PRIVACY PAPERS FOR POLICYMAKERS

2020

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 10, 2021

We are pleased to introduce FPF's 11th 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 explores the legal and policy questions related to a new era of student surveillance, which is being fueled by machine learning.
- Another paper sets out proposals for how Asian stakeholders may promote greater consistency between their respective laws and regulations on international transfers of personal data in the region.
- A third paper discusses the human rights implications of technologies like virtual reality and augmented reality, as well as actions that the industry and lawmakers can take to preserve human rights.
- A fourth paper provides a comprehensive account of the ways in which privacy impacted technological and public health responses to the COVID-19 crisis to expose the need for reforms in privacy law.
- Another paper evaluates the recent Schrems II decision and proposes ways that U.S. surveillance law can be adapted to meet the standards of the European Court of Justice and establish a lasting foundation for data transfers in trans-Atlantic commerce.
- The sixth winning paper urges the creation of fiduciary relationships between consumers and companies that would increase company liability for data protection failures.

For the fifth year in a row, we are proud to continue highlighting student work by honoring another excellent paper. The winning paper *Personal Identifiability of User Tracking Data During Observation of 360-Degree VR Video* (Miller, *et al.*) offers insight into how using only the position tracking data, they found that even with more than 500 participants to choose from, a simple machine learning model can identify participants from less than five minutes of tracking data at above 95% accuracy.

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

Chris Wolf

Christopher Wolf
Chairman, FPF Board of Directors

Jules Polonetsky

Jules Polonetsky
Chief Executive Officer, FPF

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
Privacy and Ethics Leader
PricewaterhouseCoopers LLP

Vivienne Artz
Chief Privacy Officer
Refinitiv

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

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 and Technology
University of California Berkeley School of Law

Kabir Barday
Founder, President, & Chief Executive Officer
OneTrust

Kelby Barton
General Counsel
Avast

Alisa Bergman
Vice President, Chief Privacy Officer
Adobe Systems Inc.

Elise Berkower (1957–2017)
Associate General Counsel
Nielsen

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

Douglas Bloom
Executive Director and Co-Head of Cybersecurity
and Privacy
Morgan Stanley

Brent Bombach
Senior Director, Government Relations and Public Policy
NEC Corporation of America

Axel du Boucher
Group Data Protection Officer
Criteo

Claire Borthwick
Senior Counsel
GoGuardian

Claire McKay Bowen, Ph.D.
Lead Data Scientist, Privacy and Data Security
Urban Institute

Bruce Boyden
Assistant Professor of Law
Marquette University

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

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 N. Brotman
Howard Distinguished Endowed Professor
University of Tennessee, Knoxville

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

Andres Castrillon
Senior Manager, Federal Government Relations
Stellantis

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

Anupam Chander
Professor of Law
Georgetown University

Mary Chapin
Chief Legal Officer, Vice President & Corporate Secretary
National Student Clearinghouse

Danielle Keats Citron
Jefferson Scholars Foundation Schenck
Distinguished Professor in Law
University of Virginia School of Law
FPF Senior Fellow
Member, FPF Education & Innovation Foundation
Board of Directors

Sheila Colclasure
Global Chief Digital Responsibility and Public Policy Officer
IPG Kinesso

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

Megan Cristina
Vice President & Chief Legal Officer
Slack

Mark Crosbie
Data Protection Officer
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

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

Andy Dale
General Counsel, Head of Strategic Partnerships
Alyce

Laurie Dechery
Associate General Counsel
Shutterfly, Inc.

Jolynn Dellinger
Stephen and Janet Bear Visiting Lecturer and Kenan
Senior Fellow
The Kenan Institute for Ethics at Duke University

Sara DePaul
Associate General Counsel and Senior Director of
Technology Policy
Software & Information Industry Association

Michael Dolan
Senior Director, Head of Enterprise Privacy
Best Buy

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

Peggy Eisenhauer
Founder
Privacy & Information Management Services

Jimma Elliott-Stevens
General Counsel, Chief Compliance & Privacy Officer
Thomson Reuters

Keith Enright
Chief Privacy Officer
Google

Kristen Erbes
Chief Privacy Officer
Cambia Health Solutions

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
William Donald Bain Family Professor of Law
Washington & Lee University School of Law

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 François
Managing Director, Global Chief Privacy Officer
JPMorgan Chase

Dona Fraser
Senior Vice President, Privacy Initiatives
BBB National Programs

Leigh Parsons Freund
President & Chief Executive Officer
Network Advertising Initiative

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

Kelly Gertridge
Head of Privacy
Atlassian

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

John Gevertz
Senior Vice President, Chief Privacy Officer
Visa

Shoshana Gillers
Chief Privacy Officer
TransUnion

Carolina Giuga
Director, Government & Public Affairs, Americas
LEGO

Eric Goldman
Associate Dean of Research, Professor of Law and
Co-Director, High Tech Law Institute
Santa Clara University School of Law

Melissa M. Goldstein
Associate Professor, Department of Health Policy
and Management
George Washington University Law School

