**Advancing Principled Data Practices
in Support of Emerging Technologies**

2016 ANNUAL REPORT

**FUTURE OF
PRIVACY
FORUM**

LETTER FROM FPF LEADERSHIP

We are delighted to present Future of Privacy Forum's 2016 Annual Report. Since our founding in 2008, FPF has served 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.

We pride ourselves on being positioned to help 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.

With your intellectual engagement and financial support this past year, FPF played a leadership role on a wide range of privacy issues. Our team produced impactful reports, filings and best practices, convened stakeholder meetings and events, and helped shape policies and practices for industry, government, academia and civil society. We hope you find great value in the following pages that cover highlights of our work in areas such as de-identification, connected cars, education, wearables, location and advertising practices, smart cities, and much more. We could not do this work without the committed stakeholders on our board, advisory board and corporate and foundation supporters. We look forward to our continued partnership and are excited about what lies ahead.

Jules Polonetsky
CEO

Chris Wolf
BOARD PRESIDENT
AND FPF FOUNDER

About Future of Privacy Forum

Mission:

Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

Who We Are:

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.

Vision:

We believe that...

- technological innovation and new uses of data can help solve big societal problems and improve lives.

- technological innovation must be accompanied by fresh privacy thinking.

- it is possible to build a world where technological innovation and privacy can coexist.

- it is possible to reach consensus on ethical norms, policies and business practices to address new privacy challenges.

The FPF Team

Leadership

Jules Polonetsky
CEO

Board of Directors

Christopher Wolf
Board President
and FPF Founder

Mary Culnan
Board Vice President

Sandra Hughes
Board Secretary

Debra Berlyn
Board Treasurer

Alan Raul
Board Member

Staff

John Verdi
Vice President of Policy

Brenda Leong
Senior Counsel and
Director of Strategy

Barbara Kelly
Leadership Director

Melanie Bates
Director of Communications

Kelsey Finch
Policy Counsel

Stacey Gray
Policy Counsel

Lauren Smith
Policy Counsel

Amelia Vance
Policy Counsel

Noelle Johnson
Executive Assistant

Mary Wright
Membership Development Specialist

Terry Grant
Financial Management Specialist

Gabriela Zanfir-Fortuna
Fellow

Carolina Alonso
Junior Fellow

Margaret Honda
Research Coordination Network

The FPF Team (continued)

Senior Fellows

Danielle Citron
Lois K. Macht Research Professor
& Professor of Law at the
University of Maryland

Ira Rubinstein
Senior Fellow
Information Law Institute
NYU School of Law

Henry Claypool
Policy Director at the Community
Living Policy Center

Evan Selinger
Professor of Philosophy at
Rochester Institute of Technology

Mary Culnan
Board Vice President

Peter Swire
Nancy J. and Lawrence P. Huang
Professor at the Scheller College of
Business of the Georgia Institute of
Technology

Leslie Harris
Founder and Principal
Harris Strategy Group, LLC

Omer Tene
Associate Professor
College of Management
School of Law

Advisory Board

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

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

Sharon A. Anolik
President
Privacy Panacea

Annie I. Antón
Professor of Computer Science and Chair
of the School of Interactive Computing
College of Computing,
Georgia Institute of Technology

Justin Antonipillai
Former Counselor to the Secretary of
Commerce, Delegated Duties of Under
Secretary for Economic Affairs

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

Stephen Balkam
Chief Executive Officer
Family Online Safety Institute

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

Kabir Barday
Chief Executive Officer
OneTrust

Malita Barkataki
Privacy Compliance Director
Yahoo

Inna Barmash
General Counsel
Amplify Education, Inc.

Nancy Bell
Senior Manager, External Affairs
FCA US LLC

Lael Bellamy
Chief Privacy Officer
The Weather Channel

Alisa Bergman
Chief Privacy Officer
Adobe Systems, Inc.

Elise Berkower
Associate General Counsel, Privacy
The Nielsen Company

Debra Berlyn
President
Consumer Policy Solutions

Joan (Jodie) Z. Bernstein
Counsel
Kelley Drye & Warren, LLP
Former Director of the Bureau of
Consumer Protection at the Federal Trade
Commission

Andrew Bloom
Chief Privacy Officer
McGraw-Hill Education

Bruce Boyden
Assistant Professor of Law
Marquette University Law School

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

Julie Brill
Partner
Hogan Lovells LLP

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

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

Stephanie Bryson
Senior Public Policy Associate
Uber

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

James M. Byrne
Chief Privacy Officer
Lockheed Martin Corporation

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

Sam Castic
Senior Counsel, Director of Privacy,
Risk Management
Nordstrom

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

Mary Chapin
Chief Legal Officer
National Student Clearinghouse

Lorrie Cranor
Professor, Computer Science,
Engineering, and Public Policy
Carnegie Mellon University
Former Chief Technologist,
Federal Trade Commission (FTC)

Danielle Keats Citron
Professor of Law
University of Maryland School of Law

Allison Cohen
Managing Counsel
Toyota Motor North America, Inc.

Maureen Cooney
Head of Privacy
Sprint Corporation

Mary Culnan
Professor Emeritus
Bentley University

Simon Davies
Founder
Privacy International

Laurie Dechery
Associate General Counsel
Lifetouch, Inc.

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

Michelle Finneran Dennedy
Chief Privacy Officer
Cisco Systems, Inc.

Carol DiBattiste
General Counsel & Chief Privacy and
People Officer
Comscore

Travis Dodd
Chief Privacy Officer and Associate
General Counsel
AARP

Advisory Board (continued)

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

Erin Egan
Chief Privacy Officer, Policy
Facebook, Inc.

Keith Enright
Senior Corporate Counsel
Google, Inc.

Patrice Ettinger
Chief Privacy Officer
Pfizer, Inc.

Joshua Fairfield
Professor of Law
Washington and Lee University School
of Law

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

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

Dona Fraser
Vice President
Privacy Certified Program
Entertainment Software Rating Board

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

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

Deborah Gertsen
Lead Privacy Counsel
Ford Motor Company

Jennifer Barrett Glasgow
Chief Privacy Officer
Acxiom Corporation

John Godfrey
Senior Vice President, Public Policy
Samsung Electronics

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

Scott Goss
Senior Privacy Counsel
Qualcomm, Inc.

