Daniel A. Small
Robert W. Cobbs
COHEN MILSTEIN SELLERS & TOLL
1100 New York Avenue NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Jeffrey L. Kodroff
John A. Macoretta
Mary Ann Geppert
SPECTOR ROSEMAN & KODROFF PC
2001 Market Street
Suite 3420
Philadelphia, PA 19103
Telephone: (215) 496-0300
Facsimile: (215) 496-6611

Elizabeth J. Cabraser
Michael W. Sobol
Melissa Gardner
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

Class Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE LLC STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION	Case No: 3:10-md-02184-CRB **CLASS ACTION** **PLAINTIFFS' STATUS REPORT CONCERNING CY PRES RECIPIENTS** Judge: The Hon. Charles R. Breyer

Pursuant to the Settlement Agreement in this case and the Court's Final Approval Order, Plaintiffs file with this Status Report biannual reports from the following *cy pres* recipients:

Center on Privacy & Technology at Georgetown Law (Ex. A)

Center for Digital Democracy (Ex. B)

MIT Internet Policy Research Initiative (Ex. C)

World Privacy Forum (Ex. D)

Public Knowledge (Ex. E)

Consumer Reports (Ex. F)

Rose Foundation for Communities and the Environment (Ex. G)

Electronic Privacy Information Center (Ex. H)

These reports outline how each recipient has used funds awarded in this case to protect internet privacy, and work they expect to do in the future.[1] *See* Decl. of Robert W. Cobbs Exs. A-H. To date, the *cy pres* recipients have expended approximately $4,030,000 of the $9,059,247 distributed last year. The funds have enabled a wide range of important work protecting consumers' internet privacy – from developing consumer tools to opt out of data collection and sales, to deep-dive investigative research on secretive data brokers, to legislative and regulatory advocacy. Through sub-grants by the Rose Foundation for Communities and the Environment, funds have reached impactful local community groups educating underserved groups, organizing against internet surveillance, and working with local governments to make privacy-protective procurement decisions, among others.

As set forth in the Settlement Agreement, Plaintiffs' Co-Lead Counsel will ensure that these reports are also posted on the Settlement Website.

Plaintiffs expect to distribute remaining residual funds from the Settlement Fund within 30 days and thereafter will submit a final accounting to the Court. Plaintiffs will continue to file *cy pres* recipients' biannual reports on an ongoing basis until the awards have been exhausted.

[1] One of the cy pres recipients, the American Civil Liberties Union Foundation, fully exhausted awarded funds as of the last report and their reporting obligation has expired. *See* Decl. of Jeffrey L. Kodroff, Ex. A, Settlement Agreement ¶ 30, ECF No. 166-2 (July 19, 2019); Decl. of John A. Macoretta, Ex. A, ACLU Report, ECF No. 229-4 (June 8, 2023).

Dated: December 8, 2023

Respectfully submitted,

By: */s/ Robert W. Cobbs*
Robert W. Cobbs

COHEN MILSTEIN SELLERS & TOLL
Daniel A. Small
Robert W. Cobbs
1100 New York Avenue NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
dsmall@cohenmilstein.com
rcobbs@cohenmilstein.com

SPECTOR ROSEMAN & KODROFF PC
Jeffrey L. Kodroff
John A. Macoretta
Mary Ann Geppert
2001 Market Street
Suite 3420
Philadelphia, PA 19103
Telephone: (215) 496-0300
Facsimile: (215) 496-6611
jkodroff@srkattorneys.com
jmacoretta@skrattorneys.com
mgeppert@skrattorneys.com

Class and Co-Lead Counsel

Elizabeth J. Cabraser (State Bar No. 083151)
Michael W. Sobol (State Bar No. 194857)
Melissa Gardner (State Bar No. 289096)
LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008
ecabraser@lchb.com
msobol@lchb.com
mgardner@lchb.com

Class and Liaison Counsel

Robert W. Cobbs
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, Ste. 500
Washington, DC 20011
Telephone: (202) 408-3600

Class and Co-Lead Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE GOOGLE LLC STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION	Case No. 3:10-md-02184-CRB **CLASS ACTION** **DECLARATION OF ROBERT W. COBBS IN SUPPORT OF PLAINTIFFS' STATUS REPORT CONCERNING CY PRES RECIPIENTS** Judge: Hon. Charles R. Breyer

I, Robert W. Cobbs, declare:

1. I am a partner in the law firm Cohen Milstein Sellers & Toll PLLC and a member in good standing of the Bars of the District of Columbia and the State of New York. I submit this Declaration in support of Plaintiffs' Status Report. I have personal knowledge of the facts set forth herein, and if called to testify thereto, could and would do so competently.

2. Attached as Exhibits A through H are reports from each of the eight *cy pres* recipients who received funds from the Settlement Fund in this case but have not yet exhausted those funds.

I declare under penalty of perjury that the foregoing is true and correct as to all matters of which I have personal knowledge. Executed this 8th day of December, 2023 in Washington, D.C.
.

/s/ Robert W. Cobbs
Robert W. Cobbs

EXHIBIT A

GEORGETOWN LAW
Center on Privacy & Technology

(202)-662-9879
privacy@georgetown.edu

www.law.georgetown.edu/
privacy-technology-center

December 8, 2023

Hon. Charles Breyer
Judge, U.S. District Court
Northern District of California
450 Golden Gate Avenue
San Francisco, CA 94102

Dear Judge Breyer,

As the Executive Director of the Center on Privacy & Technology at Georgetown Law (the Center), I am writing to report on our use of the funds we received in December 2022 as a cy pres beneficiary in the settlement of *In re Google LLC Street View Electronic Communications Litigation.*

The Center conducts research and advocacy to expose and mitigate the impact of mass surveillance on historically marginalized communities. We are known for our groundbreaking work on police use of face recognition technology, our exposure of dragnet surveillance by immigration authorities, and for our Color of Surveillance conference, an event that brings together scholars, activists, artists, and community members for interdisciplinary conversations on a different theme each year. Situated at Georgetown Law, we also have a pedagogical mission to train new lawyers to analyze the practical, legal, and ethical effects of digital era technologies in democratic society..

The Center is using the cy pres award to support research and advocacy across our four areas of programmatic focus: surveillance in systems of policing and punishment, surveillance of immigrant communities, surveillance of workers, and surveillance of families. Specifically, the funds are supporting salary costs for our programmatic staff who have the primary responsibility for the research in each of these four areas.

In our previous report to the Court, we projected that we would spend the majority of the cy pres award on salary for four new positions, a Director of Research & Advocacy, two Justice Fellows and a Staff Technologist. We successfully filled three of those positions and anticipate recruiting the technologist some time in 2024. Half of the technologist's salary will be paid from the cy pres award. We are also relying on the award to help fund a team of law student research assistants, to pay non-salary costs associated with our investigations (such as FOIA fees, travel, etc), and some of the costs associated with the planning and production of public facing events to disseminate our research and raise awareness about the impact of digital era surveillance.

To date, we have spent approximately half of the funds received. If our programmatic work proceeds as planned, we expect to expend the remaining funds within the next 12 months. Below is a brief description of some of the projects towards which have directed the award during the period between June 1, 2023 and November 30, 2023.

Surveillance of Immigrant Communities

Following the release of our report, American Dragnet: Data-Driven Deportation in the 21st Century, we have continued to investigate the variety of databases and networks that Immigration and Customs Enforcement (ICE) relies upon to carry out detention and deportation, with a particular focus on the way that ICE is exploiting databases developed by the state and local government agencies that administer essential benefits and services. We have provided technical support and legal research support to several grassroots immigrant rights organizations seeking to understand the implications of our research for their community members.

We also collaborated with the International Justice Clinic at UC Irvine to draft a submission to the United Nations Human Rights Committee, the body that monitors the implementation of the International Covenant on Civil and Political Rights (ICCPR), in advance of the fifth periodic review of the United States. Our submission made the case that ICE's dragnet surveillance practices amount to an egregious violation of human rights law, and of US obligations under the ICCPR. During the meetings in Geneva, one Committee member questioned the US delegation about the practices we described in our submission. In its published Concluding Observations the Committee again raised serious concerns about ICE's data practices and made several recommendations for steps the federal government should take to bring those practices in line with treaty obligations.

Research on DNA Collection and DNA Analysis Technologies

The Center is in the midst of several interconnected investigations into the expansion of public and private DNA databases, coinciding with the development and deployment of new DNA analysis technology especially in local, state and federal law enforcement contexts. In the year since we received the cy pres award, we have completed the research and drafting for our first report on this topic, which focuses on the DNA collection policies and practices of the Department of Homeland Security. We are in the final stages of revision, proofreading and publication design, and we expect the report to be released in early 2024.

Simultaneously, we are in the process of gathering information about the adoption of corporate-owned DNA analysis technologies by local police departments. We have submitted several dozen Freedom of Information Act requests to law enforcement agencies across the country, requesting documents related to the procurement and use of DNA analysis technology. We are collaborating with faculty in Georgetown's computer science department to analyze the technology itself. Informed by a robust scientific understanding of the technology, we will analyze its law and policy implications with a focus on privacy and civil rights harms. This work is resource intensive and we expect to rely heavily on the cy pres award to help pay for the staff time as well as the non-salary costs associated with these investigations.

Family Surveillance

In July of this year we opened a new program area to address the impact of surveillance technology and targeting families. This work is very broad in scope, including everything from the surveillance of abortion access to the use of discriminatory algorithms in the child welfare system. This program area is just beginning to take shape, but in November we submitted comments on the Department of Health and Human Services' Section 504 rulemaking on disability discrimination. Our comments call on HHS to look at the frontend of the family policing system — specifically, how disability discrimination shows up in reporting, screening, and investigations, including through surveillance and the use of data-driven tools. Funds from the award paid for the time of our Director of Research & Advocacy and one of our Justice Fellows to work on this project.

We are very grateful to have been selected as beneficiaries of the settlement in this important litigation, and we are eager to ensure the funds are used to further the interests of the class. We welcome any follow-up questions the Court may have about our use of the award..

