of Economics, World Trade Institute of the University of Bern and École Normale Superieure de Paris.

Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites

Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan

Proceedings of the ACM on Human-Computer Interaction, Vol. 3, CSCW, Article 81 (2019)
Available at: https://arxiv.org/abs/1907.07032

Executive Summary

Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving consumers into making decisions that—if fully informed and capable of selecting alternatives—they might not make. Such interfaces have serious implications for consumer privacy. They trick consumers into giving up vast amounts of personal information. They enable creating compulsive and addictive feedback loops by using the collected information to manipulate consumer behavior. Dark patterns also undermine notice and choice privacy paradigms, contribute to the "privacy paradox", and allow online services to continue their privacy-invasive practices under the guise of privacy-respecting design.

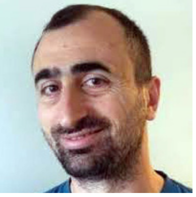
In *Dark Patterns at Scale*, we present automated techniques that enable experts to identify dark patterns on a large set of websites. Using these techniques, we surveyed shopping websites, which often use dark patterns to influence consumers into making more purchases or disclosing more information than they would otherwise. Analyzing ~53K product pages from ~11K shopping websites, we discovered 1,818 dark pattern instances, together representing 15 types and 7 broader categories. Amongst the privacy-invasive patterns, we documented many websites that used "Trick Questions" (confusing language that steers consumers into consenting) and "Forced Action" (coercing consumers to create accounts or share their information in order to continue using a service).

We also discovered that many dark patterns are enabled by third-party entities present on websites. We compiled a list of 22 such entities, two of which openly advertised practices that enable deceptive messages. Finally, we developed a taxonomy of dark pattern characteristics that classifies the underlying influence of dark patterns along five dimensions: asymmetric, covert, deceptive, information hiding, and restrictive.

While our study paints a dismal picture of the state of dark patterns on the web, it also points to ways in which researchers can design and build technical solutions to protect consumers. It also highlights that many of the dark patterns we discovered are already considered unlawful under various laws around the world. Our automated approach is also an aid to regulators, who can use them to study, mitigate, and minimize the use of dark patterns.

Authors

Arunesh Mathur is a graduate student in the department of computer science at Princeton University, where he is affiliated with the Center for Information Technology Policy (CITP). Mathur's research examines how technical systems interface with and impact society in negative ways. His current research focus is dark patterns: empirically studying how commercial, political, and other powerful actors employ user interface design principles to exploit individuals, markets, and democracy. His research has won multiple awards including the best paper awards at ACM CSCW 2018 and USENIX SOUPS 2019.



Gunes Acar is a FWO postdoctoral fellow at KU Leuven's COSIC research group. His research interests involve web tracking measurement, anonymous communications, and IoT privacy and security. Gunes obtained his PhD at KU Leuven in 2017, and was a postdoctoral researcher between 2017 and 2019 at Princeton University's Center for Information Technology Policy.

Michael Friedman is a Technical Program Manager at Google. His work focuses on monitoring compliance with privacy regulations and certifications. Michael is broadly interested in the privacy implications of information technology and the enforcement of privacy standards. He earned his Bachelor's degree in Computer Science at Princeton University with a concentration in societal implications of information technology. While there, he conducted research on the effectiveness of technology privacy policies, with a focus on children's data privacy. He also collaborated in this work on dark patterns.

Elena Lucherini is a second-year Ph.D. student at the Center for Information Technology Policy at Princeton University. Her advisor is Arvind Narayanan. Lucherini received her bachelor's degree from University of Pisa and her master's from University of Pisa and Sant'Anna School of Advanced Studies.

Jonathan Mayer is an Assistant Professor at Princeton University, where he holds appointments in the Department of Computer Science and the Woodrow Wilson School of Public and International Affairs. Before joining the Princeton faculty, he served as the technology law and policy advisor to United States Senator Kamala Harris and as the Chief Technologist of the Federal Communications Commission Enforcement Bureau. Professor Mayer's research centers on the intersection of technology and law, with emphasis on national security, criminal procedure, and consumer privacy. He is both a computer scientist and a lawyer, and he holds a Ph.D. in computer science from Stanford University and a J.D. from Stanford Law School.