Scott Goss
Vice President, Privacy Counsel
Qualcomm

John Grant
Civil Liberties Engineer
Palantir Technologies

Meredith Grauer
Chief Privacy Officer
Nielsen

Kimberly Gray
Chief Privacy Officer, Global
IQVIA

Lynn Haaland
Deputy General Counsel, Chief Compliance and
Ethics Officer, Chief Privacy Officer
Zoom Video Communications

Future of Privacy Forum Advisory Board (continued)

Sara Harrington
Legal - Head of Users, Product & Privacy
Stripe

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

Eric Heath
Vice President, Deputy General Counsel and Chief Privacy Officer
Ancestry

Rita Heimes
General Counsel and Chief Privacy Officer
IAPP - International Association of Privacy Professionals

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

Eileen Hershenov
Senior Vice President, Policy
Anti-Defamation League

Beth Hill
General Counsel, Chief Compliance Officer and Privacy Leader
FordDirect

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

David Hoffman
Associate General Counsel and Senior Director of Data Policy Strategy
Intel Corporation

Lara Kehoe Hoffman
Vice President, Privacy & Security Legal
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, Global Privacy
Apple, Inc.

Margaret Hu
Professor of Law and International Affairs
Pennsylvania State University

Doug Hudson
Vice President & Assistant General Counsel
Etsy

Sandra Hughes
Chief Executive Officer and President
Sandra Hughes, Ltd.
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 Tow-Knight Center for Entrepreneurial Journalism
City University of New York

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

Meg Leta Jones
Associate Professor
Georgetown University

Mark Kahn
General Counsel and Vice President of Policy
Segment

Damien Kieran
Chief Privacy Officer and Global Data Protection Officer
Twitter

Anne Klinefelter
Director of the Law Library, Henry P. Brandis Distinguished Professor of Law
University of North Carolina

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

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

Michael C. Lamb
Chief Privacy Officer
RELX Group

Anastasia Lang
Senior Vice President, General Counsel
Magic Leap

Elaine Laughlin
Director Of Development
WSBE Rhode Island PBS
Member, FPF Education and Innovation Foundation Board of Directors

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

Peter Lefkowitz
Vice President, Chief Privacy & Digital Risk Officer
Citrix Systems

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

Matt Levine
General Counsel & Chief Privacy Officer
CLEAR

Barbra Levy
Senior Counsel, Privacy
Samsung Electronics America

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

Caroline Louveaux
Chief Privacy Officer
Mastercard

Doug Luftman
Vice President & Deputy General Counsel, Product, IP and Regulatory Affairs
DocuSign

Brendon Lynch
Chief Privacy Officer
Airbnb

Mark MacCarthy
Senior Fellow and Adjunct Professor
Georgetown University

Knut Mager
Head Global Data Privacy
Novartis International

Larry Magid
President & Chief Executive Officer
Connect Safely

Kirsten Martin, Ph.D.
William P. and Hazel B. White Center Professor of Technology Ethics
University of Notre Dame – Mendoza College of Business

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

Matthias Matthiesen
Head of Privacy
Quantcast

Winston Maxwell
Director of Law & Digital Technology
Telecom ParisTech

Michael McCullough
Chief Privacy Officer & Governance, Risk Management, and Compliance Leader
Macy's, Inc.

William McGeveran
Associate Dean for Academic Affairs and 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

Edward McNicholas
Partner
Ropes & Gray LLP

David Medine
Consultant

Suzanne Miklos
Chief Privacy Officer and Assistant General Counsel - IT, Data, Real Estate and Legal Operations
General Motors Company

John S. Miller
Senior Vice President of Policy and Senior Counsel
Information Technology Industry Council

Douglas Miller
Vice President, Global Privacy and Trust
Verizon Media

Christina Montgomery
Vice President & Chief Privacy Officer
IBM

Cassandra Moons
Senior Privacy Legal Counsel & Data Protection Officer
TomTom

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

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

Christopher Murphy
Chief Privacy Officer and Vice President, Legal Affairs
Electronic Arts Inc.

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, Esq.
President & Founder
Nissen Consulting

Nuala O'Connor
Senior Vice President & Chief Counsel, Digital Citizenship
Walmart

Erica Olsen
Director of Safety Net
National Network to End Domestic Violence

Xinru Page
Assistant Professor, Computer Information Systems
Bentley University

Lydia Parnes
Co-Chair, Privacy and Cybersecurity Practice
Wilson Sonsini

Eleonore Pauwels
Director of the AI Lab
Woodrow Wilson International Center for Scholars

Harriet Pearson
Senior Counsel
Hogan Lovells LLP

Future of Privacy Forum Advisory Board (continued)

Bilyana Petkova
Assistant Professor
HBKU College of Law

Kenneth Propp
Senior Fellow, Atlantic Council; Adjunct Professor of Law
Georgetown University

Bekah Putz
Senior Privacy Counsel
Chegg

Kalinda Raina
Vice President, Head of Global Privacy
LinkedIn Corporation

MeMe Rasmussen
Vice President Innovation, Legal
Splunk

Katie Ratte
Associate 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 (1961 -2020)
Stanley D. and Nikki Waxberg Chair and Professor of Law, Director of the 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 Project
Center for Democracy & Technology

Mila Romanoff
Data Policy and Governance Lead
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 of Computer Science
School of Computer Science Carnegie Mellon University

Agnes Bundy Scanlan
President
The Cambridge Group
Member, FPF Education & Innovation Foundation Board of Directors

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

Corinna Schulze
Director, EU Government Relations, Global Corporate Affairs
SAP

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

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

Kara Selke
Vice President, Commercial Development and Privacy
StreetLight Data, Inc.