Justine Gottshall
Chief Privacy Officer
Signal

Kimberly Gray
Chief Privacy Officer
QuintilesIMS

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

Woodrow Hartzog
Assistant Professor
Cumberland School of Law
Samford University

Eric Heath
Chief Privacy Officer
Ancestry

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

Megan Hertzler
Director of Enterprise Information
Goverance
PG&E

Beth Hill
General Counsel &
Chief Compliance Officer
Ford Direct

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

David Hoffman
Associate General Counsel and
Global Privacy Officer
Intel Corporation

Lara Kehoe Hoffman
Global Director, Data Privacy and Security
Netflix

Bo Holland
Founder & Chief Executive Officer
AllClearID

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

Jestlan Hopkins
Privacy Manager
Inflection

Jane Horvath
Director of Global Privacy
Apple, Inc.

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

Sandra R. Hughes
Chief Executive Officer and President
Sandra Hughes Strategies

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

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

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

Michael Kaiser
Chief Executive Director
National Cyber Security Alliance

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

Cameron F. Kerry
Senior Counsel
Sidley Austin LLP

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

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

Michael C. Lamb, Esq.
Chief Privacy Officer
RELX Group

Barbara Lawler
Chief Privacy Officer
Intuit, Inc.

Ginny Lee
Director of Global Customer Privacy
Starbucks Coffee Company

Yoomi Lee
Vice President, Global Privacy
American Express

Peter M. Lefkowitz
Chief Privacy Officer
GE Digital

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

Gerard Lewis
Senior Vice President &
Deputy General Counsel
Comcast Corporation

Harry Lightsey
Executive Director, Federal Affairs
General Motors Company

Brendon Lynch
Chief Privacy Officer
Microsoft Corporation

Mark MacCarthy
Vice President of Public Policy
The Software & Information Industry
Association

Larry Magid
President & CEO
Connect Safely

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

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

William McGeveran
Professor of Law
University of Minnesota Law School

Terry McQuay
President
Nymity, Inc.

David Medine
Consultant, Consultative Group to
Assist the Poor
Former Chairman, Privacy and Civil
Liberties Oversight Board

Scott Meyer
Chief Executive Officer
Ghostery, Inc.

Doug Miller
Global Privacy Leader
AOL, Inc.

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

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

Alma Murray
Senior Counsel, Privacy
Hyundai Motor America

Jill Nissen, Esq.
Founder & Principal
Nissen Consulting

Harriet Pearson
Partner
Hogan Lovells LLP

Christina Peters
Senior Counsel, Security and Privacy
IBM Corporation

Bilyana Petkova
Postdoctoral Research Fellow
Information Law Institute, New York
University

Peter Petros
General Counsel & Global Privacy
Officer
Edelman

John Plunkett
Vice President, Policy & Advocacy
Hobsons

Kalinda Raina
Head of Global Privacy, Senior Director
LinkedIn Corp

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

Alan Raul
Partner
Sidley Austin LLP

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

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

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

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

Shirley Rooker
President
Call for Action

Michelle Rosenthal
Corporate Counsel
T-Mobile, Inc.

Alexandra Ross
Senior Global Privacy and Data Security
Counsel
Autodesk

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

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

Linda Sherry
Director, National Priorities
Consumer Action

Meredith Sidewater
Senior Vice President and General
Counsel
LexisNexis Risk Solutions

Dale Skivington
Chief Privacy Officer
Dell, Inc.

Advisory Board (continued)

Supporters

Will Smith
Chief Executive Officer
Euclid, Inc.

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

Daniel Solove
Professor of Law
George Washington University Law
School

Barbara Sondag
Senior Vice President, Head of Privacy
Westfield

Cindy Southworth
Executive Vice President
National Network to End Domestic
Violence

JoAnn Stonier
EVP, Chief Information Governance &
Privacy Officer
MasterCard Incorporated

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

Zoe Strickland
Managing Director, Global Chief Privacy
Officer
JPMorgan Chase Bank NA

Greg Stuart
Chief Executive Officer
Mobile Marketing Association

Peter Swire
Nancy J. & Lawrence P. Huang Professor
Scheller College of Business,
Georgia Institute of Technology

Scott M. Taylor
Associate Vice President &
Chief Privacy Officer
Merck Privacy Office, Pulse x-U.S.
Program, Animal Health & Global
Functions Compliance

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

Adam Thierer
Senior Research Fellow, Mercatus Center
George Mason University

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

Friederike van der Jagt
Senior Legal Counsel Privacy
Avast

David C. Vladeck
Professor, Georgetown University Law
Center
Former Director of the Bureau of
Consumer Protection at the Federal
Trade Commission (FTC)

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

Daniel J. Weitzner
Co-Director, MIT CSAIL Decentralized
Information Group
W3C Technology and Society Policy
Director
Former Deputy Chief Technology Officer
at The White House Office of Science
and Technology Policy

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

Estelle Werth
Vice President, Global Privacy Officer
Criteo

Heather West
Senior Policy Manager
Mozilla

Nicole Wong
Principal
NWong Strategies

Christopher Wood
Executive Director & Co-Founder
LGBT Technology Partnership

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

Jack Yang
Associate General Counsel
Global Privacy Office and
Enterprise Risk, Legal
Visa, Inc.

Karen Zacharia
Chief Privacy Officer
Verizon Communications, Inc.

Elana Zeide
CITP, Princeton University
Associate Research Scholar, Center for
Information Technology Policy

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

2U, Inc.
AARP
Acxiom
Adobe
ADT
Aislelabs
AllClearID
Alliance of Automobile
Manufacturers
Amazon.com
American Express
Amplify Education, Inc.
Ancestry
Anonos, Inc.
AOL
Apple
Ask.com
Atomite, Inc.
AT&T
Autodesk, Inc.
Avast
Bank of America
Catalina Marketing
Cengage
Cisco Systems, Inc.
Citigroup
ClassDojo
Cloud4Wi
Comcast
comScore
Consumer Technology
Association (CTA)
COeverywhere
Criteo
CTIA
Dell
DJI
EA
Edelman
Edmodo
Epsilon
Ernst & Young
ESOMAR
Euclid
Evernote
Facebook
Fiat Chrysler Automobiles
Ford Motor Company
Foursquare
General Electric Company