Marshini Chetty is an assistant professor in the Department of Computer Science at the University of Chicago. She specializes in human-computer interaction, usable privacy and security, and ubiquitous computing. Marshini designs, implements, and evaluates technologies to help users manage different aspects of Internet use from privacy and security to performance, and costs. She often works in resource-constrained settings and uses her work to help inform Internet policy. She has a Ph.D. in Human-Centered Computing from Georgia Institute of Technology, USA and a Masters and Bachelors in Computer Science from the University of Cape Town, South Africa. In her former roles, Marshini was on the faculty in the Computer Science Department at Princeton University and the College of Information Studies at the University of Maryland, College Park. Her work has won best paper awards at SOUPS, CHI, and CSCW and has been funded by the National Science Foundation, the National Security Agency, Intel, Microsoft, Facebook, and multiple Google Faculty Research Awards.

Arvind Narayanan is an Associate Professor of Computer Science at Princeton. He leads the Princeton Web Transparency and Accountability Project to uncover how companies collect and use our personal information. Narayanan is the lead author of a textbook on Bitcoin and cryptocurrency technologies which has been used in over 150 courses around the world. His doctoral research showed the fundamental limits of de-identification, for which he received the Privacy Enhancing Technologies Award. His 2017 paper in *Science* was among the first to show how machine learning reflects cultural stereotypes, including racial and gender biases. Narayanan is a recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE).

The Many Revolutions of Carpenter

Paul Ohm

Harvard Journal of Law & Technology, Vol. 32, Issue 2 (2019)
Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech357.pdf

Executive Summary

The Supreme Court's opinion in Carpenter v. United States has been heralded by many as a milestone for the protection of privacy in an age of rapidly changing technology. Despite this, scholars and commentators have failed to appreciate many of the important aspects of this landmark opinion. Carpenter works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more.

The most obvious revolution is the case's basic holding—information about the location of cell phone customers held by cell phone providers is now protected by the Fourth Amendment, at least when the police seek seven days or more of such information. For the first time, the Court has held that the police must secure a warrant to require a business to divulge information about its customers compiled for the business's purposes, reinventing the reasonable expectation of privacy test and significantly narrowing what is known as the third-party doctrine. This cell-site location information ("CSLI") has become a key source of evidence for criminal investigations, so this holding will revolutionize the way the police build their cases, requiring a warrant where none has been required before.

Beyond CSLI, under Carpenter, databases that can be used, directly or indirectly, to ascertain the precise location of individuals over time are likely now covered by the Fourth Amendment. The police will probably need a warrant to obtain location information collected by mobile apps, fitness trackers, connected cars, and many so-called "quantified self" technologies.

The reasoning extends beyond location information, as the opinion promulgates a new, multi-factor test that will likely cover other commercially significant data that the police have begun to access in its investigations. Massive databases of web browsing habits stored by internet service providers (ISPs) will probably now require a warrant to access. Perhaps most surprisingly, the majority's reasoning will apply even to massive databases of telephone dialing and banking records, cutting back on the holdings of two cases, Smith v. Maryland and Miller v. United States, that the Carpenter Court expressly declined to overrule.

The last revolution is a revolution of legal reasoning. In his opinion, the Chief Justice evinces, as he did in the majority opinion in Riley v. California, a profound tech exceptionalism. Recent advances in information technology are different in kind, not merely in degree from what has come before. This idea finds substantial support in two decades of legal scholarship about threats from technology to information privacy, work that has never before received such a profound endorsement from the Supreme Court.

Carpenter is an inflection point in the history of the Fourth Amendment. From now on, we will be talking about what the Fourth Amendment means in pre-Carpenter and post-Carpenter terms. It will be considered as important as Olmstead and Katz in the overall arc of technological privacy.