Sooji Seo
Vice President Legal, Ethics and Compliance, and Chief Privacy Officer
Dell Technologies

Emily Sharpe
Director of Policy
World Wide Web Foundation

Linda Sherry
Director, National Priorities
Consumer Action

Kimberly Shur
Senior Vice President, Global Compliance Counsel & Privacy Officer
Marriott International

Jim Simatacolos
Managing Counsel, Commercial Law, Sourcing & Data Privacy
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

Daniel Solove
John Marshall Harland Research, Professor of Law
George Washington University Law School

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

Amie Stepanovich
Executive Director
Silicon Flatirons Center for Law, Technology, and Entrepreneurship

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

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

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, Privacy and Product
Snap Inc.

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
Assistant Vice President, Cybersecurity and Privacy
CTIA – The Wireless Association

Linda Trickey
Assistant General Counsel, Chief Privacy Counsel
Cox Communications

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

Hilary Wandall
Senior Vice President, Privacy Intelligence and General Counsel
TrustArc

Daniel J. Weitzner
Founding Director
MIT Internet Policy Research Initiative

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

Kevin Werbach
Professor of Legal Studies & Business Ethics
Wharton School

Alexander White
Privacy Commissioner
Bermuda

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

Shane Wiley
Chief Privacy Officer
Cuebiq

Marjorie Wilson
Global Head of Privacy, Data Protection Officer
Spotify

Kurt Wimmer
Partner and Co-Chair, Data Privacy and Cybersecurity Practice
Covington & Burling LLP

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
Kogod School of Business, American University

Dennis Yeoh
VP, Deputy General 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

Tal Zarsky
Visiting Scholar, University of Pennsylvania;
Professor of Law, University of Haifa

Ruby Zefo
Chief Privacy Officer
Uber Technologies, Inc.

Elana Zeide
Assistant Professor
University of Nebraska College of Law

Anna Zeiter
Chief Privacy Officer
eBay Inc.

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

American Express

Cigna

Consumer Technology Association

Honda

Optimizley

Quizlet

Sidewalk Labs, LLC

List as of January 2021. Please send updates about this list to Judy Gawczynski at jgawczynski@fpf.org.

Table of Contents

Awarded Papers

Honorable Mentions

Awarded Student Paper

Student Paper Honorable Mention

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

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.

Tinkering with Machine Learning: The Legality and Consequences of Online Surveillance of Students

Amy B. Cyphert

Nevada Law Journal: Vol. 20 : Iss. 2 , Article 4
Available at SSRN: https://ssrn.com/abstract=3602011

Executive Summary

All across the nation, high schools and middle schools are quietly entering into contracts with software companies to monitor the online activity of their students, attempting to predict the next school shooter or to intervene with a student who might be contemplating suicide. Systems using algorithms powered by machine learning trawl the Facebook posts of fifteen-year-olds and weed through the Twitter feeds of seventeen-year-olds. When certain keywords or features are flagged, the posts are forwarded to school administrators, who can decide whether the post requires an intervention and whether the student requires discipline. Who (or what) decides what these keywords are? What protections are given to the massive amounts of student data these third parties are collecting? Do parents and students even realize such online surveillance is happening?

Too often, the answers to these questions are unclear. This Article explores the legal and policy questions related to this new era of surveillance, which is fueled by machine learning. Although this technology is relatively new to schools, it has been used for decades in the criminal justice system, which has embraced sentencing algorithms and predictive policing. As is true with so many things in the criminal justice system, there is evidence that these technologies have had a disproportionate impact on people of color. In much the same way, evidence is emerging that the online monitoring of students is having a disproportionate impact on students of color. Despite having an aura of neutrality, at each stage in the machine learning process, there is a possibility for bias to creep in.

The legality of schools entering into contracts for third-party surveillance of their students is uncertain, as courts have not ruled on it specifically and have just begun to rule on the legality of schools regulating student internet speech at all. The fact that every state has a cyberbullying law that arguably requires schools to police their students' online speech complicates the legality question. This Article explores what legal challenges to third-party surveillance under the First and Fourth Amendments and the Equal Protection Clause might look like, and the likelihood of success of those arguments. Because the legal challenges are hypothetical at best, and perhaps years away, the Article concludes with some policy recommendations aimed at ensuring safety and fairness for all students.

Author

Amy Beth Cyphert is a Lecturer in Law at the West Virginia University College of Law and also the Director of the ASPIRE Office, which assists students who are applying for nationally competitive scholarships and fellowships. Cyphert is a 2001 graduate of Carnegie Mellon University, where she was awarded a Truman Scholarship. Cyphert graduated cum laude from Harvard Law School in 2005, and went on to clerk for the Honorable Laura Taylor Swain in the Southern District of New York. Prior to joining WVU, Cyphert was a senior litigation associate with WilmerHale in New York City, where she focused on complex commercial litigation as well as first amendment pro bono matters.