Sincerely,

Emily Tucker
Executive Director
Center on Privacy & Technology
Georgetown Law Center

EXHIBIT B

CENTER FOR
DIGITAL
DEMOCRACY

December 1, 2023

Robert W. Cobbs
Cohen Milstein Sellers & Toll PLLC
1100 New York Avenue, 5th Floor
Washington, DC 20005

I am pleased to report on the Center for Digital Democracy's (CDD) work under the "Google Street View" *Cy Pres* funding for the period of June 2 to December 1, 2023. We have been engaged in four broad areas of privacy-focused research and advocacy efforts:

1. **Analysis of "connected" TV (CTV) and streaming video data and marketing practices and their impact on consumer privacy.** Streaming video is now the leading source of television programming in the U.S. CDD has made it a priority to analyze the new and evolving data gathering, targeting and measurement systems that are spreading across the connected TV (CTV) landscape, encompassing programmers, networks, advertisers, retailers, device manufacturers, as well as a growing list of other partners. A key focus of this research is to document how CTV data tactics specifically impact both young people and communities of color. During the past six months, we have shared our research with policymakers, the press, and other key organizations. For example, we released a report in July examining the implications of CTV data and marketing operations on the contract negotiations between the U.S. entertainment creative community and the Hollywood studios and networks. We also provided information and analysis in the streaming industry's new lobbying efforts to journalists and policymakers. We are in the process of writing a report for the general public on the privacy issues raised by the contemporary streaming video practices, which we plan to release in the first quarter of 2024.

2. **Promoting digital privacy and consumer protection policies for children and adolescents.** CDD is considered one of the country's leading NGOs working to promote policies for protecting young people's data on social media, mobile, and other digital platforms. Our current work is a continuation of the pioneering role we played during the 1990s in spearheading the campaign that led to passage of the Children's Online Privacy Protection Act (COPPA), as well as our successful leadership efforts to ensure that the rules for implementing this historic law remain up to date in the rapidly evolving digital marketing system. Over the last six months, we have worked closely

with regulators to help them craft new policies to address a range of new digital marketplace developments and practices. For example, we collaborated with our allies in the advocacy community to document and compile information on Google's child-directed behavioral marketing practices, and also reviewed independent research on the company's internal operations. These materials were submitted to the Federal Trade Commission (FTC) and to journalists, leading to significant coverage in the *New York Times* and other major news outlets. To assist the FTC in its review of parental consent mechanisms, which allowed by COPPA for the collection of data from children, CDD provided staff (as well as reporters) with our documentation of some of the most recent industry developments that pose new threats to children's online privacy, and filed comments urging the Commission to adopt additional regulatory tools to address the problem.

3. **Monitoring contemporary data and marketing practices for targeting youth with unhealthy food and beverage products.** CDD continues to advise public health groups, scholars, policymakers and advocates on the latest data-driven practices deployed by food and beverage corporations, ad agencies, tech companies, and retail outlets to target children and adolescents with advertising for soft drinks, fast food, and other unhealthy products. Our 2021 report, *Big Food, Big Tech and the Global Childhood Obesity Pandemic,* has been cited extensively by scholars, advocates, and health organizations around the world. Our most recent work has included three new reports: 1) a case study of the twenty-year campaign that led to forthcoming comprehensive regulations in the United Kingdom to end online marketing of unhealthy foods and beverages to the public; 2) an analysis of the threats posed by digital marketing to health equity; and 3) a paper we commissioned by a leading global scholar reviewing recent scholarly research around the world to measure the scope and impact of digital food marketing on youth health behaviors. We are in the process of preparing these reports for release to the public. We also presented our research at a meeting organized by the Transatlantic Consumer Dialogue (TACD), representing the leading consumer and privacy rights groups in both the U.S. and EU; and conducted two briefings with grantees of leading public health foundations—Bloomberg Philanthropies and the Robert Wood Johnson Foundation.

4. **Ongoing "big picture" research and analysis of contemporary commercial data technologies, systems, and practices.** CDD is one of the few U.S. digital rights NGO's that closely tracks and analyzes the broad technological and industry developments that are impacting the digital privacy of consumers. We are particularly focused on such new and evolving areas as Generative AI, "attention measurement," neuromarketing, "contextual marketing 2.0," and geolocation surveillance, assessing how their combined impacts will further shape and refine the marketplace and pose additional challenges to consumer privacy. This work includes ongoing analysis of data and digital marketing practices across major "vertical" markets, including health, financial, retail, politics, and entertainment. We also monitor digital marketing application developments on multiple platforms – including gaming, social media, mobile, and online video – to explore their implications for privacy and consumer protection. We regularly share this expert analysis with regulators, journalists and other

advocates. For example, during this reporting period, CDD briefed the FTC's antitrust and consumer protection leadership on data privacy issues involving retail media, identity curation, and so-called "clean rooms." We conducted similar briefings for the staff of the Consumer Financial Protection Bureau (CFPB).

We remain grateful for the generous financial support we received from the *Cy Pres* funds, and we look forward to continuing our leadership role to ensure privacy protections for consumers in the evolving commercial digital landscape.

Sincerely,

Jeff Chester
Executive Director

Center for Digital Democracy

Statement of Expenditures

May 26, 2023 - November 30, 2023

	Cy Pres Award Expenses	Other Grant Expenses	Total
Expenses			
Salaries	124,607.14	92,642.84	217,249.98
Benefits & Payroll Taxes	17,163.08	15,511.09	32,674.17
Consultant Services	-	44,100.00	44,100.00
Accounting Fees		5,349.17	5,349.17
Bank Charges		249.24	249.24
Depreciation Expense		5,412.18	5,412.18
Grants and Contributions		500.00	500.00
Information Technology	997.29	3,394.75	4,392.04
Insurance		874.41	874.41
Membership Dues		175.00	175.00
Miscellaneous		400.00	400.00
Occupancy Costs		1,035.60	1,035.60
Office Supplies		1,761.86	1,761.86
Postage and Delivery		9.99	9.99
Printing & Publications	1,964.20	8,235.97	10,200.17
Telephone & Communications		2,740.40	2,740.40
Travel & Meetings	-	1,689.70	1,689.70
	144,731.71	184,082.20	328,813.91
share of Administrative costs	14,473.17	17,753.05	(32,226.22)
Total Expenses	159,204.88	201,835.25	296,587.69

EXHIBIT C

Internet Policy Research Initiative
Massachusetts Institute of Technology

Progress Report #1: Privacy Education and Design Lab (PEDaL)
December 2023

Project Summary

The new MIT Privacy Education and Design Lab (PEDaL is developing new approaches to privacy education and research to assure that the software developers educated at MIT will learn to be aware of privacy risks as a core part of their computer science education. PEDaL will building on the novel, multi-disciplinary education approach of MIT's Internet Policy Research Initiative by extending two courses currently offered by IPRI faculty: 6.4590: Foundations of Internet Policy, and 6.S978: Privacy Legislation Law and Technology (offered jointly between MIT Electrical Engineering and Computer Science Department and Georgetown Law School (see New York TImes: Natasha Singer, Top Universities Join to Push 'Public Interest Technology', March 11, 2019; MIT Spectrum, Legal/Code-MIT engineering students team up with Georgetown lawyers-in-training on internet privacy legislation, Winter 2018). These courses teach 30+ computer science and engineering students each semester to develop the intellectual skills necessary to understand the complex public policy questions, including privacy, raised by computing in our society today. PEDaL will add a hands-on laboratory component to each course giving students in-depth experience of actually building and analyzing technical systems that address privacy harms. PEDaL will materially advance the interests of the Class in Joffe v. Google, helping to assure the members of the class, and those similarly situated in the future are far less likely to be victims of privacy harm arising from poorly-educated software developers and careless product managers.

PEDaL will also lead technical research on privacy-enhancing data systems and analytic techniques to develop new software architectures that reduce the risk of privacy harm such as was suffered by the plaintiff class. We propose to lead research projects in the following areas:

- Database Systems: Explore new data management architectures to provide enterprises with purpose management, provable delete and automated accountability tools for managing personal data according to legal rules and institutional commitments. Database systems that do a better job of tracking legal purposes, and detecting unlawful purposes, are possible and could go a long way to alert against harm experiences in the Streetview case.

- Human Computer Interaction: Apply rigorous HCI research methodologies to understand the impact of various privacy policy environments on user behavior and learn when the user experience is producing chilling effects. This research will inform both services design and policymaking.

Background

Project home: Project Principal Investigation, Daniel J. Weitzner, holder of the 3Com Founders Senior Research Scientist chair at the MIT Computer Science and Artificial Intelligence Lab (CSAIL), founded IPRI in 2015 as a response to the critical need for technology-informed policy making in the areas of privacy, security, networks and the Internet economy. The group plays an important bilingual role of informing policy making with technical expertise, and helping engineers build secure and privacy protecting products that are informed by policy. To achieve this mission, IPRI produces fundamental, cross-disciplinary technology and policy research (an average of 38 research papers a year since 2018); engages with global policymakers, industrial partners, and civil society organizations; and is building a network of students educated in the field of Internet policy.

MIT is one of the top research universities in the world across a number of disciplines, including engineering, computer science, and economics. MIT has 11,376 students and 13,000 employees. Recently the Institute announced the creation of the Schwarzman College of Computing which represents a new paradigm for computer science research and education that recognizes the importance of addressing the social, ethical and policy impact of computing on society.

IPRI's senior leadership has strong consumer and Internet civil liberty advocacy backgrounds. Daniel Weitzner was the first staff member in Washington DC for the Electronic Frontier Foundation and founder of the Center for Democracy and Technology. He was also a senior policymaker (White House Deputy CTO for Internet Policy). While at the White House, Weitzner was responsible for developing the Consumer Privacy Bill of RIghts in 2012. Taylor Reynolds was the senior economist at the OECD responsible for the Internet economy, and his research on broadband pricing led to multimillion dollar fines against incumbent telecommunication firms engaged in deceptive advertising.

Of particular relevance, Daniel Weitzner has a long history of successful Internet civil liberties advocacy. His work led directly to amendments to the Electronic Communications Privacy Act in 1994 that offered groundbreaking protections for web browsing logs, email records, and other transactional data. (18 USC 2703(d)) Under Weitzner's leadership, the interests of the Class in better privacy protection will be materially advanced.

Expenditures

Between June 1 and November 30, 2023, PEDal has expended a total of $35,529.24 covering initial research and planning for the new course curriculum. Our spending reflects primarily planning and start-up costs for PEDal, which we expect to expand significantly at the start of the new academic year in February 2024. Details on expenditures are provided in the Activities section below.