Author

Paul Ohm is a Professor of Law and the Associate Dean for Academic Affairs at the Georgetown University Law Center, where he also serves as a faculty director for the Center on Privacy & Technology and the Institute for Technology Law & Policy. His writing and teaching focuses on information privacy, computer crime law, intellectual property, and criminal procedure. A computer programmer and computer scientist as well as a lawyer, Professor Ohm tries to build new interdisciplinary bridges between law and computer science, and much of his scholarship focuses on how evolving technology disrupts individual privacy.

Professor Ohm began his academic career on the faculty of the University of Colorado Law School, where he also served as Associate Dean and Faculty Director for the Silicon Flatirons Center. From 2012 to 2013, Professor Ohm served as Senior Policy Advisor to the Federal Trade Commission. Before becoming a professor, he worked as an Honors Program trial attorney in the U.S. Department of Justice's Computer Crime and Intellectual Property Section and a law clerk to Judge Betty Fletcher of the United States Court of Appeals for the Ninth Circuit and Judge Mariana Pfaelzer of the United States District Court for the Central District of California. He is a graduate of the UCLA School of Law.

Awarded Student Paper

Privacy Attitudes of Smart Speaker Users

Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner

Proceedings on Privacy Enhancing Technologies (PoPETs), Vol. 2019, Issue 4 (2019)
Available at: https://dx.doi.org/10.2478/popets-2019-0068

Executive Summary

Smart speakers (such as Amazon Echo, Google Home, and Apple HomePod) are increasingly widespread consumer devices, with hundreds of millions sold. They also have significant privacy implications, since they are always-on microphones located inside people's homes. To explore how users think about the privacy of this emerging technology, we surveyed smart speaker owners about their beliefs, attitudes, and concerns about the recordings that are made and shared by their devices.

Rather than collecting respondents' opinions abstractly, we grounded participants' responses in concrete interactions with their devices. We did this by randomly selecting five recordings that the user's device had stored, then having the participant listen and answer questions about them. Our survey included 116 owners of Amazon and Google smart speakers, who listened to a total of 580 distinct recordings.

Our results contain several important findings:

People exhibited a notable lack of knowledge about the behavior and features of their devices. Almost half did not know that their recordings were being permanently stored and that they could review them; many expressed surprise when they found out about this. Only a quarter of participants reported reviewing interactions, and very few had ever deleted any.

Respondents expressed dissatisfaction with current retention policies. Currently, by default, interactions are stored forever. However, a significant majority of participants felt that recordings should be stored for only a limited amount of time and then automatically deleted. Many said that they would find it unacceptable for humans to listen to their recordings. Yet (after our study had ended), media investigations revealed that this was a widespread practice among all intelligent voice assistants.

Most currently-stored data was not considered sensitive, since, today, typical interactions involve only basic commands and instructions. However, participants who heard children or guests in their recordings reported being much more concerned and were considerably less comfortable with their voices being stored, suggesting that these groups require extra protection.

Participants expected their data to be used only for the purpose of carrying out the commands they issued to their smart speaker. Respondents were strongly opposed to the use of their data by third parties and for advertising.

Based on these results, we suggest that:

- Consumers need to be better informed about what happens to their data
- Companies should make their retention policies more limited by default
- Regulators ought to enforce that data flows conform with consumers' expectations

Authors

Nathan Malkin is a PhD student in computer science at the University of California, Berkeley, where he is advised by Serge Egelman and David Wagner. His research focuses on understanding how human factors can lead to problems for privacy and security, and designing systems to overcome these challenges. He has published work on understanding privacy requirements for smart speakers and smart TVs, as well as drawing on behavioral economics to help users make security decisions while avoiding cognitive biases. He has also studied how users protect their smartphones, why people delay updating software, and how to improve anonymity software.

Joe Deatrick obtained his Bachelors in Computer Science from the University of California, Berkeley in 2019. While pursuing his Bachelors he conducted research for the Berkeley Lab for Usable and Experimental Security (BLUES) with a focus on privacy research. His main academic interests are in privacy and cryptography. Joe joined the Security Engineering team at Tesla this past December and is working on the development of embedded software security systems from vehicles to servers. He is currently working on data protection improvements for securing sensitive Tesla IP.