Cyphert's research focuses on varying areas, including artificial intelligence and law, creating change for children in vulnerable situations, and algorithmic decision making in schools and the criminal justice system.

Transferring Personal Data in Asia: A Path to Legal Certainty and Regional Convergence

Clarisse Girot

Asian Business Law Institute (ABLI): May 2020
Available at FPF: https://fpf.org/wp-content/uploads/2021/01/Transferring-Personal-Data-in-Asia-A-Path-To-Legal-Certainty-And-Regional-Convergence-1.pdf

Executive Summary

This Comparative Review sets out proposals for how Asian public stakeholders may promote legal certainty and greater consistency between their respective laws and regulations on cross-border transfers of personal data in the region. The Privacy Enforcement Authorities of the region have expressed their support to ABLI's work by providing comments or clarifications on their respective national frameworks, and industry representatives, law practitioners, academics and think tanks from across the region have provided input to ensure its practical relevance.

Despite differences between the philosophies and the regulatory structures of each regime, there exist enough connecting points between national frameworks which lawmakers, governments, and data protection regulators can capitalize on, so as to promote and ensure responsible data flows between jurisdictions. Interoperability would be further enhanced by a common movement to align the standards by which legal grounds, mechanisms, and schemes for data transfers should be assessed.

Alignment should be with a similarly high level of data protection so as to improve the situation of individuals and facilitate multi-jurisdictional compliance, as well as regulatory cooperation. Alignment not just to a regional standard but to global standards is a worthwhile goal, especially given the integration of Asian economies in global trade and the increased privacy expectations of the Asian public.

The Review aims to provide lawmakers, governments, and regulators in Asia who are currently drafting, reviewing, or implementing data transfer provisions in their respective jurisdictions with a comparative overview and analysis of the transfer principles, legal grounds, mechanisms, and schemes that operate in the laws of their regional partners and neighbours. This work is also relevant to US policymakers and public agencies in varied ways. It demonstrates that provisions relative to overseas data transfers exist in most Asian jurisdictions. In other words, they are not a European specificity and US policymakers must increasingly take this factor into account when dealing with their APAC partners. Further, until recently the extension and promotion of APEC CBPRs has been the key element of US data transfer policies in APAC.

Author

Clarisse Girot is a Senior Fellow at the Asian Business Law Institute (ABLI), a legal think tank chaired by Chief Justice Menon of the Supreme Court of Singapore, which conducts projects that promote the convergence of business laws in Asia. Since 2017, Clarisse has led a unique project on the convergence of data privacy laws in Asia, with an initial focus on international data transfers regulations, in coordination with a unique network of public and private stakeholders in Asia. Prior to relocating to Singapore in 2016, she acted as Counsellor to the President of the French Data Protection Authority (CNIL).

Reimagining Reality: Human Rights and Immersive Technology

Brittan Heller

Carr Center Discussion Paper Series: 2020-008
Available at Carr Center for Human Rights Policy: https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology

Executive Summary

Proponents of immersive technologies point to the transformational power of the medium. The experience of being in a VR environment for the first time is like stepping into a new world, where the program and head mounted display (HMD) create a digital blank slate for experience. Simply put, it feels real. Benefits like increased human connection, augmented empathy, and new opportunities for education are commonly listed as proof of VR's potential. Critics caution against unfettered optimism and focus on the opportunities for misuse and abuse, like harassment and violations of consumer privacy.

Because of the decreasing cost and rapid pace of development of immersive hardware, we are at a tipping point. Society is poised at the cusp of widespread adoption of immersive technologies by consumers, educators, advertisers, artists, journalists, and mainstream computer users. It is a rapidly growing player in the entertainment industry, encroaching on other large players like professional sports, video games, and film. But immersive technology is about to move from a tool for gamers, early adopters, and laboratory scientists to something that average people have in their living rooms. The Oculus Quest was a top gift for the 2019 Christmas season and sold out its entire stock going forward three months. It was equal in price to an Xbox or PlayStation gaming system, positioning it as a viable competitor to mainstream gaming. Over the next 3 years, VR and AR are each predicted to become a multi-billion dollar industry, with some estimates reaching $150 billion dollars in combined AR and VR revenue in 2020.

As we have seen from the emergence of other new media—from the telegraph to the telephone, from the television to the internet—the promise of innovation comes with a corresponding sense of peril. Because of the psychological aspects that make VR and AR immersive, and the potential for negative impacts on individual users and their communities, I argue that we should examine immersive media through a human rights-oriented lens. A human rights-based framework would integrate human dignity into the DNA of immersive systems, just like privacy- by-design frameworks foreground privacy-related concerns at the onset of product and policy development. Specifically, a human rights lens would mean that immersive creators and lawmakers should examine mismatches between existing privacy law and new forms of potential safety violations that implicate the fundamental rights of users—along with examining nascent risks inherent in both the interfaces and the immersive content itself.

Author

Brittan Heller works at the intersection of law, technology, and human rights. She is counsel at Foley Hoag's CSR practice, advising companies on privacy, freedom of expression, content moderation, online harassment, disinformation, civic engagement, cyberhate and hate speech, and online extremism.