General Motors
Ghostery, Inc.
Gimbal, Inc.
Global Automakers
GoGuardian
Google
Graduate Management Admission
Council
HID Global
Hobsons
Houghton Mifflin Harcourt
Hyundai
IBIA (International Biometrics &
Identification Association)
IMS Health
Inflection
Intel
Information Technology Industry
Council (ITI)
International Association of
Privacy Professionals
Intuit
JPMorgan
Khan Academy
Knewton, Inc.
Lifetouch, Inc.
LinkedIn
Lockheed Martin
Loeb & Loeb LLP
Lotame
Lyft
Macy's, Inc.
Marketo, Inc.
MasterCard Worldwide
MaxPoint
McGraw-Hill Education
Measurence
Merck and Co., Inc
Microsoft
Mobile Marketing Association
Mozilla
Network Advertising Initiative
National Student Clearinghouse
Netflix
Neustar
Nike, Inc.
Noble Hour
Nordstrom, Inc.
Nymity
OneTrust

Pearson
Pfizer, Inc.
Privo
Privoro
Procter & Gamble
Prudential
Purple WiFi
Qualcomm
Quantcast
Radius
Radiolocus
RELX
Retail Industry Leaders Association
RetailNext
SAP
Shoppertrak
Sidley Austin LLP
Signal
Slack
Software & Information Industry
Association
Solomo Technology
Sprint
Starbucks
StreetLight Data
T-MOBILE USA, Inc.
The Nielsen Company
The Walt Disney Company
The Weather Channel
TomTom
Toyota
TRUSTe
Tune, Inc.
Turnstyle Solutions, Inc.
Uber Technologies, Inc.
UnitedHealth Group
Verizon
Visa
WalMart Stores Inc
Westfield
Wilson Sonsini Goodrich & Rosati,
Professional Corporation
Yahoo!
Yodlee
Zebra
Zeotap
ZwillGen PLLC
Zynga

Cars

FPF's Connected Car Project advances privacy practices and understanding as new mobility technologies come to market. We help ensure responsible practices are in place so that the benefits of technologies will be well-received by consumers. FPF's goal is to promote leading privacy practices and industry solutions for these emerging technologies.

Our Connected Car Project working group is an ongoing collaborative effort to pursue best practices by car manufacturers and technology suppliers.

Highlights of our work in 2016
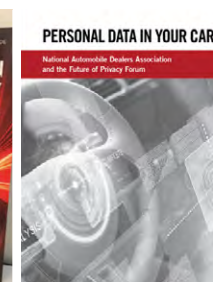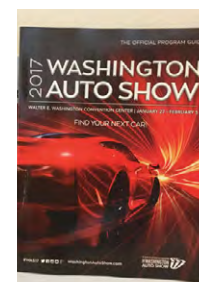
Personal Data In Your Car

FPF developed, in partnership with the National Automobile Dealers Association, a consumer guide to educate drivers about data collection and use. The guide provides consumers with an understanding of how to protect information that is stored, synced, or shared with a vehicle and provides privacy tips such as how to clear data from a vehicle before reselling it.

FPF Hosts Roundtable with DOT, NHTSA and the FTC

FPF hosted an in-person meeting in our DC office with representatives from the Department of Transportation, National Highway Transportation Safety Administration, and Federal Trade Commission, the three main federal agencies engaged in privacy related to connected cars. The robust two-hour discussion covered the role of each agency, and provided opportunities for Q&A and discussion between attendees and regulators.

In the Press

Self-Driving Cars: Transforming Mobility For The Elderly And People With Disabilities (Jules Polonetsky and Henry Claypool, Huffington Post, October 21, 2016)

"The benefits for facilitating the deployment of autonomous vehicles are so compelling and policymakers should be doing all they can to smooth and speed the way for these technologies to improve as quickly as possible."

Connected cars: What information about you & your driving is being tracked and collected? (Lauren Smith, WXYZ-TV, July 21, 2016)

"Some of the information may be going to the manufacturer, some may be staying locally on the car, some may be going to your insurance company if you've selected that, some may be going to some technology you've opted into. So we're trying to clarify for consumers what kind of information your car may collect and where the information is being sent."

Safeguarding the data that power safer cars (Jules Polonetsky and Lauren Smith, The Hill, March 15, 2016)

"It is critical, at the front-end of the connected car revolution, to build responsible data practices into connected cars, just as we have in other new and unfamiliar technologies."
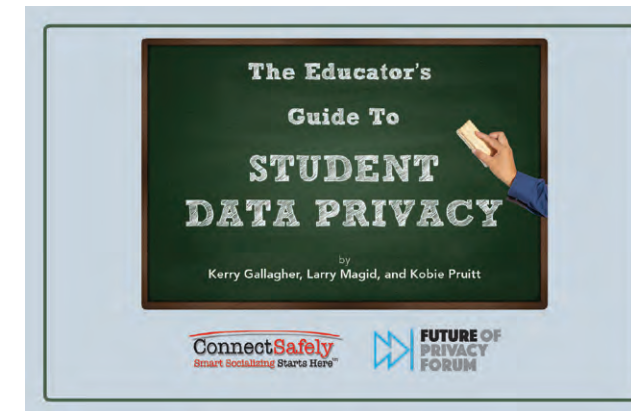
Education

Education is changing. New technologies are allowing information to flow within schools and beyond, enabling new learning environments and providing new tools to improve the way teachers teach and the way students learn. Data-driven innovations are bringing advances in teaching and learning but are accompanied by concerns about how education data, particularly student-generated data, are being collected and used.

FPF's student privacy program produces policy guidance and scholarship about finding the balance between protecting student privacy and allowing for the important use of data and technology in education. FPF examines both the K-12 and Higher Education landscape to find best practices and create practical tools to advance the responsible use of data.

Highlights of our work in 2016

Educator's Guide to Student Data Privacy

Technology tools and applications are changing the way schools and teachers educate students across the country. New resources are making it easier for teachers and students to communicate in and outside of the classroom making learning a 24/7 activity. When schools use technology, a student's personal information is often collected and shared for the purpose of furthering their education.

The Educator's Guide will help teachers utilize technology in the classroom responsibly and protect their students' privacy, explaining among other things: 1) Why student privacy matters, including legal requirements; 2) Teachers options for vetting an app for privacy considerations; and 3) Available resources, including a quick reference checklist for teachers to use as they continue to incorporate technology.

Beyond One Classroom: Parental Support for Technology and Data Use in Schools

FPF released its 2016 education privacy parent survey, Beyond One Classroom: Parental Support for Technology and Data Use in Schools. The survey asked parents to comprehensively outline their goals and concerns about the use of technology and student data. The key findings of Beyond One Classroom indicate that the closer the use of data is to individual classrooms and to the parent's child, the more strongly parents support, and desire, the benefits of student data collection and use.