Activities

- Research in preparation for new privacy curriculum: During this period of time one of our Post-Doctoral Research Fellows conducted technical work on privacy-preserving computation systems for both research on cybersecurity risk measurement and problem sets and in-class exercises which will be used in our Fall 2024 course Foundations of Internet Policy (MIT 6.4590).
  This study will be used to shape course materials and future PEDal research agendas.
- PEDal provided leadership and financial support to a new conference called the ACM Symposium on Computer Science and Law, designed to be a leading venue for interdisciplinary scholarship conducted by computer scientists and lawyers. We are pleased that based on the success of this Symposium that the sponsoring organization, the Association for Computing Machinery (the leading professional and academic society in computer science) has agreed to support this symposium on an ongoing basis. This symposium is vital as a venue for encouraging interdisciplinary scholarship by lawyers and computer scientists working together, a key requirement for making progress on privacy law, public policy and privacy-aware computer systems design.

EXHIBIT D

WORLD **PRIVACY** FORUM

Re: World Privacy Forum 6-Month Report
December 2023

This report provides an overview of how the World Privacy Forum has been utilizing the cy pres funding we received from the Google Street View litigation. We launched several projects in response to the grant earlier this year. As a substantive public interest research group, our work demands the construction of a methodology for each project, careful attention to detail, extensive fact checking, and review prior to publication. This process takes time. We are pleased to report we have two significant projects that are now completed. In addition to these two completed projects, we have also completed the first half of one other project.

In this report we will will outline the projects we have undertaken, and what has been accomplished to date.

I. About the World Privacy Forum

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. The World Privacy Forum is dedicated to understanding and reimagining data governance and data protection in a digital and AI era through pioneering research, analysis, and consumer education of the highest quality. By fostering an inclusive culture of thoughtful inquiry and collaboration, we strive to provide a compelling factual foundation for the development of sound policies and practices that illuminate modern data ecosystems and their governance, safeguard privacy, and uphold the digital rights of individuals and communities alike.

Our work is centered on comprehensive, high-quality research concerning data governance and privacy, with particular emphasis on complex data ecosystems. We publish a wide range of research spanning various subjects such as digital identity, mobile and online privacy, location privacy, identity theft, and more. Our materials regarding health privacy and ecosystems are extensive and range from investigations into genetic privacy, precision medicine, electronic health records, and much more. Our research has led to substantial and meaningful improvements in consumer privacy over now 20 years of work.

As an organization, WPF actively voices its expert opinions and research findings, providing testimony before Congress and federal agencies, as well as regularly commenting on privacy-related regulations. We hold positions in several multilateral organizations; WPF co-chairs the World Health Organization's Research, Academia, and Technical constituency, and participates in a data governance workgroup. We are also proud to serve as co-chair of the civil society stakeholder group at the OECD's Working Party on Artificial Intelligence Policy, AIGO. Additionally, we co-chair the UN Statistical Division's Global Task Force on Data Governance, contributing to a global research project.

You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

II. Complete: Part One of Modern Data Broker Research (This is a two-part project)

WPF has a long history of producing original research regarding data brokers, including data brokers working across ecosystems such as health, finance, technology, and wireless communications, ICT, and other areas. A new project that we have undertaken is to update our research regarding the data broker ecosystem; in the past, data brokers used "data cards" and simple APIs and paper lists to sell consumer data. This has changed significantly now. Today's data broker practices involve larger digital ecosystems, real-time exchanges, and large amounts of data from new sources, for example, from digital wallets …. among many other sources. This project will document the modern data broker ecosystem, what data it ingests, and what, if any, regulations apply, when.

A. Completed deliverable: Regulatory filing, Consumer Financial Protection Bureau.

We have researched and filed formal comments with the Consumer Financial Protection Bureau on modern data broker activities with a request for action to address a range of problems. This was an important — and to our knowledge — the only update on data broker activities that includes intersections with de-identified data as well as identity data. This work was deeply researched, and forms the base of our ongoing research work in this area.

See:

Comments of the World Privacy Forum to the Consumer Financial Protection Bureau regarding Request for Information Regarding Data Brokers and Other Business Practices

Involving the Collection and Sale of Consumer Information, Docket No. CFPB-2023-0020 (PDF, 16 pages)
(Available at: https://www.worldprivacyforum.org/wp-content/uploads/2023/08/WPF_Data_Broker_RFI_CFPB_15July2023_fss.pdf)

B. Completed deliverable: Participation in White House Roundtable on Data Brokers

One aspect of our work is consumer eduction. This extends to ensuring that the research we complete is disseminated publicly and discussed so as to create awareness and positive change. This August, the World Privacy Forum was invited to participate in a Roundtable held by the White House, based on prior work and based on the regulatory filing with CFPB. The Roundtable included a public session and a closed session. We participated in both sessions, and we presented and discussed our new research on modern data brokering issues to peers, government officials, and other invitees.

See:

Readout of White House Roundtable on Protecting Americans from Harmful Data Broker Practices
(Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/16/readout-of-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/)

III. Ongoing: Part Two of Modern Data Broker Research

We have additional research to conduct in regards to this project, which will we undertake in Q 1-4, 2024. The goal of the work is to continue to document and understand data flows, data uses, data brokers and their operations in the US in particular, and how these data flows and activities impact people, groups of people, and communities in regards to privacy, and data sharing (consented and not consented), among other issues.

In fall 2023 WPF added a senior fellow on consent, AI, and privacy. She is an ethicist and experienced privacy engineer with more than 10 years of experience designing digital consent systems used in sensitive human subject research, which has highly regulated consent requirements. Her work integrates with the data broker project, and is focused on consent issues in modern digital ecosystems, including those incorporating AI.

WPF is interested in bringing in work on the consent aspects of the data broker project, because it ties in with an important aspect of the Street View litigation, which involved consumers that had their personal data collected without their knowledge or consent. Today there are similar parallels with additional types of personal consumer data that are being drawn into sophisticated and complex new ecosystems — in some cases without clear lines of consent, or in some cases, without consent. We are examining and documenting how consent is operating today in these more advanced data ecosystems and we are working to find solutions that will improve privacy and improve how consent operates in advanced systems. This research is detailed, and sensitive. We expect to publish next year.

IV. Mapping and Data Visualization Initiatives

A. Completed Project: Mapping Initiative, Global table of data protection laws, regulations, and data protection authorities

The *global table of data protection laws, regulations, and data protection authorities* is a WPF research project that launched in 2021. We crafted a strong methodology and undertook extensive primary source interviews and fact checking to ensure accuracy and quality. This summer, we completed the research and undertook a thorough fact check of our total results, and have now completed the peer review from statistical experts and country-level experts. The funds paid for the US parts of the table only, and only for the work completed after January of 2023.

This work is important because it is the first of its kind that has been completed with desktop and field research that utilizes the UN / ISO M49 standard as an integral part of the methodology. This standard is the internationally accepted, politically neutral standard for the designation of territories and jurisdictions, and it allows for a genuinely comprehensive data set of privacy regulations, privacy regulators, and privacy norms today.

Completed Deliverable: The research for the global table is now complete, and is now in the final draft design stage to create an interactive visualization of the data. We have already reviewed the draft data visualization, and we will be publishing it within the next two to three weeks. This deliverable will be published at www.worldprivacyforum.org.

B. Mapping and Data Visualization Projects Still in Process

WPF has two ID systems-related mapping efforts that are ongoing, and one mapping project relating to AI that is ongoing.

1.) Global table of national and subnational identity systems (including digital ID systems): WPF has already published an extensive global table of national ID systems. This global table is one that WPF keeps up to date on a routine basis. We are currently finalizing the 2023 update to the map, and are preparing to publish within one month. The funds paid for the US parts of this mapping work only.

2.) Mobile digital IDs and digital wallets in the US: We are expanding the identity map data to include a state-by-state mapping of mobile digital IDs in the US, including digital IDs held in digital wallets. Mobile digital IDs that are formal government credentials are new in the US. We will be publishing materials as the digital IDs begin to roll out in the US this year. We are using funds for this part of the project, as it is relevant to the class.

3.) US Laws, Regulations, and Standards regarding Artificial Intelligence and Machine Learning: Currently, there is not a resource that accurately or completely lists all of the US regulatory activity regarding AI / ML. This data visualization addresses this gap. We have already begun this work; we have a methodology in place, and we are now well underway on a systemic review of state and federal law and regulations around AI/ML as well as AI/ ML U.S. standards. This particular table will lay the groundwork for understanding what aspects of AI and ML have regulatory constraints in the US, what those constraints are, what aspects are unconstrained, and how the regulations relate to consumer data privacy.

We have been with these three research projects since May of this year, and estimate that we will begin publishing deliverables for this in March 2024 and continuing through the year.

V. Completed: Significant Research Publication Regarding Privacy, Data Governance, and AI

The World Privacy Forum undertook a significant piece of investigative research in April 2023. This work was very sensitive, and we were not able to publicly discuss the early phases of the work due to these concerns. WPF has a general policy of not discussing or writing about in-process investigative research that is not yet fact-checked and not yet peer-reviewed.

WPF has now completed the research, including final text, fact check, and peer review for this project. We will be publishing this new and groundbreaking research regarding privacy, fairness, and other trustworthiness issues regarding AI in December, 2023. This research is intended to facilitate meaningful improvements in the privacy and trustworthiness of AI systems.

The final, pre-design raw text of the report is 125 pages. The project in total includes a report, which will be published in multiple forms including traditional report form, and as an electronic book. (EPUB). The project deliverables include multiple data visualizations based on the research. To educate consumers and the public, WPF will be holding multiple public-facing live casts and events in Q1 - 2 regarding this work. We will also be presenting a half-day tutorial at a national conference to the technical and standards community (IEEE) on privacy and AI where we will discuss the research, findings, and suggestions in the report.

When the report publishes, which is imminent, we will be posting it and the interactive data visualization on www.worldprivacyforum.org.

VI. Ongoing: Collaboration with Harvard Public Interest Technology Lab Regarding Health Privacy Data and Data Flows

WPF is engaged in its engagement in a significant research project examining standards, methods, and metrics for handling and managing sensitive health data, health data flows, and the effectiveness of existing standards, laws, and practices in the context of today's highly digitalized health sector.

This study fills a critically important gap in today's knowledge base about digital health information and how this information is flowing and regulated / protected outside of HIPAA regulations, and how this information is being utilized by third party entities, including large technology companies, among other entities.

The completed study will answer a roster of pressing privacy questions at the intersection of privacy and digitalized health data, and will provide technical / policy recommendations for addressing the privacy issues per the research documentation.