Heller was the first Director for Technology and Society for ADL and established ADL's Center for Technology and Society, to examine issues like combating cyberharassment and cyberbullying; bringing civil rights into a digital environment; and leveraging innovations like AI, VR/AR/XR, and gaming to promote justice and fair treatment for all.

Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis

Tiffany C. Li

Loyola University Chicago Law Journal: Vol. 52, Iss. 3 (March 2021 Forthcoming)
Available at SSRN: https://ssrn.com/abstract=3690004

Executive Summary

The COVID-19 pandemic has caused millions of deaths and disastrous consequences around the world, with lasting repercussions for every field of law, including privacy and technology. The unique characteristics of this pandemic have precipitated an increase in use of new technologies, including remote communications platforms, healthcare robots, and medical AI. Public and private actors are using new technologies, like heat sensing, and technologically-influenced programs, like contact tracing, alike in response, leading to a rise in government and corporate surveillance in sectors like healthcare, employment, education, and commerce. Advocates have raised the alarm for privacy and civil liberties violations, but the emergency nature of the pandemic has drowned out many concerns.

This Article is the first comprehensive account of privacy in pandemic that maps the terrain of privacy impacts related to technology and public health responses to the COVID-19 crisis. Many have written on the general need for better health privacy protections, education privacy protections, consumer privacy protections, and protections against government and corporate surveillance. However, this Article examines these problems of privacy and technology specifically in light of the pandemic, arguing that the lens of the pandemic exposes the need for both wide-scale and small-scale reform of privacy law. This Article approaches these problems with a focus on technical realities and social salience, and with a critical awareness of digital and political inequities, crafting normative recommendations with these concepts in mind.

Understanding privacy in this time of pandemic is critical for law and policymaking in the near future and for the long-term goals of creating a future society that protects both civil liberties and public health. It is also important to create a contemporary scholarly understanding of privacy in pandemic at this moment in time, as a matter of historical record. By examining privacy in pandemic, in the midst of pandemic, this Article seeks to create a holistic scholarly foundation for future work on privacy, technology, public health, and legal responses to global crises.

Author

Tiffany C. Li is a visiting professor at Boston University School of Law and a Fellow at Yale Law School's Information Society Project. Li is an expert on privacy, artificial intelligence, and technology platform governance. She is regularly featured as a legal commentator in national and global news outlets, and her writing has appeared in popular publications including the Washington Post, the Atlantic, NBC News, and Slate. She also writes a recurring column on technology and privacy for MSNBC Daily.

After Schrems II: A Proposal to Meet the Individual Redress Challenge

Kenneth Propp and Peter Swire

LawFare: August 2020
Available at LawFare: https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge

Executive Summary

In its Schrems II decision, the Court of Justice of the European Union (CJEU) invalidated the EU/US Privacy Shield, and cast doubt on the validity of standard contractual clauses, the principal alternative for transferring personal data from EU territory to the United States and other countries. This article outlines a proposal for how to amend US law to meet the Court's stated legal requirement that an EU individual has a right to individual redress for violations of rights by US intelligence agencies.

In Schrems II, the CJEU stated that privacy protections in nations receiving data from the EU must be "essentially equivalent" to those afforded within the EU, including with respect "to any access by the public authorities to the personal data transferred [and] the relevant aspects of the legal system of that third country." The CJEU identified two ways in which U.S. surveillance law lacks essential equivalence to EU safeguards. The first, and the focus of this article, is that the US lacks an "effective and enforceable" right of individual redress.

The article explains the history of the Schrems litigation and of previous EU/US negotiations on trans-Atlantic flows of personal data. Specifically, it discusses the CJEU's finding that the Ombudsperson mechanism in the Privacy Shield for individual redress provided inadequate protections. Based on the CJEU's decision, any future attempt by the United States to successfully address this perceived deficiency in judicial redress thus must have two dimensions: a credible fact-finding inquiry into classified surveillance activities in order to ensure protection of the individual's rights, and the possibility of appeal to an independent judicial body that can remedy any violation of rights should it occur. For fact-finding, the authors propose that individual complaints be investigated by existing Privacy Civil Liberties Officers within the US intelligence community, or alternatively by the Privacy and Civil Liberties Oversight Board. Neither approach constitutes complete independence from the executive branch, and the possibility of such independence was narrowed by the US Supreme Court in its 2020 Seila Law opinion.

The independent review required by EU law would occur upon appeal to the US Foreign Intelligence Surveillance Court, composed of fully independent federal judges. Our proposal meets the US constitutional requirement of standing by imposing a legal duty on the agencies to examine complaints similar to the duty imposed under the Freedom of Information Act. If the agency does not meet the required standard of investigation and protection of rights, the judge can order the agency to correct any violation of individual rights. Creation of this judicial review function would require new federal legislation.

The article also discusses the legal standard for judicial review and suggests extending the new statutory protections to both US and EU persons. By meeting the individual redress requirements of EU law and the standing requirements of US law, the proposal complies with both EU and US law, and would be workable in practice.