Allen Tong is an undergraduate studying computer science at UC Berkeley. Allen is a member of the Berkeley Laboratory for Usable and Experimental Security (BLUES) directed by Dr. Serge Egelman, where his research interests include web security and online privacy.

Primal Wijesekera is a staff research scientist in the Usable Security and Privacy research group at ICSI and also holds an appointment in the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. His research focuses on exposing current privacy vulnerabilities and providing systematic solutions to meet privacy expectations of consumers. He has extensive experience in mobile app analysis for privacy violations and implementing privacy protections for Android. He has published in top-tier security venues (IEEE S&P, Usenix Security) and usable security and privacy venues (ACM CHI, SOUPS, PETS). He received his Ph.D. from the University of British Columbia. He also has a Masters from UBC in Distributed Systems and a BSc in CS from the University of Colombo, Sri Lanka.

Serge Egelman is Research Director of the Usable Security & Privacy Group at the International Computer Science Institute (ICSI) and also holds an appointment in the Department of Electrical Engineering and Computer Sciences (EECS) at the University of California, Berkeley. He leads the Berkeley Laboratory for Usable and Experimental Security (BLUES), which is the amalgamation of his ICSI and UCB research groups. Serge's research focuses on the intersection of privacy, computer security, and human-computer interaction, with the specific aim of better understanding how people make decisions surrounding their privacy and security, and then creating data-driven improvements to systems and interfaces. This has included human subjects research on social networking privacy, access controls, authentication mechanisms, web browser security warnings, and privacy-enhancing technologies. His work has received multiple best paper awards, including seven ACM CHI Honorable Mentions, the 2012 Symposium on Usable Privacy and Security (SOUPS) Distinguished Paper Award for his work on smartphone application permissions, as well as the 2017 SOUPS Impact Award, and the 2012 Information Systems Research Best Published Paper Award for his work on consumers' willingness to pay for online privacy. He received his PhD from Carnegie Mellon University and prior to that was an undergraduate at the University of Virginia. He has also performed research at NIST, Brown University, Microsoft Research, and Xerox PARC.

David Wagner is a Professor in the Computer Science Division at the University of California at Berkeley with extensive experience in computer security and cryptography. He and his Berkeley colleagues are known for discovering a wide variety of security vulnerabilities in various cellphone standards, 802.11 wireless networks, and other widely deployed systems. In addition, David was a co-designer of one of the Advanced Encryption Standard candidates, and he remains active in the areas of computer security, cryptography, and privacy. David is currently active in studying mobile security and smartphone security, especially security for apps on platforms such as Android, iPhone, and others. David also studies web security and other topics related to security on the Internet. David also studies e-voting security. In 2004, David co-authored an analysis of SERVE, an Internet voting system proposed by the Pentagon for overseas and military voters. The report, which described multiple security flaws in the system, led to the project's cancellation. David is a member of the federal advisory committee tasked with developing standards for next-generation voting systems.

Honorable Mentions

Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps

Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On, and Irwin Reyes

Berkeley Technology Law Journal, Vol. 35 (2020)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3464667

Executive Summary

"Paid" digital services have been touted as straightforward alternatives to the ostensibly "free" model, in which users actually face a high price in the form of personal data, with limited awareness of the real cost incurred and little ability to manage their privacy preferences. Yet the actual privacy behavior of paid services, and consumer expectations about that behavior, remain largely unknown.

This Article addresses that gap. It presents empirical data both comparing the true cost of "paid" services as compared to their so-called "free" counterparts, and documenting consumer expectations about the relative behaviors of each.

We first present an empirical study that documents and compares the privacy behaviors of 5,877 Android apps that are offered both as free and paid versions. The sophisticated analysis tool we employed, AppCensus, allowed us to detect exactly which sensitive user data is accessed by each app and with whom it is shared. Our results show that paid apps often share the same implementation characteristics and resulting behaviors as their free counterparts. Thus, if users opt to pay for apps to avoid privacy costs, in many instances they do not receive the benefit of the bargain. Worse, we find that there are no obvious cues that consumers can use to determine when the paid version of a free app offers better privacy protections than its free counterpart.