Thus far, we have been doing the necessary work of setting up the research. We have had a number of on-site and virtual meetings, lasting a total of 10 days of full time work. The primary work thus far has been to set up a working research group between the two organizations, craft a methodology for the work, get sign-off on the methodology, and set parameters for the research tasks as well as timeframes and staff for the research phases. WPF has added a health fellow / intern to assist in the project as of February 2023, and Harvard has added (paid out of their budget) a full-time student to work on this project this summer and into the fall of 2023. The research for this project began in the spring. We are in the midst of the research phase now, which will continue through at least the first half of 2024.

VII. Deputy Director

In order to address capacity issues, WPF hired a highly competent deputy director in February 2023. The deputy director is tasked with assisting with all of the cy-pres - related projects to ensure the timelines for development and completion are staying on track, and to ensure that our quality of work remains at the highest levels. Thus far, the Deputy Director has put in lengthy and substantive work on our forthcoming report, as well as substantive work on the other projects discussed in this document.

VIII. Funds Utilized

Funds utilized thus far are approximately $140,000. These consist primarily of payroll expenses for the project leads and contractors to pay for their time spent on the projects discussed in this report. The funds utilized focused on the US aspects of the research. Project leads are the full-time employees of WPF, contractors include legal review and analysis, copyediting, fact checking, and report design and data visualization.

IX. Conclusion

WPF has undertaken new and meaningful research and data visualization projects since January 2023 to specifically address consumer privacy in data ecosystems in the US context. These projects are high-impact and directly address one or more gaps in knowledge that are highly consequential.

We are pleased that we have had success with Part I of our modern data broker project with its two deliverables. And we are pleased that two large projects are publishing in December, the global tables and the new report on AI and privacy and trustworthiness issues. We've worked quite hard to bring these large projects to fruition. Other projects will take longer to bring to completion, but we will continue to keep the research moving along at a good pace. We have planned an assertive publication schedule with a substantive additional work planned for 2024.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum

EXHIBIT E

Google Street View Funding Report

June 8, 2023 - December 8, 2023

Purpose of Work:

Despite decades of digital platforms monetizing user data that is collected for other purposes, consumers still lack choice and control over the personal information they provide to companies. The U.S. lacks clear standards that dictate acceptable data collection and use, leaving companies' data practices largely unmitigated and consumers in the dark about how their information is used.

Companies take advantage of the current notice-and-choice-based privacy paradigm, in which they can ask for and use the information they want as long as they receive consent. As a result, digital platforms grow by burdening consumers to read lengthy privacy disclosures and provide informed consent, rather than taking responsibility themselves to determine a business model that is not reliant on rampant and unnecessary data collection. Once digital platforms amass data, it becomes easier to grow, feeding a positive feedback loop of data-based dominance.

Tech companies collect data that may go beyond the bounds of what is reasonable and necessary to provide their core product or service because they can, and it benefits them to do so. Reasonable data uses are up to the company's discretion.

While California, Colorado, and other states have passed privacy laws, comprehensive federal privacy legislation is imperative to curtail digital platforms' widespread data abuses and to protect consumers everywhere, not just in certain states.

Public Knowledge (PK) works toward protecting consumers' privacy by advocating for data minimization, meaningful consent, and effective user privacy controls. Consumers should have the right to access the information a company has about them and to correct, delete, and move that information across platforms. PK supports a comprehensive federal privacy law that allows for states to expand on those baseline protections and ensures a private right of action so that consumers can act when others cannot on their behalf. PK also believes that agencies must be entrusted with broad rulemaking authority to regulate different types of digital platforms and harms that may arise as technology evolves. Going a step further, PK advocates for a regulatory agency with the expertise and the tools to address the problems posed by big platforms, including privacy, should be created. PK created a proposal for such an agency in 2019.

Projects & Outcomes:

Privacy & Congress

PK joined a group of 87 public interest organizations in a letter to Congressional members urging action to ensure AI safety and accountability. The letter highlighted how unchecked use of Americans' information to build Large Language Models threatens privacy.

PK published a blog post from Government Affairs Director Sara Collins, "*The Battle for Control: TikTok, Parental Consent, and the Rights of Children*," which discusses legislation aimed at protecting children's safety online.

PK is continuing to push for the reintroduction of the American Data Privacy and Protection Act (ADPPA). In November, PK President and CEO Chris Lewis testified in the U.S. Senate's AI insight Forum #4, focused on privacy and liability. There he contributed to a broad consensus calling for a comprehensive privacy bill like the ADPPA that would reduce the privacy harms of AI significantly. PK staff has also covered two more Congressional hearings on the topic of privacy, intended to build momentum towards moving quality privacy legislation.

Privacy & Federal Agencies

PK submitted comments to the Bureau of Consumer Financial Protection on the need for consumer protections from data brokers and other business practices that handle consumer information.

PK submitted comments to the US Copyright Office's Request for Information on Artificial Intelligence that highlighted policy solutions for concerns related to generative AI, including privacy protections.

PK submitted comments to the President's Council of Advisors on Science and Technology on safety measures for the development and deployment of generative AI. The comments call for incorporating principles like transparency, privacy and security, and equity and inclusion.

PK submitted comments in response to the Office of Science and Technology Policy's request for information on national priorities for artificial intelligence. The comments called for comprehensive privacy legislation.

PK submitted comments in response to the National Telecommunications and Information Administration's Request for Comment on policies on AI accountability. The comments explained how establishing a sector-specific digital regulator and comprehensive privacy law are necessary steps for a healthier AI environment and better preparedness for the future.

PK published a factsheet about how Title II empowers the FCC to establish and enforce strict privacy protections as well as ensure that consumers have a solid recourse for privacy violations.

Events and Outreach

PK staff worked to organize over 400 public interest participants into an AI Big Tent virtual gathering. In partnership with Public Citizen, The Leadership Conference on Civil and Human Rights, AFL-CIO, and Center for American Progress, PK guided this Big Tent of progressive activists through the policy themes and implications of AI, including privacy, as well as the ways to participate in the policy process in the months to come.

PK published three relevant blog posts on generative AI during this time period. "*Hey, That's My Voice! – The Significance of the Right of Publicity in the Age of Generative AI*" discusses how a right of publicity for generative AI could prevent unauthorized use of identity that could lead to false endorsements, misrepresentations, or infringements on their privacy. "*Lies, Damn Lies, and Generative Artificial Intelligence: How GAI Automates Disinformation and What We Should Do About It*" and "*AI Policy and the Uncanny Valley Freakout*" discuss regulatory solutions for generative AI's risks, including privacy. As a result of her writing on the topic, Senior Policy Analyst Lisa Macpherson was asked to be a speaker about generative AI and elections at the annual retreat of the States United Democracy Center, and to be on a panel, "Getting Serious About AI," at the Georgetown Law Summit on Emerging Technology Policy, presented by the Institute for Technology Law & Policy.

PK organizes the Movement for a Better Internet, an initiative co-led by PK that unites passionate advocates, activists, and organizations across the globe who seek to create an internet shaped by public interest values. During this time period, PK published the Movement's first community output: a report from a members-facilitated workshop at the MozFest conference on generative AI opportunities, concerns, and solutions.

Future Plans:

During this time period, PK began planning an in-person convening called Knowledge Exchange, as well as two virtual convenings leading up to it, to take place in early 2024. Its format is intended to build strategic, intergenerational bridges between the youth organizing advocates for privacy and kids safety with PK's traditional digital rights community of policy experts.

PK will also be continuing our regulatory work on privacy. We expect that the Federal Trade Commission's Commercial Surveillance rulemaking, which will include hearings and more opportunities for comments. The White House's Executive Order on AI included significant privacy protections, which will need to be implemented by a variety of agencies like the National Telecommunications and Information Administration and the National Institute of Standards and Technology. This implementation process will create another set of opportunities for comments and advocacy.

PK is in the process of hosting a series of listening sessions related to its digital regulator proposal. The sessions aim to build consensus among civil society groups, and to inform a multi-day convening PK will host in 2024. The convening will explore how a digital regulator should function.

Our cy pres award will help fund these events, as well as our annual conference on Emerging Technologies in May. This conference explores policy implications (including privacy policy) related to the growth of AI, virtual and augmented reality, and decentralized web technologies.

Key Staff:

- Michele Ambadiang, Events & Development Manager
- John Bergmayer, Legal Director
- Sara Collins, Government Affairs Director, PK Lead on Privacy
- Harold Feld, Senior Vice President
- Nick Garcia, Policy Council
- Chris Lewis, President & CEO
- Lisa Macpherson, Senior Policy Analyst
- Will McBride, Digital Content Manager
- Meredith Rose, Senior Policy Counsel
- Charlotte Slaiman, Vice President
- Shiva Stella, Communications Director

Public Knowledge
Statement of Activity

December 2022 - October 2023

	2900 - Privacy
Revenue	
Total Revenue	**$ 1,006,582.88**
Gross Profit	**$ 1,006,582.88**
Expenditures	
5001 Salaries and Benefits	
5000 Salaries	79,531.19
Total 5001 Salaries and Benefits	**$ 79,531.19**
Total 5469 Travel & Meetings	**$ 1,584.31**
Total Expenditures	**$ 81,115.50**
Net Operating Revenue	**$ 925,467.38**
Other Expenditures	
9000 Overhead Allocation	28,234.20
Total Other Expenditures	**$ 28,234.20**
Net Other Revenue	**-$ 28,234.20**
Net Revenue	**$ 897,233.18**

EXHIBIT F

CR Consumer Reports™

Advancing Consumer Privacy and Security
Report for Cy Pres Award
No. 5:10-md-02184 JW
December 2023

Summary

As an independent, nonprofit member organization committed to a fair and just marketplace for all, Consumer Reports (CR) is working to ensure pro-consumer ground rules in the digital marketplace. Our strategy integrates CR's historic strengths—in research, testing, and ratings; advocacy and mobilization; and journalism and communications—with new tools that meet consumers' needs while shaping the marketplace in their favor. CR's tools include Permission Slip, our free mobile app that empowers individuals to send companies legally enforceable requests to delete or stop selling their data, and Security Planner, our guide that provides consumers with personalized recommendations on how they can improve their data privacy and security. Working in collaboration with privacy allies, we coordinate Global Privacy Control, a browser signal that informs websites of a user's privacy preferences. We are also helping to develop a framework for a national security and privacy labeling system or trustmark to help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks.

In the last six months, we have participated in two White House events, shaped numerous state privacy related bills, educated and engaged hundreds of thousands of consumers about privacy, and secured more than 100,000 users for Permission Slip in less than ten days from the app's launch. We published important information about privacy and product reviews, presented our research findings and policy recommendations in multiple venues, and have been frequently cited in the press.