Student Privacy Pledge reached over 300 Signatories

FPF and the Software and Information Industry Association (SIIA) were pleased to announce that the Student Privacy Pledge passed a new milestone – over 300 ed tech company signatories. The Pledge is a list of commitments that school service providers can make to affirm that K-12 student information is kept private and secure. It has been endorsed by President Obama, the National PTA, and the National School Boards Association.

Companies who take the Student Privacy Pledge commit to twelve legally enforceable obligations, including that they will not sell student personal information, and will not collect or use student personal information other than what is needed for the given educational purposes. The commitments in the Pledge concisely detail existing federal law and regulatory guidance regarding the collection and handling of student data, and encourage service providers to more clearly articulate these practices.

In the Press

Supporting Parental Choice for Student Data
The Hill (September 21, 2016) Jules Polonetsky and Brenda Leong

"Parents, as those most in-tune with their individual child's needs, have the right to be an active partner and make the final decision about additional sharing and use of their child's information."

The Colleges Are Watching
The Atlantic (November 1, 2016) Brenda Leong

Leong said she often hears boosters of big data referring to the growing amounts of student information as "fields of gold." "That's the kind of phrase that puts a lot of people off," she said. "It's not data, it's students; it's real people with real lives."

Data privacy report shows parents need education in school technology use
Ed Scoop (December 8, 2016) Amelia Vance

"Parents are the strongest advocates for their children's educational success, and all other stakeholders in the educational system should embrace the opportunity to communicate and work with parents as partners in addressing these issues," said Amelia Vance, FPF's new policy counsel.

This paper identifies 19 studies – a relatively small sample – where data was successfully used to evaluate a program, create a new strategy, or delve into equity and bias issues. The appropriate protection and responsible use of student data in such studies is a fundamental value. But the power of data to shed light on current student and educational system outcomes and improve the opportunity for individual success is overwhelming.

New data analysis techniques provide the opportunities to understand and transform learning theory and practice. As Ms. Zeide concludes: "Properly used, mindfully implemented, and with appropriate privacy protections, student data is a tremendous resource to help schools fulfill the great promise of providing quality education for all."

19 Times Data Analysis Empowered Students and Schools

FPF's paper, by Elana Zeide, demonstrates the power of data to show school, districts, parents, and students, the trends and outcomes that are occurring, and inspire ways to make those outcomes better.

Smart Cities

Smart cities are faster, more efficient, environmentally friendly, and better prepared in emergencies. Civil servants have used data for years to track and understand traffic patterns, but opportunities presented by information technologies extend well beyond managing the roads. FPF sees the value in technologies that inform and streamline municipal services without treading on consumer expectations of anonymity and privacy. FPF commits itself to engaging service providers, developers, policy makers and consumers in a dialogue over the application of data tools for the public good.

Highlights of our work in 2016

FPF developed important privacy resources for municipalities, including a chapter on Privacy and Security in the Smart City Readiness Guide and an infographic Shedding Light on Smart City Privacy.

Privacy in the Smart City: Finding the Middle Ground

As part of Smart Cities Week, FPF hosted a roundtable titled "Privacy in the Smart City: Finding the Middle Ground." The roundtable explored some of the major advancements in technology, certain economic and political changes, as well as the societal shifts that have generated interest in developing smart cities. The event focused on finding the balance between securing social benefits and protecting individual privacy. Thought leaders from the City of Seattle, the District of Columbia, and the U.S. Department of Transportation were in attendance, as well as experts from industry and academia. The result was an engaging discussion of responsible data practices in a hyper-connected world.

FPF has been contracted by the City of Seattle to create a methodology for performing a privacy risk assessment for an Open Data Program, and to conduct an assessment of Seattle's Open Data Program. The project includes input from experts at the University of Washington and the Berkman Klein Center for Internet & Society at Harvard University.

SHEDDING LIGHT ON SMART CITY PRIVACY
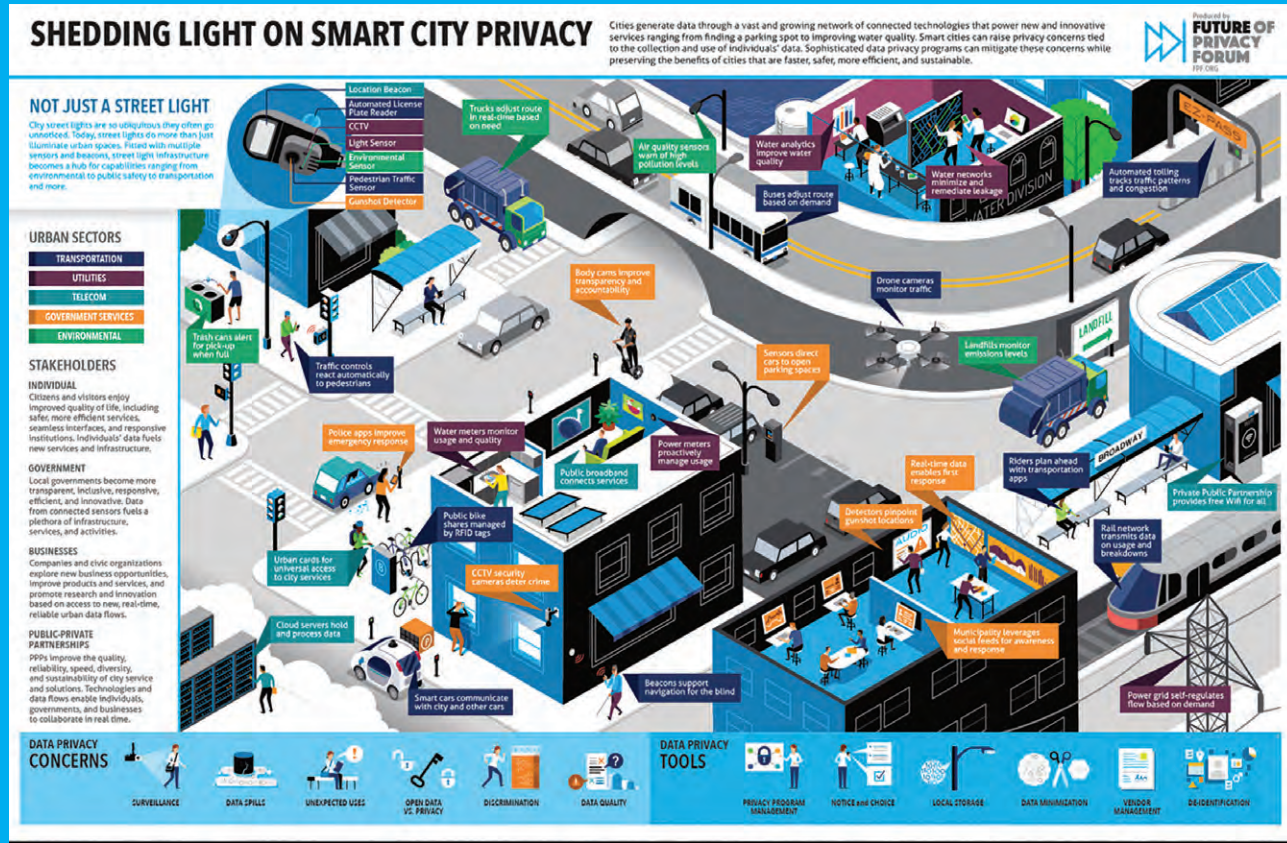
It's not just your phone that's gotten smarter. Here's a smart city example: city streetlights are so ubiquitous they usually go unnoticed—but there's more to them than meets the eye. Today's lights can be fitted with multiple sensors and beacons, upgrading existing infrastructure into a hub for capabilities ranging from environmental to public safety to transportation. Released in 2017, this infographic allows users to click on features to learn more about smart city technologies, how they're used and what they mean for privacy. The tool also acts as a central repository for privacy-related guidance documents, best practices, reports, codes of conduct, and other resources that can help local policymakers, technologists, and citizens navigate these complex issues and integrate digital services in privacy-protective ways.