We complement this data with a second study: surveying 1,000 mobile app users as to their perceptions of the privacy behaviors of paid and free app versions. Participants indicated that consumers are more likely to expect the paid version to engage in privacy-protective practices, to demonstrate transparency with regard to its data collection and sharing behaviors, and to offer more granular control over the collection of user data in that context.

Together, these studies identify ways in which the actual behavior of apps fails to comport with users' expectations, and the way that representations of an app as "paid" or "ad-free" can mislead users. They also raise questions about the salience of those expectations for consumer choices.

In light of this combined research, we then explore three sets of ramifications for policy and practice.

First, our findings that paid services often conduct equally extensive levels of data collection and sale as free ones challenges understandings about how the "pay for privacy" model operates in practice, its promise as a privacy-protective alternative, and the legality of paid app behavior.

Second, our findings support research into ways that users' beliefs about technology business models and developer behavior are actually shaped, undermining the legitimacy of legal regimes relying on fictive user "consent" that does not reflect knowledge of actual market behavior.

Third, our work provides technical tools for offering transparency about app behaviors, empowering consumers and regulators. law enforcement, consumer protections organizations, and private parties seeking to remedy undesirable or illegal privacy behavior in the most dominant example of a free vs. paid market—mobile apps—where there turns out to be no real privacy-protective option.

Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?

Lilian Mitrou

SSRN (2018)
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914

Executive Summary

Artificial Intelligence (AI)—in its interplay with Big Data, Internet of Things, ambient intelligence and cloud computing—augments the existing major, qualitative and quantitative, shift regarding the processing of personal information. Personal data and AI are “a two-way street”: personal data feeds AI and AI produces more inferred data. AI may affect privacy in various aspects: informational privacy, including surveillance privacy, but also the autonomy of a person.

The questions that arise are of crucial importance both for the development of AI and the efficiency of data protection arsenal: Is the current legal framework AI-proof? Are the data protection and privacy rules and principles adequate to deal with the challenges of AI or do we need to elaborate new principles to work alongside the advances of AI technology?

Our research focuses on the assessment of the European data protection framework, the General Data Protection Regulation (GDPR) that, however, does not specifically address AI, as the regulatory choice consisted more in what we perceive as “technology–independent legislation.” The paper gives a critical overview and assessment of the provisions of GDPR that are relevant for the AI-environment, i.e. the scope of application, the legal grounds with emphasis on consent, the reach and applicability of data protection principles and the new (accountability) tools to enhance and ensure compliance.

In this respect, we discuss the requirements of fair processing in the context of AI applications. Fairness concerns are raised with reference to biased algorithms that may lead to inaccurate or—mostly—discriminating outcomes. We suggest that fairness is linked to processing of personal data in an ethical manner, involves the requirement of values-sensible design/responsible (research and) innovation and goes beyond the transparency obligations. Addressed are also the issues raised by the purpose limitation principle and the data minimization principle, which seem to be at odds with AI processing capabilities. We highlight the transparency element that is articulated as a need to face the “opacity of the algorithm.” Complying with transparency obligations is related to major difficulties regarding the accessibility and comprehensibility of information. Emphasis is given to the new principle/tool of accountability, which refers also to the ability to explain the AI processing and the outcome thereof.

Further, we discuss the introduction of Data Protection Impact Assessment as an innovative element of GDPR that may serve to respond also proactively to unforeseen technological challenges and anticipate and/or mitigate the respective risks. In this context we refer also to data protection by design, a new requirement of GDPR that compels data controllers and systems/applications designers to embed legal principles and norms in the technological architecture. Such a framework should anticipate both intended and unintended impacts of technology. Finally, we deal with the relation between GDPR legal requirements and AI Ethics: even if balancing as core part of decision making with regard to data processing, does not consist in ethical assessments, we propose to include also the examination of an ethical perspective.