As of the end of November, we have spent $195,000 of the award on personnel costs. We anticipate that we will exhaust the funds by July 2024 as the spending rate will increase significantly starting in December when we expand the number of positions partially offset by the award. All of the positions work directly on our digital privacy agenda including policy, consumer education and engagement, testing and research, and product development for Permission Slip and Security Planner.

Research and Testing

Our testing team has conducted tests on multiple product categories including robotic vacuums, home security camera, televisions, password managers, and banking apps. We discovered 12 privacy and security vulnerabilities in televisions and eight vulnerabilities in the robotic vacuum and home security cameras categories. As a matter of practice, CR contacts companies when we discover any vulnerabilities or safety concerns. Two manufacturers—one of baby monitors, the other of wireless routers— fixed security vulnerabilities previous CR testing had identified.

Advocacy and Mobilization

To secure pro-consumer ground rules in the digital marketplace, we work across a variety of issues and forums.

In July, CR met with the chief technologists of the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) to brief them on CR's policy priorities and to urge regulators to more aggressively rein in the data brokers that sell consumers' personal information.

In August, CR was invited to present on how to mitigate data broker harms at a roundtable discussion at the White House. We focused on how the FTC should use its existing rulemaking to institute a data minimization requirement. We also highlighted several bills in states like California and Massachusetts that would address some of the harms of data brokers, and shared how state laws that allow for authorized agents (legally recognized intermediaries) can help users manage their privacy to exercise data rights. (CR’s Permission Slip app functions as an authorized agent). Senior officials from the White House, FTC, Justice Department, and other agencies were on hand, and the head of the CFPB announced the Bureau’s proposal for new rules for data brokers.

In August, we filed comments in response to the FTC's notice of proposed rulemaking to update its Health Breach Notification Rule. CR largely supports the FTC's proposals to expand the reach of the rule. The proposals would ensure that most health and wellness apps not otherwise covered by Health Insurance Portability and Accountability Act (HIPAA) that collect personally identifiable health information would be responsible for providing breach notices when they share information with unauthorized third-parties.

We also participated in a July White House event announcing the creation of a new cybersecurity labeling initiative overseen by the Federal Communications Commission (FCC). Like an Energy Star label for cybersecurity, the program would create a trust mark that companies can display on IoT products that meet certain key security benchmarks for security, privacy, and transparency. CR was the sole consumer advocate invited to the event that included executives from companies such as Amazon, Samsung, LG, and Google. The National Security Council and National Institute of Standards and Technology convened the event which provided a platform for CR to deliver remarks and demonstrate our own prototype cybersecurity labeling program. CR was quoted in stories by Associated Press, Washington Post, Vox, and other media. In October, we filed detailed comments with the FCC in support of the proposed labeling program. We offered recommendations on important elements that companies should have to commit to, including a minimum device support period and a robust vulnerability disclosure program.

State Advocacy

While we aspire to secure a robust federal consumer privacy law, we recognize that it is unlikely in the near term. Consequently, CR works to advance pro-consumer policy at the state level. Highlights from the last six months include:

- **California**:
  - CR testified in Sacramento, submitted letters, and lobbied in support of California's "Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE Act). This Act, signed into law by Governor Newsom in October 2023, will make it easier for consumers to control their data. It allows consumers to delete their information from all of the state's more than 500 registered data brokers with a single click. The DELETE Act is the first law in the nation to allow consumers to request universal deletion of their data.
  - In April of this year, CR testified about a bill in the California Senate designed to protect data provided to fertility and sexual health apps (AB 254). The bill's author cited CR's research into period tracker apps as a rationale for the bill. It

passed in the California Senate with a 40-0 vote and headed back to the Assembly where a similar version has already passed.

- **Colorado**: Colorado has a new privacy law that says consumers may use universal tools to opt out of data sales and targeted advertising. CR submitted an application to urge the state to certify Global Privacy Control in its registry of recognized opt-out tools. Several privacy groups joined CR in support of our application, which was one of the three provisionally accepted.
- **Delaware**: The governor of Delaware signed a comprehensive privacy bill (H.B. 154) that includes several measures advocated by CR, including provisions for universal opt-outs and authorized agents. During testimony in support of the bill, the Delaware Attorney General repeatedly noted that authorized agents, like CR's Permission Slip, make this bill's provisions more workable. We commended lawmakers for advancing the bill, and recommended ways to close loopholes and strengthen the legislation.
- **Florida**: We made recommendations to improve Florida's new privacy law. NewsNation and The Record shared CR's perspectives about the law.
- **Maine**: CR submitted written testimony and testified to the Maine Judiciary Committee on three privacy bills we support (comprehensive, biometric privacy, and health privacy). The comprehensive bill would institute strong data minimization provisions, while the biometric bill would require affirmative opt-in consent before biometric information is sold or shared, and the health privacy bill would ban the sale of health information outright. The state's Joint Judiciary Committee asked us to provide expert testimony about the concept of data minimization.
- **Massachusetts**: CR testified at a legislative hearing before the Massachusetts state legislature's Joint Committee on Advanced Information Technology, the Internet and Cybersecurity in support of a comprehensive data privacy and protection bill. If enacted as drafted, this would be the strongest state privacy law yet.
- Montana: CR's detailed critique of an initial version of Montana's privacy bill prompted the bill's Republican sponsor, Sen. Daniel Zolnikov, to champion amendments including universal opt-out requirements and allowing the state attorney general to immediately begin assessing fines and other penalties for violating the law starting in April 2026., and the Montana Consumer Data Privacy Act (MTCDPA) SB 384 passed with unanimous bipartisan support in both chambers and came into effect on October 24, 2024. (An article in Politico details CR's role.

- **New Hampshire**: CR testified before the New Hampshire Senate Judiciary Committee about the state's consumer privacy legislation. We urged the committee to consider how it could improve the legislation by lowering the threshold for coverage, adding data minimization provisions, and strengthening the enforcement mechanism.
- **New Jersey**: CR met with New Jersey state legislators sponsoring a privacy bill we consider as weak. We also shared concerns with legislative leaders and the Attorney General's office. We alerted ACLU-NJ who joined our efforts to press lawmakers to halt their consideration of the bill. State legislators dropped consideration of the bill.
- **Oregon**: The Oregon state legislature approved a CR-endorsed privacy bill that provides more protections than many of the industry-backed measures in other states this year. Our advocates worked with lawmakers and the Attorney General's office throughout the process to strengthen the bill.
- **Pennsylvania**: CR wrote Pennsylvania lawmakers to recommend improvement to a consumer privacy bill (H.B. 1201) under consideration. We highlighted the pro-consumer provisions in the bill, while pointing out the significant loopholes that would hinder its overall effectiveness. Our recommendations include broadening the opt-out rights to include all data sharing and ensuring targeted advertising is adequately covered.
- **Texas**: CR urged lawmakers in Texas to strengthen the recently signed privacy law. While the signed bill as not as strong as we would like, we were able to secure improvements into the final, signed bill.
- **Wisconsin**: CR submitted comments to Wisconsin state lawmakers on the pros and cons of their proposed privacy bill, with suggestions to strengthen it, including adding a private right of action, expanding the definition of sale, and banning price discrimination.

Mobilization

When a new congressional report revealed that three of the leading online tax prep companies have been sharing sensitive consumer data—including tax return dollar amounts, gross income, and the names of dependent children—with Facebook and Google for years, CR responded with a petition calling on the FTC, IRS, and Justice Department to investigate H&R Block, TaxAct, and TaxSlayer, and hold them accountable. In just three days, the petition secured 27,000 signatures. We directed consumers who signed to a new research project we are conducting to determine which companies are sharing users' personal data with Facebook. More than 1,000 new participants joined the project.

In November, CR hosted a webinar with Common Sense Media, Staying Safe Online - Security Planner to help families protect themselves online. During the event, the CR team walked through the Security Planner Tool and shared articles about determining whether you need a VPN, removing your information from people search sites, choosing a password manager, and addressing stalkerware. More than 1600 consumers RSVPed for the event with more than 450 attending the live stream.

Journalism & Communications

We shared our insights with consumers, rulemakers, industry, and privacy allies through a variety of strategies. Our reporting includes solutions journalism—stories that identify issues and suggest evidence-based solutions—as well as the product ratings and reviews for which we are well-known. We published reports, placed op-eds in a variety of publications, responded to reporters' questions, and presented at conferences and other events. Highlights from the last six months include:

Solutions Journalism

- How to Turn Off Smart TV Snooping Features, All smart TVs—from Samsung, LG, you name it—collect personal data. These TV privacy settings limit what manufacturers learn.
- How to Take Back Control of Online Data With Apps Like Consumer Reports' Permission Slip
- What You Say to Google Assistant and Alexa (but Not Siri) Gets Used for Ad Targeting. Here's How.
- Car Insurance Quote Comparison Websites Save You Time, But Watch for Privacy Pitfalls
- Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price? (Updated)
- The Consumer Reports Scam Protection Guide
- Take Control of Tech Clutter, Get rid of old electronics, make space on your phone and computer, manage your passwords and email inbox, and more

Product Review Articles (behind our paywall) include:

- Best 75-Inch TVs of 2023
- Best Wireless Home Security Cameras of 2023
- Best Video Doorbell Cameras of 2023
- Best Video Doorbell Cameras Without a Subscription
- Best Password Managers of 2023
- Best Mesh Routers of 2023
- Best Baby Monitors of 2023

Op-Eds

- Cal Matters published (and Mercury News republished) our piece, California took a major step to boost privacy laws and crackdown on data brokers detailing how data broker business practices can harm consumers, and how the California DELETE Act will make it easier for consumers to control their data.
- The Messenger published our op-ed, An FCC Label Will Improve Trust in Connected Devices and Our Collective Cybersecurity, about how the FCC's plans for cybersecurity labeling program has the potential to give consumers, retailers, and manufacturers the tools to keep the devices secure over time. They also published, An FCC Label Will Improve Trust in Connected Devices and Our Collective Cybersecurity,
- The Hill published our piece about the FTC's historic lawsuit against Amazon for anticompetitive business practices, and how this could lead to a better online marketplace for consumers.
- Indiana Capital Chronicle published a CR op-ed about how the state's new consumer privacy law is not "road ready."

References to our work

- The Record spoke with CR about the health data privacy law passed in Washington state.
- San Francisco's KQED Public Radio spoke with CR about Meta asking European users for permission before targeting them with advertisements.
- CR spoke with Pluribus and The Record about data brokers and the DELETE Act, noting that data brokers are "some of the most opaque but impactful collectors of information that exist and they've been largely unregulated."