Consumer Wellness and Wearables

Consumer-generated data represents an important and growing subsection of personal health data, as consumers adopt wearables and health-tracking devices in record numbers. Devices that help users track physiological information hold the potential to greatly improve consumers' lives, and research based on data collected by wearables could reveal insights with broad societal benefits. While sensitive health and wellness data is critical to giving consumers the experiences they want and need, it will be essential that privacy concerns raised by the collection and use of this data are addressed.

FPF is committed to supporting responsible privacy and security practices for wearables, mobile apps, services, and devices that utilize consumers' health, wellness, and physiological data. As the leading advocate for business practical approaches to consumer privacy, FPF has been at the vanguard of privacy issues around the growing Internet of Things, including the smart grid, smart home devices, mobile location tracking, wearables, and connected cars.

## Highlights of our work in 2016

Best Practices for Consumer Wearables and Wellness Apps and Devices

FPF released Best Practices for Consumer Wearables and Wellness Apps and Devices, a detailed set of guidelines that responsible companies can follow to ensure they provide practical privacy protections for consumer-generated health and wellness data. The document was produced with support from the Robert Wood Johnson Foundation and incorporates input from a wide range of stakeholders including companies, advocates, and regulators.

2016 FPF Mobile Apps Study

FPF released 2016 FPF Mobile Apps Study, which underscores the necessity of strong best practices for health and wellness data. The study revealed that health and fitness apps – which often control and link to wearable devices, and which can collect sensitive health and wellness data – do worse than average at providing privacy policies.
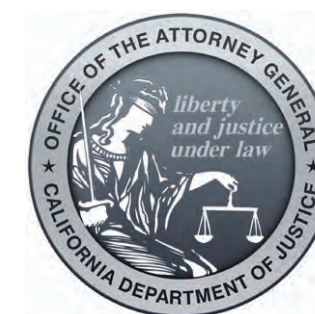
FPF and Carnegie Mellon University Research Leads to New Tool from California Attorney General

In October 2016, the current Attorney General of California, Kamala D. Harris, announced the release of a new form that allows consumers to report potential violations of the California Online Privacy Protection Act (CalOPPA) by websites and online services. Attorney General Harris' announcement explained that FPF's 2011 research into app privacy policies had prompted an earlier agreement between her office and prominent mobile app platforms to encourage apps to post privacy policies. Now, a new FPF study commissioned by Attorney General Harris revealed the need for further work, leading to the release of the new complaint form.

August 2016
FPF Mobile Apps Study

FUTURE OF PRIVACY FORUM

The 2016 FPF Mobile Apps Study underscores the necessity of strong Best Practices for health and wellness data. The App Study revealed that while the number of apps that provide privacy policies continues its upward trend from our previous surveys in 2011 and 2012, health and fitness apps – which may access sensitive, physiological data collected by sensors on a mobile phone, wearable, or other device – do worse than average at providing privacy policies. Only 70% of top health and fitness apps had a privacy policy (6% lower than overall top apps), and only 61% linked to it from the app platform listing page (10% lower than overall top apps).

The App Study also looked specifically at period tracking and sleep aid apps. Only 63% of period tracking apps provided a link to the privacy policy from the app platform listing page. More disappointingly, only 54% of sleep aid apps provided a link to the privacy policy from the app platform listing page.

"Even though a privacy policy is not the be all and end all for building consumer trust, there is no excuse for failing to provide one – doing so is the baseline standard," said John Verdi, FPF's Vice President of Policy. "App platforms have made it easier for developers to provide access to privacy policies. Consumers expect direct access to privacy policies, and users can review them before downloading an app."

Location & Ad Practices

Addressing the privacy issues related to advertising technology and online tracking has been a key focus since FPF's founding. Increasingly, the mobile advertising space and emerging geo-location tracking technologies are at the forefront of new consumer offerings. Thus it is not surprising that regulators, industry leaders, and advocates are all taking a hard look at questions about how to appropriately collect and handle consumer data for advertising, location targeting, and audience measurement.

As a leading advocate for practical approaches to consumer privacy challenges, FPF is at the forefront of conversations about the commercial benefits of advertising technologies and the need to address related privacy issues in order to build and maintain consumer trust. FPF's goal is to explore new and evolving advertising technologies and provide guidance on potential privacy issues that may emerge.