Authors

Kenneth Propp teaches European Union Law at Georgetown University Law Center, and is a Senior Fellow with the Future Europe Initiative at the Atlantic Council in Washington, D.C. He was for many years a senior lawyer in the Office of the Legal Adviser, U.S. Department of State, and served as Legal Counselor at the US Mission to the European Union in Brussels from 2011-15. His writings on cross-border data issues have been published by the American Society of International Law, the Council on Foreign Relations, the Cross Border Data Forum, and the Progressive Policy Institute, among others.

Peter Swire is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business, a Senior Counsel to Alston & Bird LLP, and Senior Fellow of the Future of Privacy Forum. He served as one of five members of President Obama's Review Group on Intelligence and Communications Technology.

Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions

Lauren Henry Scholz

Journal of Corporation Law: Vol. 46 : Iss. 1, 2020
Available at SSRN: https://ssrn.com/abstract=3620164

Executive Summary

Consumer-firm interactions in the information age have come to resemble fiduciary relationships, yet American law has failed to recognize this new reality, leaving the consumer vulnerable to loss of privacy and elevated cybersecurity risks.

In fiduciary relationships, one party (the fiduciary), has discretionary power over important practical interests of another party (the entrustor). There are many types of fiduciaries recognized at law, as disparate as clergy, medical professionals, and corporate officers. What unites all fiduciaries is the potential for the fiduciary to misuse the power granted to her by the entrustor, for her own benefit and the entrustor's detriment. To prevent abuse of power, fiduciary law imposes duties upon the fiduciary, the core purpose of which is to hold the fiduciary to loyalty toward the entrustor and her interests. Enforcing fiduciary loyalty at law has both moral and utilitarian justifications.

The result of applying general contract principles to the consumer boilerplate has been a mass transfer of unrestricted rights to use and sell personal information from consumers to companies. This has enriched companies and enhanced their ability to manipulate consumers. It has also contributed to the modern data insecurity crisis. Information age consumer transactions should create fiduciary relationships between firm and consumer as a matter of law. Recognizing this fiduciary relationship at law honors the existence of consumer agreements while also putting adaptable, context-sensitive limits on opportunistic behavior by firms. In a world of ubiquitous, interconnected, and mutable contracts, consumers must trust the companies, with which they transact, not to expose them to economic exploitation and undue security risks: the very essence of a fiduciary relationship. Firms owe fiduciary duties of loyalty and care to their customers that cannot be displaced by assent to boilerplate.

This paper argues that consumer transactions in the information age should create fiduciary relationships between consumer and company. This means companies would have fiduciary duties to consumers that consumers cannot waive, regardless of the text of the boilerplate. In a fiduciary law framework, the role and significance of consumer boilerplate would be as follows. The offer of a consumer boilerplate contract by a company signals its intent to enter into an ongoing fiduciary relationship with consumers in the course of provision of services. A consumer's assent to the boilerplate signals the intention of a consumer to participate in a fiduciary relationship with the company. The effect of fiduciary duties in this context is to create technology-neutral protections for consumers against exploitation. Fiduciary duties would mean expanded liability for data protection failures for companies.

Author

Lauren Henry Scholz is the McConnaughhay and Rissman Professor at Florida State University College of Law. Before coming to FSU, she was a fellow at the Project on the Foundations of Private Law and the Berkman Klein Center for Internet & Society, both at Harvard Law School. She also was a fellow at Yale Law School's Information Society Project.

Her work has appeared in Indiana Law Journal, Iowa Law Review, and the University of Chicago Law Review Online. Her research interests include contracts, torts, commercial law, and information privacy.

Honorable Mentions

Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence

Frederik J. Zuiderveen Borgesius

The International Journal of Human Rights (2020): 1-22
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561441

Executive Summary

The use of algorithmic decision-making has become common practice across a wide range of sectors. We use algorithmic systems for spam filtering, traffic planning, logistics management, diagnosing diseases, speech recognition, and much more. Although algorithmic decision-making can seem rational, neutral, and unbiased, it can also lead to unfair and illegal discrimination. The two main questions for this paper are: (1) What legal protections against algorithmic discrimination exist in Europe, and what are their limitations?; and (ii) How could those legal protections be improved?

The paper focuses on the two most relevant legal instruments for defending people against algorithmic discrimination: non-discrimination law and data protection law. The paper speaks of 'discrimination' when referring to objectionable or illegal discrimination, for example, on the basis of gender, sexual preference, or ethnic origin. The word 'differentiation' refers to discrimination, or making distinctions, in a neutral, unobjectionable sense.

The paper's main contributions to scholarship are made in three ways. First, there has not been much legal analysis of European non-discrimination law in the context of algorithmic decision-making. The few papers that discuss European non-discrimination law do so with a focus on EU law. Second, assessing how data protection law can help to protect people against discrimination. And third, the paper proposes an approach to regulate algorithmic decision-making in a sector-specific way. The paper could be useful for scholars, practitioners, and for policymakers that want to regulate algorithmic decision-making.

The paper focuses on the overarching rules in Europe (the region of the Council of Europe, with 47 member states); national rules are out of scope. Because of the focus on discrimination, questions relating to, for instance, privacy and freedom of expression are outside the scope of the paper. The paper is based on, and includes text from, a report by the author for the Anti-Discrimination Department of the Council of Europe.