Honorable Mentions

Usable and Useful Privacy Interfaces

Florian Schaub and Lorrie Faith Cranor

Chapter to appear in: *An Introduction to Privacy for Technology Professionals*, published by the IAPP (2020)
Available at: https://iapp.org/media/pdf/certification/IAPP-Intro-to-Privacy-for-Tech-Prof-SAMPLE.pdf

Executive Summary

The design of a system or technology affects and shapes how people interact with it. Privacy engineering and user experience design frequently intersect. Privacy laws and regulations require that data subjects are informed about a system's data practices, asked for consent, and given access to their own data.

However, too often privacy notices are not readable, people do not understand what they consent to, and people are not aware of certain data practices or the privacy controls available to them. An emphasis on meeting legal and regulatory obligations alone is not sufficient to create privacy interfaces that are *usable* and *useful* for users. Usable means that people can find, understand and successfully use provided privacy information and controls. Useful means that privacy information and controls align with users' privacy needs. This chapter provides insights on why it can be difficult to design privacy interfaces that are usable and useful, by discussing how people make privacy decisions and what drives their privacy concerns and behavior. We further discuss common usability issues in privacy interfaces, and describe a set of privacy design principles and a user-centric process for designing usable and effective privacy interfaces, including guidance and best practices for user-centric privacy design that meets both legal obligations and users' needs. Designing effective privacy user experiences not only makes it easier for users to manage and control their privacy, but also benefits organizations by minimizing surprise for their users and facilitating user trust. Importantly, a privacy notice or control is not just a compliance tool but an *opportunity* to engage with users about privacy, to explain the rationale behind practices that may seem invasive without proper context, to make users aware of potential privacy risks, and to communicate the measures taken to mitigate those risks and protect users' privacy.

Privacy laws, privacy technology, and privacy management are typically centered on information—how information is collected, processed, stored, transferred, how information can and must be protected, and how to ensure compliance and accountability. To be effective, designing privacy user experiences requires a shift in focus: while information and compliance are of course still relevant, user-centric privacy design focuses on people, their privacy needs, and their interaction with a system's privacy interfaces.

The design of usable privacy notices and controls is not trivial, but this chapter describes why it is important to invest in getting the privacy user experience right—making sure that privacy information and controls are not only compliant with regulation but also address and align with users' needs. Careful design can support users in developing an accurate and more complete understanding of a system and its data practices. Well-designed and user-tested privacy interfaces provide the confidence that an indication of consent was indeed an informed and freely-given expression by the user. Highlighting unexpected data practices and considering secondary and incidental users reduces surprise for users and hopefully prevents privacy harms, media outcries, and regulatory fines.

Thank you to our 2019 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 policymaking. For more information, visit fpf.org/privacy-papers-for-policy-makers/.

Advisory Board Reviewers

Joe Ashkouti
Change Healthcare

John Breyault
National Consumers League

Stuart Brotman
Woodrow Wilson International Center for Scholars

Maureen Cooney
Sprint

Mark Crosbie
Dropbox

Michael Dolan
Best Buy

Philip Fabinger
HERE

Jonathan Fox
Cisco

John Grant
Palantir

Barbara Lawler
Looker Data Sciences

Lisa Martinelli
Highmark Health

Winston Maxwell
Telecom ParisTech

Vivek Narayanadas
Shopify

Michelle Richardson
Center for Democracy and Technology

Alexandra Ross
Autodesk, Inc.

Matt Scutari
Optimizely

Kara Selke
Streetlight Data, Inc.

Heather West
Mozilla

Shane Witnov
Facebook, Inc.

Finalist Judges

Mark MacCarthy
Senior Fellow and Adjunct Professor, Georgetown Law
Senior Policy Fellow, Center for Business and Public Policy, Georgetown's McDonough School of Business
Senior Fellow, Future of Privacy Forum

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

Jules Polonetsky
CEO, Future of Privacy Forum

PRIVACY PAPERS FOR POLICYMAKERS 2019

FUTURE OF PRIVACY FORUM

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