Highlights of our work in 2016

Kids & The Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots

FPF released a white paper co-authored with the Family Online Safety Institute (FOSI), Kids & The Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots, in which we discussed the benefits of connected toys while pushing for more companies to adopt leading industry practices for the responsible protection of data from children.
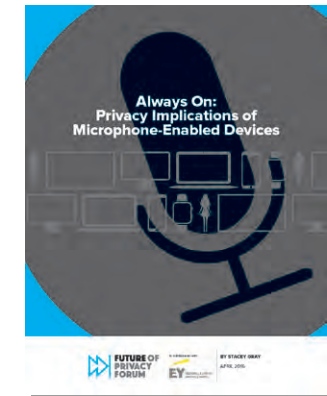
Always On: Privacy Implications of Microphone-Enabled Devices

FPF released Always On: Privacy Implications of Microphone-Enabled Devices, a white paper by Stacey Gray detailing the benefits of speech recognition, and discussing the uses of data by home devices that are using voice command as their primary user interface.

FPF hosted its first annual Tech Lab, in which we invited regulators to visit our offices and explore a range of technologies, including retail phone tracking, beacon-enabled signage, Smart Home gadgets, and voice-enabled toys.

International

FPF maintains expertise regarding emerging privacy issues in the EU, including: providing education regarding EU legal regime and procedure; convening the Brussels Privacy Symposium; hosting events at the Data Protection Commissioners' conference and CPDP; and performing research and education regarding the impact of GDPR Article 8, which raises the age of consent for data processing in Europe to 16.

Highlights of our work in 2016

FPF and Goethe-Institut presented an intensive education program titled: 'Understanding EU Law, Institutions and Policymaking: An Advanced Legal Colloquium for Privacy Leaders.' The goal of the program was to provide privacy experts with a deeper understanding of the broader legal environment in Europe. The program focused on politics and policy that will help privacy and policy leaders of US multi-nationals better understand our partners across the Atlantic.

FPF and the Vrije Universiteit Brussel have established a joint program to develop and promote research, scholarship and best practices to support beneficial uses of data while respecting individuals' fundamental rights. The Brussels Privacy Symposium draws on the expertise of leading EU and US academics, industry practitioners, and policy makers to produce an annual workshop highlighting innovative research on emerging privacy issues. The Symposium launched on November 8 with the workshop, Identifiability: Policy and Practical Solutions for Anonymization and Pseudonymization.

Algorithms

FPF convened leading stakeholders from industry, civil society, and academia for a small, invitation only cross sector discussion designed to better understand the issues surrounding the use of sensitive data and algorithms. A few experts from civil society and industry led the discussion. All attendees participated in a thoughtful examination of the concerns that have been raised and how to best address them. Our work in this area continues with a presentation at the 2017 RightsCon in Brussels.

Privacy Research and Data Responsibility Research Coordination Network

FPF launched a Privacy Research and Data Responsibility Research Coordination Network (RCN). The RCN is a project funded by the National Science Foundation to help academic researchers and industry practitioners better communicate and collaboratively address research priorities identified in the National Privacy Research Strategy. The RCN will inform the public debate on privacy, provide useful information to policy makers, and contribute to the development of systems and products used to help society realize the benefits of networked information technology without sacrificing privacy and individual rights.

De-Identification

In the era of big data, the debate over the definition of personal information, de-identification and re-identification has never been more important. Privacy regimes often rely on data being considered personal in order to require the application of privacy rights and protections. Data that is anonymous is often considered free of privacy risk and available for public use.

FPF has proposed that legal rules for data should be calibrated depending on multiple gradations of identifiability and that administrative controls should be credited as part of a responsible approach to de-identification efforts. FPF developed a practical framework for de-identification based on the nature of the identifiers and the safeguards and controls placed on the way data are obtained, used or disseminated. FPF is continuing to develop models that improve transparency and terminology around de-identification, and that advance practical de-identification and support the utility of data.
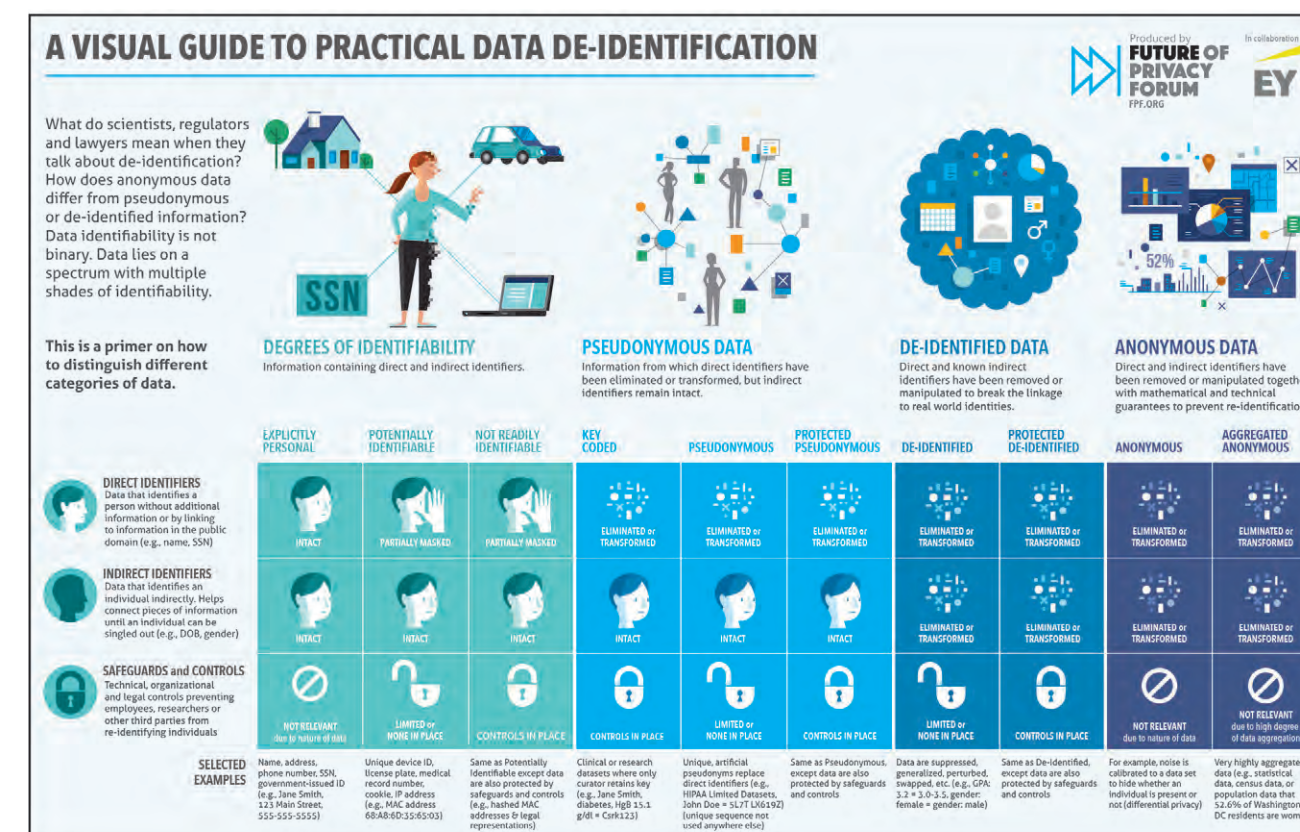
Highlights of our work in 2016:

FPF's framework described in *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, was published in the Santa Clara Law Review and FPF also created an accompanying *Visual Guide to Practical Data De-Identification.*

Participant at "Ensuring Individual Privacy in a Data Driven World" in Paris at Criteo Labs reads our *Visual Guide to Practical Data De-Identification.*

FPF's framework described in *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, was published in the Santa Clara Law Review and FPF also created an accompanying *Visual Guide to Practical Data De-Identification.*

Data Research Ethics

FPF is calling for new frameworks and standards to promote valuable research and to ensure the ethical use of data for research. Sponsored by the National Science Foundation and the Alfred P. Sloan Foundation, FPF held a day-long workshop to move the discussion on ethical review mechanisms for data collected in corporate, nonprofit, and other non-academic settings. As part of the *Beyond IRBs* workshop, FPF and the Washington & Lee School of Law issued a call for papers addressing ethical, legal, and technical guidance for organizations conducting research on personal information. The papers were published in Spring 2016 in the *Washington & Lee Online Law Review*.


The workshop brought together over 60 researchers, including lawyers, computer scientists, ethicists and philosophers, as well as policy makers from government, industry and civil society, to discuss a blueprint for infusing ethical considerations into organizational processes in a data rich environment.

Drones

Drones, otherwise known as unmanned aircraft systems (UAS), promise to carry a wide array of payloads and serve a variety of different functions for use in both the public and private sectors. However, the same characteristics that make drones versatile platforms — compact design, maneuverability, load-bearing capacity, and networks of recording and sensory devices — also raise privacy issues. As regulators consider the safety challenges posed by UAS, consumers need transparency and accountability from organizations and drone operators alike on the issue of data collection.

Highlights of our work in 2016
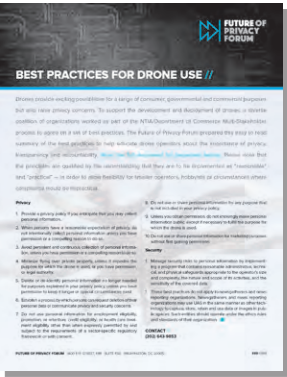
Multi-Stakeholder Group Finalizes Agreement on Best Practices for Drone Use

In May 2016, a wide range of privacy groups and industry stakeholders participating in the National Telecommunications & Information Administration (NTIA) Multi-Stakeholder process concerning privacy, transparency, and accountability issues regarding commercial and private use of unmanned aircraft systems (drones) agreed on a set of best practices. FPF worked with the group to help achieve consensus and created an easy to read summary of the best practices to help educate drone operators.

Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft

In response to the Administration's call to-action on privacy protections related to drone operations, FPF, Intel, and PrecisionHawk released Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft.

Consumer Business Dialogue and Capital-Area Academic Network

FPF's Consumer Business Dialogue convenes regular meetings to discuss the launch of a new product or service, to talk through privacy implications of existing technologies, and to answer questions from consumer advocates. The Capital-Area Academic Network serves to build academic relationships and connect scholars with privacy professionals.

Highlights of our work in 2016

"Owned: How the Internet of Things Took Our Property and Privacy"

Professor Joshua Fairfield from the Washington and Lee University School of Law joined us to discuss a chapter from his upcoming book, "Owned: How the Internet of Things Took Our Property and Privacy." The chapter highlights the importance of ownership in preserving privacy – and what society may lose with the erosion of ownership in the digital age. The chapter focuses on how more "concrete" property rights can serve as a backstop for buttressing harder-to-define privacy rights. A diverse group of attendees from business, government, advocacy, and academia joined to debate and discuss the chapter.

The 7th Annual Privacy Papers for Policymakers

Each year, FPF invites privacy scholars and authors with an interest in privacy issues to submit papers to be considered for FPF's Privacy Papers for Policymakers Award (PPPM). The PPPM Award recognizes leading privacy scholarship that is relevant to policymakers in the United States Congress, at U.S. federal agencies, and for data protection authorities abroad.

This year, the winning authors were invited to join FPF and Honorary Co-Hosts Senator Edward J. Markey, Congressman Joe Barton, and Congresswoman Diana DeGette, to present their work at the Dirksen Senate Office Building with policymakers, academics, and industry privacy professionals. FPF published a printed digest of summaries the winning papers for distribution to policymakers, privacy professionals, and the public.

FPF Education and Innovation Foundation

The FPF Education and Innovation Foundation, a 501(c)(3), endeavors to educate the public about issues relating to data privacy. Through research, publications, educational meetings, and other related activities the Foundation advances responsible data practices and brings together leaders from industry academia, law, and advocacy groups. Using its research, the Foundation educates the public on the importance of data privacy, new and developing issues in data privacy, and responsible data practices to best protect the public's interest.

FPF Education and Innovation Foundation Board of Directors

Mary Culnan	**Christopher Wolf**	**Debra Berlyn**	**Jules Polonetsky**
President	Secretary	Treasurer	CEO

The Foundation supports key FPF activities, such as:

Best Practices for Consumer Wearables and Wellness Apps and Devices

A detailed set of guidelines that responsible companies can follow to ensure they provide practical privacy protections for consumer-generated health and wellness data.

Beyond IRBs: Ethical Review Processes for Big Data Research

A workshop designed to animate the discussion on ethical review mechanisms for data collected in corporate, nonprofit, and other non-academic settings.

FERPA|SHERPA

A website providing service providers, parents, school officials, and policy makers easy access to laws, best practices, and guidelines that are essential to understanding education privacy.

Research Coordination Network

A community of academic researchers and industry practitioners to support industry-academic cooperation to address research priorities identified in the Administration's recently released National Privacy Research Strategy.