- A Los Angeles Times op-ed, The misuse of personal data is everywhere. Here's one measure that fights back in support of the Delete Act that mentions CR and Permission Slip, and how the app can make opting out of information sharing easier. The author notes that data brokers have been crafty in finding excuses not to comply with privacy requests and rules.
- CyberScoop spoke with CR for its podcast Safe Mode to discuss what data brokers are and how to delete your data from people search sites.
- Seattle Times asked CR about the FTC's investigations and penalties aimed at two of the city's biggest employers—Amazon and Microsoft—for failing to protect consumers' data, including from users under the age of 13. CR noted that, while the child online privacy law, the Children's Online Privacy Protection Act (COPPA), has been in place for decades, the interest in children's digital safety has increased in the past year, following allegations by a Facebook whistleblower that the company prioritized profits over safety on its platform.
- Tall Poppy spoke to CR for a blog that urges people to send comments to the CFPB in response to its request for feedback about the data broker industry. We covered Security Planner, people search sites, how to reduce risk of identity theft, and other topics.
- Montana Free Press spoke with CR for a story about the state's approval of new data privacy laws, despite industry opposition. The reporter credits CR with helping develop one of the laws, which provides a number of digital privacy protections for Montana consumers.
- Politico also published a detailed story on how lobbyists shaped Montana's new privacy law. The story credits CR for pushing back against industry efforts and for convincing policymakers to include several provisions to strengthen the bill.
- CBS News Radio asked CR about the privacy issues presented by today's internet-connected cars. CR supports the use of technologies such as distracted driver monitoring systems, and at the same time, we want protections in place to limit data collection and sharing for other purposes, such as marketing.
- Pluribus interviewed CR about state privacy law making activity in 2023. The piece, which included a link to our model privacy bill, highlighted our advocacy work and our view that many of the latest state privacy laws should go much further to protect consumers.
- USA Today recommended that people "try Consumer Reports Security Planner" in a story about Apple's emergency patch to fix a serious security flaw for iPhones and iPads.

Presentations

- CR moderated a panel at Def Con, the annual hacker convention. The panel focused on the federal government's Secure by Design work. Panelists included officials from the Cybersecurity and Infrastructure Security Agency (CISA) and the White House Office of the National Cyber Director (ONCD). Following the panel, attendees marked up a draft of CISA's latest guidance on Secure by Design, and offered edits, comments, and suggestions to inform the final version of the guidance.
- CR was invited to discuss memory safety—a property of some programming languages that prevents programmers from introducing certain types of bugs related to how memory is used— in a meeting with the CSIA's interagency working group. The group coordinates federal research and development to protect information and information systems from cyber threats. We briefed the group on the current state of memory safety issues in computing and prospective ways forward for the next federal cybersecurity R&D strategic plan. The group's members are technical program managers and directors responsible for overseeing the research activities for a wide range of federal agencies, including the National Science Foundation and the Department of Homeland Security.
- CR and the Atlantic Council hosted a workshop on how to implement the FCC's labeling program. Attendees included CISA, Carnegie Mellon, NSA, Cisco, Google, Microsoft, Silicon Labs, Home Depot, and the Cyber Statecraft Initiative.
- CR hosted two sessions at RightsCon, which focuses on human rights in the digital age. We moderated a workshop on what can be done to improve privacy and security knowledge so people can engage online safely, and we shared a case study of our Security Planner tool. We also screened our video series on algorithmic bias, Bad Input, and held a discussion on how biases in algorithms and data sets result in unfair practices towards people—often without them knowing—through a lens of racial equity.
- CR spoke about privacy laws and the latest updates on regulation at a Bloomberg Government webinar, as well as a Practicing Law Institute seminar on Communications Law in the Digital Age.
- CR spoke about cybersecurity for journalists and journalism educators at a gathering of international scholars participating in the Study of the United States Institutes (SUSI) Scholars initiative at Arizona State University. It's part of a six-week Institute on

Journalism, Technology, and Democracy sponsored by the Walter Cronkite School of Journalism and Mass Communication and ASU's Global Security Initiative. The discussion included our Security Planner tool and our VPN research.

- CR participated in a panel for the nonprofit Free Press entitled "When Privacy is Not the Policy: What's Next for Data Privacy & Consumer Rights." We highlighted how Permission Slip helps fill a gap in many state privacy laws that otherwise require individuals to opt out individually from each of the businesses with which they interact. We reiterated the need for Congress to pass a national privacy law with strong data minimization provisions. The event featured keynote remarks from U.S. Senator Ed Markey.

Reports

As part of Cybersecurity Awareness Month in October, CR published our second annual report on cybersecurity in collaboration with Aspen Digital and Global Cyber Alliance. The report reveals continued progress in consumer cybersecurity practices through the adoption of data and privacy practices, awareness of security tools, and improved posture online. It highlights findings from a nationally representative CR survey and perspectives from leaders in government, industry, and civil society and underscores the importance of more consumer education to ensure people are taking the proper steps to protect their digital safety.

Tools

Permission Slip

In October, CR officially launched our free data privacy app Permission Slip, which helps consumers take back control over their personal data. Users discover what kind of data companies collect and can send those companies legally enforceable requests to delete or stop selling their data. Available on both iOS and Android, Permission Slip secured more than 100,000 active accounts and one million data deletion requests within the first 10 days of the launch. The app is currently rated 4.7 in the Play Store (Google) and 4.6 in the App Store (Apple).

Permission Slip has garnered significant media coverage. From October 3 - 20th, there were 47 unique stories that led to 240 syndicated stories for an estimated audience of almost 400 million. This includes articles in the Washington Post, Delete your digital history from dozens of companies with this app; Gizmodo, Think You're Too Lazy to Protect Your Privacy? Try the Permission Slip App (also available in Spanish); the New York Post, How to defend your digital footprint in one tap with free 'Permission Slip' app; and CNET, Here's What to Need to Know About Permission Slip, the App That Can Help Protect Your Online Data. Coverage has continued beyond October 20th including an article in Forbes, "With Its New Permission Slip App, Consumer Reports Aims To Make Online Privacy More Accessible To Every Person."

In November, 2023, *Fast Company* named Consumer Reports a winner in the Nonprofit and Academic Institutions category for *Fast Company's* 2023 Next Big Things in Tech Awards to celebrate our innovative application of cutting-edge technology to solve a real-world problem.

Global Privacy Control (GPC)

GPC is a browser signal to inform websites of a user's privacy preferences. CR's Justin Brookman, Director, Consumer Privacy and Technology, chairs the group of collaborating organizations that developed and launched the tool. With more than 75 million active users, GPC is legally recognized by California as a valid opt-out mechanism and Colorado has conditionally approved GPC as a binding mechanism. We anticipate that several other states will likely follow. Mozilla recently announced it would include the Global Privacy Control in settings for Firefox users, starting with version 120. CR has asked Apple to implement some minor changes to their privacy settings, including implementation of the Global Privacy Control. CR and Apple have had extensive discussions around GPC and the company's settings. Apple has previously made changes to accommodate GPC.

EXHIBIT G

ROSE
FOUNDATION
FOR COMMUNITIES &
THE ENVIRONMENT

201 4TH STREET, SUITE 102
OAKLAND, CALIFORNIA 94607
TELEPHONE 510.658.0702

December 8, 2023

Honorable Charles R. Breyer
U.S. District Court Judge, Northern District of California
450 Golden Gate Avenue, Courtroom 6 – 17th Floor
San Francisco, CA 94102

Status Report: In Re Google Streetview Electronic Communications Litigation *Cy pres* Administration

Dear Judge Breyer:

In November 2022, the Rose Foundation for Communities and the Environment was approved as a recipient for the In Re Google Streetview Electronic Communications Litigation (Google Streetview) *cy pres*. This report provides the results of the Consumer Privacy Protection Fund grant cycle that was recently executed.

As previously reported to this Court in June 2023, we planned for a Fall 2023 funding opportunity, and we have just successfully exhausted the Goggle Streetview *cy pres* funds. Starting in August 2023, we conducted extensive outreach and publicized the grant opportunity to privacy groups nationwide. We then convened a funding board of privacy experts to assist us with our review and assessment of the proposals received. Overall, we received 45 applications with requests totaling $5.3 million for the available $936,122 in funding.

After extensive review, 11 organizations were recommended to receive funding, and the Rose Board of Directors has recently approved a docket of grants ranging from $5,000 to $150,000. We are currently in the process of executing contracts with these grantees whose projects will begin in 2024. The organization’s name, project name (italicized), and grant amount are set forth below along with a short summary of the grant project.

We were honored to have the opportunity to serve the Google Streetview class with the Consumer Privacy Protection Fund, and we are happy to provide any additional details on grantmaking as needed.

Sincerely,

Jodene Isaacs

Jodene Isaacs
Mitigation Funds Director
The Rose Foundation for Communities and the Environment

#

In Re Google Streetview Electronic Communications Litigation *cy pres*
Grant Docket - Rose Foundation for Communities and the Environment
11 grants totaling $936,122

Fairplay
Protecting Young People's Privacy in the Metaverse
$75,000

Protecting Young People's Privacy in the Metaverse project will determine whether existing federal privacy and consumer protection laws can effectively ensure young people's privacy rights in virtual reality (VR) environments. Fairplay will use this grant to conduct original research to identify privacy risks to minors on VR apps for Meta's Quest 3 headset and analyze whether the privacy policies and practices of Meta and the VR app developers violate the Children's Online Privacy Protection Act or Section V of the FTC Act. If the group's analysis finds violations of existing law, they will file a Request for Investigation of Meta and/or VR app developers. Should existing laws be deemed insufficient to adequately protect children and teens from the unique privacy threats of VR environments, the group will draft model legislation and share it with federal lawmakers for consideration. In addition to these tasks, Fairplay will educate consumers about the privacy risks for young people through either media coverage of the anticipated FTC complaint or by releasing a report to accompany model legislation.