Honorable Mentions (continued)

Business Data Ethics: Governance Transformations for the Era of Advanced Analytics and AI

Dennis Hirsch, Timothy Bartley, Aravind Chandrasekaran, Srinivasan Parthasarathy, Piers Norris Turner, and Davon Norris

Ohio State Public Law Working Paper: No. 522
Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478826

Executive Summary

This Final Report conveys the findings of an interdisciplinary Ohio State research project on corporate data ethics management. Data ethics management, as we define it here, refers to a company's governance of the threats that its own use of advanced analytics and artificial intelligence (AI) pose to individuals, the broader society and the company itself. Companies refer to this as "data ethics" largely because the law lags behind the rapid emergence of advanced analytics and AI and so, to address the risks that their use of these technologies poses, companies need to go beyond legal requirements. As they see it, this takes them into the realm of "ethics."

The authors of this report are scholars who have studied, among other things, corporate self- regulation beyond compliance behavior. We were intrigued by early corporate statements about their data ethics or AI ethics practices. We sought to learn what companies meant by "data ethics," why they were pursuing it, and how they went about this. To explore this, we spent two years interviewing companies who were recognized by their peers as leaders in this emerging area of corporate management, as well as the lawyers and consultants who work with them on this topic. We then conducted a survey that reached a broader array of companies involved in this area. This Final Report conveys our research findings.

This Report occupies a distinct place in the literature on data ethics and AI ethics. Much of the growing literature on this topic focuses on normative ideas as to what data ethics should be, or on proposals for the legislation or regulation required to achieve this normative state. By contrast, this Report is empirical and descriptive. It seeks to document the state of corporate data ethics management as it existed during the period when we conducted the interviews (2018–2019) and survey (2019–2020). Our research into what data ethics looks like "on the ground" (Mulligan and Bamberger 2015) should provide useful information to legislators and policymakers as they begin to develop laws and policies to govern business use of advanced analytics and AI. It should also provide ideas to companies and governmental organizations interested in pursuing data ethics with respect to their own use of advanced analytics and AI.

Awarded Student Paper

Personal Identifiability of User Tracking Data During Observation of 360-degree VR Video

Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A. Landay, and Jeremy N. Bailenson

Scientific Reports: (2020) 10:17404
Available at Nature Research: https://www.nature.com/articles/s41598-020-74486-y#disqus_thread

Executive Summary

The ways users sit, stand, and move in virtual reality is not normally treated as identifying information, yet can be used to re-identify previously anonymized data.

Virtual reality uses computer technology to simulate virtual environments. In order to be realistic, a VR application must track the user in space. Just as a person's view of the people in a room depends upon his or her location within it, the user's view of a virtual scene depends upon and reacts to their placement within it. The collection and storage of this data is usually viewed to be harmless. In short, we argue this collection can be a privacy risk.

In contrast to previous research, which has focused on picking the right VR tasks to identify or authenticate users, the study we performed used a task that was not designed for identification. In fact, the tracking data we use is from a separate study examining the associations between motion, self-report emotion data, and video content.

Using only the position tracking data, we find that even with more than 500 participants to choose from, a simple machine learning model can identify participants from less than five minutes of tracking data at above 95% accuracy. Therefore, we contribute data suggesting typical VR experiences produce identifying data. In our paper, we shed some light on the possible mechanism behind identification by examining different types of models and different feature sets, and suggest some technical strategies to prevent abuse.

If tracking data is by nature identifying, there are important implications for privacy as VR becomes more popular. The most pressing class of issues falls under the process of de-identifying data. It is standard practice in releasing research datasets or sharing VR data to remove any information that can identify participants or users. In both the privacy policy of Oculus and HTC, makers of two of the most popular VR headsets in 2020, the companies are permitted to share any de-identified data. If the tracking data is shared according to rules for de-identified data, then regardless of what is promised in principle, in practice taking a name off a dataset accomplishes very little.

The second class of threats is broadly concerned with an improved ability to link VR sessions together. Information that was previously scattered and separate is now able to be joined by a "motion signature." In connecting some tracking data to a name, for example, now tracking data in many other places are attached to the same name. This increases the effectiveness of privacy threats based upon inference of protected health information from tracking data.

A third class of threats stems from ""private browsing"". In principle, there is a way to enter a ""private browsing mode"" in a web browser. While it may be difficult and require many tools hiding many layers of information, it is possible. With accurate VR tracking data, a ""private browsing mode"" is in principle impossible.

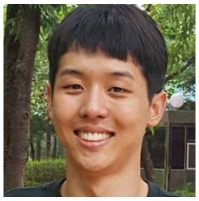
We ask policymakers, researchers, and the general public to consider that tracking data can be identifying in many cases.

Awarded Student Paper Authors

Mark Roman Miller is a fifth-year Ph.D. student in the Human-Computer Interaction program at Stanford University, advised by Jeremy Bailenson and James Landay. His research interests include social interaction, especially nonverbal behavior, in augmented and virtual reality. His previous work tests whether people respond to virtual humans in AR the same way they do towards real people. Currently, he is investigating how design teams work together in virtual environments. He received his B.S. in Computer Science from the University of Illinois at Urbana-Champaign.