Student Privacy Boot Camps

Comprehensive programs held for small and startup ed tech companies to provide training on US privacy laws, best practices, and advocate concerns.

Student Privacy Pledge

Effective January 1, 2015, this is a promise to parents and students by leading ed tech companies regarding the handling of student data. Endorsed by President Obama, the Pledge now has over 300 signatories and continues to grow.

Surveys of Parent Perceptions on Technology and Student Data Use

Designed to gain a better understanding of what public school parents actually know and want concerning the use of technology and data within the educational system. FPF has committed to conduct this survey annually to track trends in parent responses over time.

By the Numbers

137
Corporate Supporters

34
New Corporate Supporters since January 2016

39
Academics

20
Advocates

11
Full-Time Staff

8
Senior Fellows

1
Fellow

1
Junior Fellow

1
RCN Network Director

84%
Corporate Contributions

12%
Grants

The FPF Team

Future of Privacy Forum and FPF Education and Innovation Foundation Financials

Consolidated Statement of Activities for the fiscal year ending on December 31, 2015.

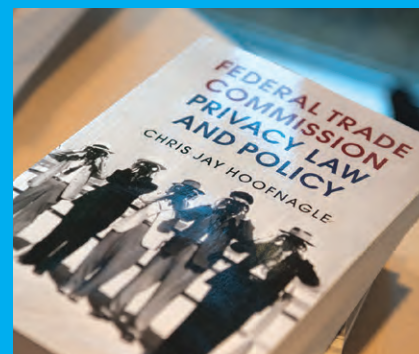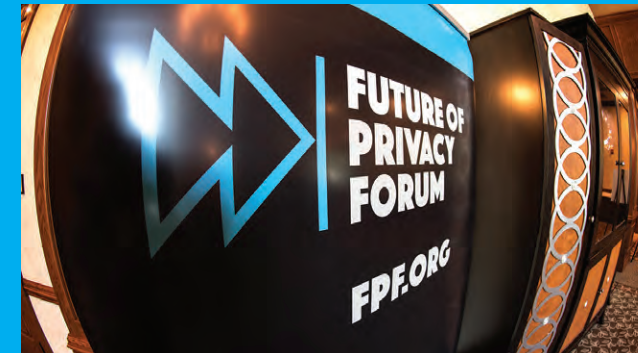|	FPF	EIF	FY 2015
REVENUE			
Grants and Contributions	3,099,833	1,358,964	4,458,797
In-Kind Contributions	10,767	12,499	23,266
Registrations and Sponsorships	22,181	—	22,181
Total Revenue	**3,132,781**	**1,371,463**	**4,504,244**
EXPENSES			
Program Services	1,638,361	966,630	2,604,991
General and Administration	207,880	305,654	513,534
Fundraising	229,741	15,977	245,718
Total Expenses	**2,075,982**	**1,288,261**	**3,364,243**
NET ASSETS			
Beginning of Year	912,614	342,401	1,255,015
Change in Net Assets	1,056,799	83,202	1,140,001
Total Net Assets, End of Year	**1,969,413**	**425,603**	**2,395,016**

FY 2015 Combined Expenses

- Program Services
- General Administration
- Fundraising

7%

15%

77%
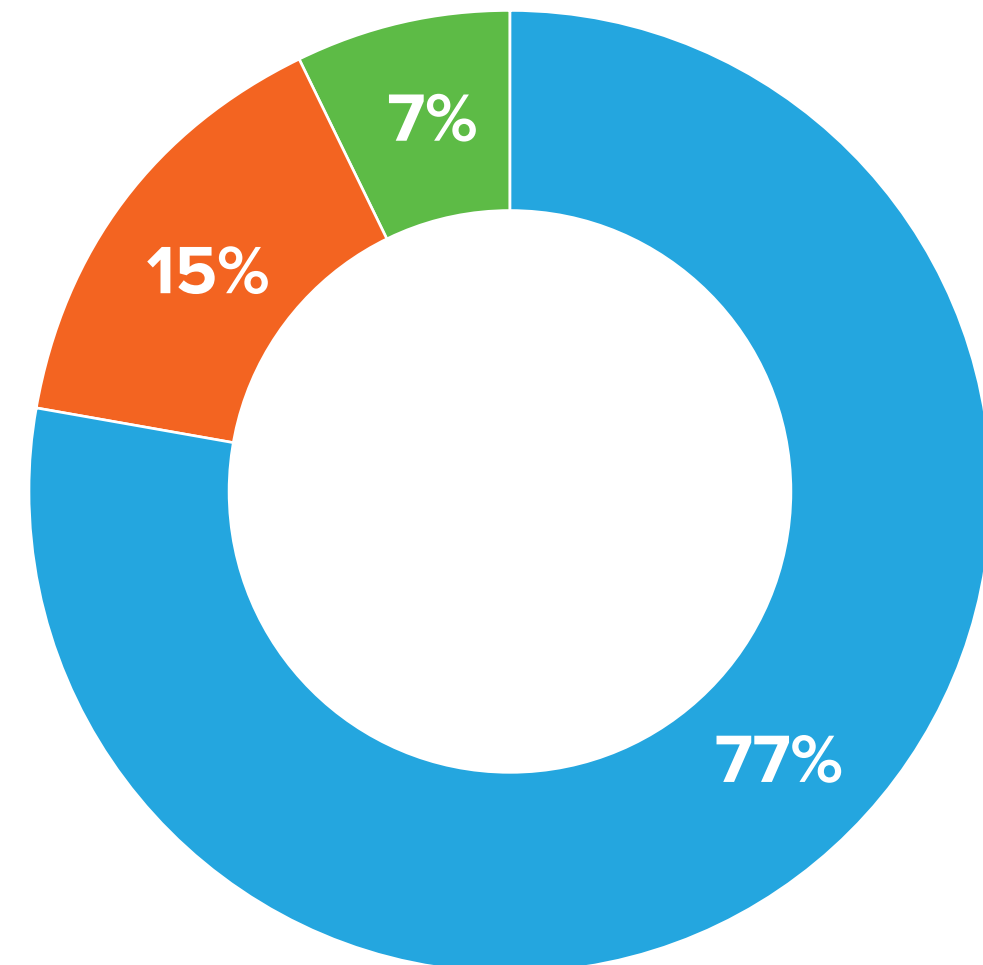
2016 Future of Privacy Forum Advisory Board Meeting