Fight for the Future Education Fund
Stopping the spread of consumer biometric surveillance
$75,000

Fight for the Future Education Fund (FFEF) has long been advocating against broad biometric surveillance and campaigning to stop its current spread and future adoption. Biometric tech, including facial recognition technology, palm scanning, and emotional Artificial Intelligence (AI), is unlike any other form of surveillance. Its automated monitoring of entire populations is nearly impossible to avoid or opt-out of, and its chilling effect on autonomy and privacy includes such harms as: invasive tracking of consumer behavior; infringement on freedom of movement, protest, and speech; discriminatory misidentification of Black and brown people; and unwarranted use by law enforcement. It also creates myriad chances for data breaches and unauthorized data collecting, sharing, and selling. FFEF will use this grant to focus on schools, where biometric tech, particularly facial recognition technology is rapidly spreading, and where use of this tech disproportionately affects vulnerable communities, including children of color. The group will educate administrators, parents, teachers, children's rights groups about the ways in which surveillance technologies such as those increasingly being used to monitor attendance and as "anti-cheating" e-proctoring software are proliferating. FFEF will also mobilize these key constituents to help stop their spread and educate the larger public about the increasing use of biometric surveillance at sports and live events, travel and retail establishments, as well as by the auto industry.

InvestigateWest
Abortion, Consumer Data Privacy, and Law Enforcement Access in Idaho
$15,245

InvestigateWest will use this funding to produce a long-form investigative article exposing the potential dangers of personal data (such as web browsing history, health records, financial records, geolocation information, and electronic communications) being exposed to law enforcement officials in Idaho who could seek such information to shed light on an individual's abortion decision. In a state with one of the most restrictive abortion laws in the country, activists are concerned agencies could collect this information without the consumer's knowledge. The Fourth Amendment generally requires law enforcement officials to obtain a warrant before collecting personal data, but this requirement typically does not apply when the information is held by a third party to whom the data has been shared or sold. Further, federal data privacy law provides relatively limited constraints upon law enforcement's ability to acquire privacy data relating to criminal activity, potentially including abortion activity proscribed under the state laws. The purpose of the article will be to raise awareness of how this may be playing out in Idaho in particular, and more broadly, to help inform lawmakers of the need for new laws that would specifically address the treatment and disclosure of abortion-related data.

Just Futures Law
Centering Immigrants' Rights and Racial Justice in the Consumer Rights Sector
$150,000

Just Futures Law (JLF) seeks to transform how litigation and legal support serves communities and builds movement power. The group works to combat the sprawling systems of surveillance and mass deportation through movement lawyering through local, state, and federal advocacy campaigns. Led by women of color and 100% female founded, JFL staff are experienced legal strategists who have decades of experience in legal advocacy and litigation. Just Futures will use the grant to complete two short term projects to support privacy enforcement and advocacy in the areas of artificial intelligence (AI) and data broker surveillance and technologies, both of which implicate privacy, consumer rights, immigrants' rights, and human rights. First, Just Futures will produce legal and advocacy memos related to the viability of interventions in AI uses in immigration enforcement and policing. On databroker surveillance, the group will continue its successful federal, local, and state advocacy campaigns to uplift the role that commercial and personal data have in immigration enforcement and limit the sale, transfer, or sale of such data. The group will also provide support for policies currently under development in Illinois. By demonstrating proof of harm to immigrant communities, this project will help generate new tactics in litigation and policy to tackle the abusive use of AI. The group aims to advance a pro-immigrant and pro-privacy narrative that can be used to educate the public and needed policy stakeholders.

Library Freedom Project, Inc.
Popular privacy education through libraries with Library Freedom Project
$146,000

Library Freedom will use this grant to expand their work through the creation of a new Privacy Advocacy intensive training for librarians and the development of new resources. The group's previous intensives–Library Freedom Institute and LFP Crash Courses–were enormously successful and turned dozens of librarians into privacy experts in their communities. Training librarians on privacy issues allows this information to both efficiently and effectively reach communities across the country. The group will develop new resources for in-person trainings and expand their standalone online trainings to reach an even wider audience. These educational materials aim to support librarians-as-trainers and the diverse publics they serve on how everyday people are impacted by the loss of privacy. This grant will have a multiplier effect on the group's current work, engaging librarians to promote privacy advocacy and education in communities nationwide. The grant will also allow the group to identify gaps in current educational materials and needed content for improvement, and Library Freedom will hold an annual weekend-long summer retreat which gives their librarian members an opportunity to meet, share strategies, resources, and successes.

Oakland Privacy
Enhancing Regional Privacy Rights Infrastructure - Privacy Rights Fellowship
$50,000

Oakland Privacy, a largely volunteer run organization, will use the funding to support two Privacy Rights Fellows to build out the organization's capacity on crucial fronts. Overall, the group will focus on the growing artificial intelligence debate, continue educating people about the lack of transparency associated with the Chrome browser's privacy controls, and offer digital security and online safety resources to the public. In particular, the fellows will oversee and submit comprehensive comments to the California Privacy Protection Agency in their ongoing artificial intelligence and algorithmic decision-making rulemaking. The fellows are expected to suggest enhancements for proposed rules, parameters for future rulemakings, and will expose industry pushback. They will also track and guide responses to state-level legislation expected to be introduced in 2024 and develop targeted model legislation focusing on impact auditing, algorithmic transparency, and complaint/appeal processes. These model policies will be used to educate local city and county municipalities in Northern California on how local regulations can be used to strengthen individual privacy rights. Finally, the fellows will create a comprehensive advocacy guide to spread the message that smart consumers should not use the Chrome browser due to its being compromised and under-protective of individual's privacy.

Stop LAPD Spying Coalition
Fighting Social Media Surveillance, Youth Data, & Political Targeting
$75,000

The Stop LAPD Spying Coalition is a community group based in the Skid Row neighborhood of downtown Los Angeles. Founded in 2011, the group has been researching, exposing, and organizing as part of broader movement-building to abolish police spying and infiltration. For years, Stop LAPD Spying has mobilized around the concept of 'datafication' i.e. the non-consensual collection of information about communities, which is then used to control or commodify populations. The group is most concerned with the fact that police both generate and gather data about local communities that is repurposed for profit. Individual's relationships, communication, movements, and biographies are reduced to data points that are collected and shared by the police, who have become the largest data brokers. With this grant, the group will grow their work by addressing surveillance and data gathering in several key areas. First, the group will focus on identifying partnerships between social media corporations, law enforcement agencies, and third-party social media surveillance software companies. They will also intensify organizing efforts against a youth surveillance app known as "Los Angeles Schools Anonymous Reporting" (LASAR) which collects data on Los Angeles students. In addition, Stop LAPD Spying is committed to expanding its efforts in highlighting LAPD's suppression of protests. The group will hold monthly meetings to inform local residents and empower them to advocate on all of these issues.

Taraaz
Protecting Privacy and Civil Rights Through Responsible Municipal AI Procurement
$75,000

Taraaz is a research and advocacy non-profit dedicated to advocating for human rights in the digital age by conducting human rights impact assessments, developing educational tools, and advocating for responsible tech policy. Through successful a campaign and coalition building, the group was able to help ban the use of predictive policing technology that led to discrimination against marginalized communities in Santa Cruz County. This project will develop educational resources and hands-on engagement to help municipal policymakers responsibly procure AI technology to protect constituents' privacy and provide equitable access to public services. Through extensive literature review and interviews with municipal policymakers and civil society experts, the group will evaluate various AI vendors that sell software to municipalities and create tailored guides for vetting vendors, structuring contracts, and implementing oversight to prevent discrimination, inequity, and surveillance. After creating educational resources, the group will organize a workshop, in partnership with the National League of Cities, to provide hands-on experience to 45+ municipal officers to apply these guides to real-world municipal AI procurement scenarios. This project aims to empower municipal policymakers and officers with practical tools to embed consumer privacy rights, surveillance, and equitable access in public sector AI adoption.

The Regents of the University of California - UC Berkeley Center for Economic Justice
Protecting Consumers from Harmful Technologies Through Advocacy Networks
$148,000

The Berkeley Center for Consumer Law & Economic Justice is the nation's leading academic center dedicated to building the field of consumer law. The Center works to create economic justice by developing policies that prevent fraud and deception, protect low-income communities and communities of color, and promote financial security and empowerment. The Center will use this grant to activate the Economic Justice Policy Advocacy Conference (EJPAC) and Consumer Law Advocates, Scholars & Students (CLASS) networks—nationwide teams that it launched and co-directs—to address urgent threats to the privacy and economic security of low-income consumers from emerging technologies. The grant will enable the Center to hire for the first time a Policy Director who will transform EJPAC from a periodic convening into a standing active coalition of policy advocates focused on issues of privacy, technology, and economic justice. The Director will also galvanize the student and professorial resources of the CLASS network to design, refine, promulgate, and implement new legislative and regulatory initiatives. The Center will facilitate cutting-edge policy research, engage in regulatory advocacy, and use the courts to protect and implement policy victories to address consumer privacy from a consumer/economic justice focus, in contrast to other organizations that tend to approach the issue from technocentric or democracy/human rights perspectives.

United States Public Interest Research Group Education Fund
Don't Sell My Data Campaign
$125,000

Since 1984, U.S. PIRG Education Fund has used research, public education, advocacy, and litigation to achieve dozens of milestones for consumer protection and support organizations committed to a strategic approach to social change. U.S. PIRG Education Fund's Don't Sell My Data campaign will build upon PIRG's historical work in the privacy space, and the organization will continue fighting for consumer internet privacy rights. In partnership with state PIRG groups, U.S. PIRG will launch a state lawmaker and consumer education project, creating and releasing a state privacy law scorecard, holding a national briefing for state lawmakers on how to protect consumers' data privacy online, and disseminating state-specific tips guides for consumers on how to exercise their rights. The group will also support the CFPB in its Fair Credit Reporting Act rulemaking and continue work to identify and uplift emerging Gen Z privacy leaders on campuses. The goal of this work is to both arm lawmakers with information about what effective consumer privacy protections look like as well as to empower consumers in states with laws to use their rights. Informed and motivated consumers are a powerful force when given the right tools. Empowering consumers in states with privacy laws to use their right to access & delete data will not only help individual consumers, including youth and families, better protect themselves, this will send the marketplace a signal that the public is becoming less tolerant of abusive data practices.