Fernanda Herrera received her B.S. in Psychology from the University of Texas at Austin and her M.A. and Ph.D. in Communication from Stanford University. Her research focuses on examining the psychological and social effects of Augmented Reality and Virtual Reality experiences. More specifically, her research examines the effect of VR experiences on empathy and prosocial behaviors, assesses the effect of avatar representation and system affordances on social interactions inside collaborative virtual environments, and studies how face-to-face social interactions are impacted by the use of AR technology.

James Landay is a Professor of Computer Science and the Anand Rajaraman and Venky Harinarayan Professor in the School of Engineering at Stanford University. He specializes in human-computer interaction. He is the founder and co-director of the World Lab, a joint research and educational effort with Tsinghua University in Beijing. He is also the co-founder and Associate Director of the Stanford Institute for Human-centered Artificial Intelligence (HAI). He was named to the ACM SIGCHI Academy in 2011 and as an ACM Fellow in 2017. He formerly served on the NSF CISE Advisory Committee.



Hanseul Jun studies augmented reality and virtual reality in the Virtual Human Interaction Lab at Stanford University, advised by Professor Jeremy Bailenson. As a fourth year communication Ph.D. student, his research interest is currently focused on social interaction in virtual environments, especially through telepresence systems. Before starting his Ph.D., he received a bachelor's degree in Electrical Engineering at Seoul National University and worked as a computer graphics engineer.

Jeremy Bailenson is founding director of Stanford University's Virtual Human Interaction Lab, Thomas More Storke Professor in the Department of Communication, Professor (by courtesy) of Education, Professor (by courtesy) Program in Symbolic Systems, a Senior Fellow at the Woods Institute for the Environment, and a Faculty Leader at Stanford's Center for Longevity. He studies the psychology of Virtual and Augmented Reality, in particular how virtual experiences lead to changes in perceptions of self and others. In 2020, IEEE recognized his work with "The Virtual/ Augmented Reality Technical Achievement Award."

Student Paper Honorable Mention

“It’s a scavenger hunt”: Usability of Websites’ Opt-Out and Data Deletion Choices

Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti,
Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub

CHI ’20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems:
April 2020, Pages 1–12
Available at SSRN: https://usableprivacy.org/static/files/habib_chi_2020.pdf

Executive Summary

An expanding body of privacy regulations requires websites and online services to present users with notices and choices regarding the usage of their data. These regulations aim to provide transparency about data processing policies and give users access and control over their own data. Some regulations—such as the General Data Protection Regulation (GDPR) and a few US laws—include specific usability requirements. In part due to these regulations, privacy choices now seem to be ubiquitous on websites. Particularly common are opt-outs for email communications or targeted ads, options for data deletion, and controls and consent for use of cookies.

However, availability does not imply usability, leaving open the question of whether these controls are actually useful to consumers. We contribute a holistic usability evaluation of the end-to-end interaction required to use common implementations of these privacy choices. Past work has found various usability problems with such controls, particularly in tools for limiting targeted advertising. We expand on that work by exploring the usability of websites’ own opt-outs for targeted ads. Furthermore, we examine choices beyond those related to advertising, providing insight into the usability of email marketing and data deletion choices required by the CAN-SPAM Act and GDPR, respectively. We conducted an in-lab usability study with 24 participants. Participants were first asked about their expectations regarding websites’ data practices and privacy controls. They completed two tasks that were representative of common practices for offering privacy choices, as identified by prior work. Tasks differed by the choice type (opting out of email communication, opting out of targeted ads, or requesting data deletion), choice location (account settings, privacy policy), and mechanism type (described in policy text, link from policy text).

We find that despite general awareness of deletion mechanisms and opt-outs for advertising and email, participants were skeptical of the effectiveness of controls provided by websites. On the nine websites studied, participants struggled most with discovering and recognizing pages with opt-out information and resorted to consulting help pages or contacting the website. Participants also expressed desire for additional controls over data sharing and deletion. Our findings suggest several implications applicable to websites similar to those in this study for making these online opt-out and deletion choices more usable and useful to consumers.

Thank you to our 2020 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 https://fpf.org/privacy-papers-for-policy-makers/.

Advisory Board Reviewers

Kurt Wimmer
Covington & Burling LLP

Sara DePaul
Software & Information Industry Association

Doug Luftman
DocuSign

Rita Heimes
IAPP - International Association of Privacy Professionals

Amy Yeung
Lotame Solutions, Inc.

John Grant
Palantir Technologies

Kristen Erbes
Cambia Health Solutions

Harvey Jang
Cisco Systems, Inc.

Farah Zaman
Meredith

Douglas Miller
Information Technology Industry Council

Michelle Richardson
Center for Democracy & Technology

Finalist Judges

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

Michael McCullough
Chief Privacy Officer & Governance, Risk Management, and Compliance Leader, Macy's, Inc.
Advisory Board Member, Future of Privacy Forum

Amie Stepanovich
Executive Director, Silicon Flatirons Center for Law, Technology, and Entrepreneurship
Board Member, Internet Education Foundation
Advisory Board Member, Future of Privacy Forum

Jules Polonetsky
Chief Executive Officer, Future of Privacy Forum

John Verdi
Vice President, Future of Privacy Forum

PRIVACY PAPERS FOR POLICYMAKERS 2020

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