Youth For Privacy
General Support
$3,123*

The Youth Privacy Ambassadors Program aims to empower a select group of young individuals to champion privacy rights in their communities and schools. This grant will support six ambassadors who will be chosen and will go through a several month-long training process, where they will learn the basics of privacy, in intersection with topics like disarmament and data values. At the end of the training, they'll be provided with both a mentor and a $500 mini-grant each to execute privacy-related projects (with preference toward creative and joint deliverables). The program will prioritize publicity and promotion, ensuring a wide reach for the call for ambassadors and the final virtual showcase event. Ambassadors will be recognized at

this event, celebrating their contributions. The project aligns with the organization's mission to foster a youth-led privacy-focused responsible internet through education and advocacy.
** A total grant of $5,000 was made to this group, with $3,123 coming from the Google Streetview cy pres and the remainder from another source.*

EXHIBIT H

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Funding Report for *Cy Pres* Funds From

In re: Google LLC Street View Electronic Communications Litigation

Electronic Privacy Information Center (EPIC)
Washington, DC

December 2023

CONTACT INFORMATION

Alan Butler, Executive Director and President
Caitriona Fitzgerald, Deputy Director and Policy Director

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Avenue NW
Washington, DC 20036
+1 202 483 1140 x103 (office)
butler@epic.org
fitzgerald@epic.org

DESCRIPTION OF THE ORGANIZATION

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit research and advocacy center in Washington, DC, that was established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. Over the last three decades, EPIC has led numerous campaigns to safeguard the privacy of Internet users in general and users of Google's services in particular. EPIC advocates for stronger Internet privacy protections through complaints to federal and state enforcement bodies including the Federal Trade Commission, the Federal Communications Commission, State Attorneys General, and others. EPIC also advocates for heightened protections for personal data in its friend of the court briefs in state and federal courts, through its testimony and statements in legislative proceedings, and in its reports and other educational publications.

As a recipient of *cy pres* funds in *In re Google Street View Electronic Communications Litigation*, 611 F. Supp. 3d 872 (N.D. Cal. 2020), EPIC has been able to continue its important work promoting the protection of Internet privacy. EPIC received disbursement of its award in the amount of $1,006,582.88 on December 7, 2022. This report covers the second six months of EPIC's activities funded in part by this award. EPIC's total organizational budget for 2023 is $3,218,000. We have allocated the *cy pres* award from *In re Google Street View* to support our work over the course of two years. This second six-month period represents use of 25 percent of the total award ($251,645.72).

EPIC's work to promote the protection of Internet privacy comprises several discrete sub-projects as well as other research, education, and advocacy work. We have specific sub-projects focused on Consumer Privacy Advocacy, Surveillance Oversight, AI & Human Rights, Communications Privacy, Platform Accountability, and more. With support from this *cy pres* award and other sources EPIC was able to make significant strides in its various program areas over the past six months. We advocated for comprehensive privacy rules to protect personal data online, pushed for a human rights-focused framework for the use of automated decision-making systems, worked to limit biometric surveillance by governments, and more.

In 2023 and beyond, much of our program activity will be focused on advocating for strong regulatory models for data governance and oversight that can preserve individual privacy and autonomy, protect against bias and discrimination, and promote healthy communication systems that support democratic institutions. EPIC will also be working to ensure that privacy rules are robustly enforced and that businesses comply with their data protection obligations.

CONSUMER PRIVACY ADVOCACY

Project Overview

EPIC is an expert voice for consumer privacy and is focused on shaping the future of privacy policy and tech accountability in the United States. There are currently two major avenues to accomplish this goal: through rulemakings at the state and federal level—with both California and Colorado promulgating new state privacy regulations and the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau developing federal regulatory proposals to combat commercial surveillance and strengthen data security—and through the enactment of comprehensive privacy laws in Congress and in state legislatures. EPIC is well suited to be a leading advocate for strong privacy protections in both state and federal arenas. We routinely provide expert input to lawmakers considering new tech-related legislative proposals, file complaints concerning emerging privacy violations with the FTC and state attorneys general, and more.

Recent Work

Over the last six months, EPIC has engaged in a wide range of research, education, and advocacy activities to promote and protect the privacy of Internet users; we:

- Provided testimony in the Maine State Legislature Judiciary Committee in support of LD 1977: An Act to Create the Data Privacy and Protection Act, which is based on the State Data Privacy and Protection Act proposed by EPIC.
- Testified in both the Massachusetts State House and Senate on H83/S25 (An Act establishing the Massachusetts Data Privacy Protection Act).
- Encouraged Massachusetts legislators to create a commission on automated decision-making by government entities in the state via the passage of H64/S33.
- Presented information on the State Data Privacy and Protection Act to Maryland Cybersecurity Council's Subcommittee on Law and Policy led by the Maryland Attorney General.
- Helped to lead the *amicus* effort in support of the California's Age-Appropriate Design Code (AADC) in a First Amendment challenge brought by NetChoice–whose members include Google, Meta, Amazon, Twitter, and TikTok. In July EPIC submitted an amicus brief defending the state's right to enact a strong privacy law.
    - In September, the district court held that the AADC likely violates the First Amendment. The California Department of Justice has appealed that decision and EPIC responded to that ruling and launched a blog series on the case.
- Developed a state privacy bill scorecard and began the process of "grading" existing state privacy laws and proposed legislation. We anticipate releasing a report on our analysis in the coming months.
- Convened regular coalition meetings of civil society groups to coordinate our advocacy efforts directed at the FTC and the public, share updates and intelligence, and prepare for the next phase(s) of the rulemaking process.
- Launched a blog series on data minimization and FTC rulemaking, which we believe will inform the rulemaking process as our resources are reviewed by key decisionmakers.
- After publishing our report, *Generating Harms: Generative AI's Impact & Paths Forward,* EPIC met with FTC leadership to review the report and its implications for further rulemaking.
- Alongside Fairplay and CDD, EPIC urged the FTC to require an independent audit of a face-scanning parental consent tool.
- Submitted comments to both the FTC and the DOJ on the latest Merger Guidelines recommending that both agencies require that data consolidation and consumer privacy be considered in the review of future mergers.

- Urged the CFPB to impose data minimization requirements on third-party apps and services that access consumers' personal financial information—a recommendation that the Bureau incorporated into its newly-proposed rule on personal financial data rights.
- Helped lead a coalition effort to ensure that credit header data (names, address, social security numbers, and the like) comes within the privacy protections of the Fair Credit Reporting Act (FCRA).
  - Followed this up with extensive comments urging the CFPB to make the most of its rulemaking authority under FCRA by broadening the scope of covered entities, narrowing the permissible purposes for which data brokers and credit reporting agencies can sell or disseminate personal data, and banning several particularly harmful consumer reporting practices.
  - CFPB has indicated that it will adopt many of these recommendations, and EPIC renewed several others in follow-up comments filed late last month.
- Supported the launch of the FCC's new Privacy and Data Protection Task Force. EPIC highlighted the Task Force as a positive step, expressing that the FCC could be more aggressive in using their authority.
- Worked with both caucuses in the House Energy and Commerce Committee towards reintroduction of a comprehensive federal privacy bill. EPIC recently advised Committee staff in a hearing in the Innovation, Data, and Commerce Subcommittee on "Safeguarding Data and Innovation: Building the Foundation for the Use of Artificial Intelligence."
- Continued to provide technical assistance to many offices on other pending or proposed legislation, including working with the House Committee on Oversight and Accountability on AI legislation, with Senate Judiciary on the SHIELD Act, with Senator Markey's office on COPPA 2.0, and with offices on the issue of age verification/age assurance in kids' online safety legislation.
- Participated in a panel on "The US Data Privacy and Security Legislative Landscape" hosted by ForumGlobal as a part of their 5th Annual Data Privacy Conference.
- Wrote an op-ed for *Bloomberg Law*, calling for a national standard for privacy online.
- Published analysis on the harms caused by surveillance advertising and a lack of comprehensive consumer privacy protections, as well as analysis on the role that data minimization must play in FTC rulemaking.

Key Staff

- Alan Butler, EPIC Executive Director
- Caitriona Fitzgerald, EPIC Deputy Director

- John Davisson, EPIC Senior Counsel and Litigation Director
- Megan Iorio, EPIC Senior Counsel
- Calli Schroeder, EPIC Senior Counsel and Global Privacy Counsel
- Ben Winters, EPIC Senior Counsel
- Sara Geoghegan, EPIC Counsel
- Suzanne Bernstein, EPIC Law Fellow
- Kara Williams, EPIC Law Fellow
- Caroline Kraczon, EPIC Law Fellow

PROJECT ON SURVEILLANCE OVERSIGHT

Project Overview

EPIC's Surveillance Oversight Project was established to confront the reality that increasing surveillance—particularly indiscriminate, mass surveillance—negatively impacts our democracy and is often disproportionately directed towards traditionally marginalized groups. In recent years, the project has focused public attention on the collection and use of biometrics, particularly facial recognition, by governments.

Recent Work

EPIC has long called for Congress to amend Section 702 of the Foreign Intelligence Surveillance Act (FISA) and has been working with members of Congress and with a bipartisan coalition of civil liberties groups to develop consensus reforms, including more robust safeguards on the collection and querying of U.S. person information under Section 702, greater accountability and meaningful avenues for redress, and greater transparency of the government's use of Section 702 in the cybersecurity context. EPIC joined a bipartisan coalition of civil liberties organizations in underscoring the need for significant reform to warrantless government surveillance activities ahead of a meeting with Director of National Intelligence (DNI). In September, The Privacy and Civil Liberties Board recommended that agencies be required to obtain individualized judicial approval for accessing Americans' communications under Section 702. Following the PCLOB report's release, privacy, civil liberties, and civil liberties groups released a joint statement reiterating the need for these reforms.

Jeramie Scott, EPIC Senior Counsel & Director of the Project on Surveillance Oversight, released the following statement regarding the PCLOB's report: "The PCLOB's report puts to rest any debate over requiring individualized judicial approval before accessing Americans' communications acquired without a warrant. However, as our bipartisan coalition has made clear for months, reforming Section 702 alone will not address the broader warrantless surveillance ecosystem that affects Americans and their communities every day. Congress must rise to the occasion and prohibit the government from relying on proclaimed executive authority or data brokers to skirt its constitutional and statutory obligations to Americans."

EPIC has also continued to pursue important work addressing current gaps in surveillance oversight, constitutional protection, transparency, and agency accountability. This includes researching and tracking Fourth Amendment cases concerning emerging surveillance technologies and analyzing new programs and systems of surveillance being put into place by government. In the last six months, we have:

- Testified on changes to electronic monitoring programs before a hearing of the DC Council Committee on the Judiciary & Public Safety on the Safer Stronger Amendments Act of 2023.
- The Superior Court of New Jersey ruled in *New Jersey v. Arteaga* that a defendant is entitled to detailed information on how he was identified by a facial recognition search, a case in which EPIC filed an amicus brief arguing for human review of facial recognition systems.
- Filed comments urging the TSA not to proceed with a temporary waiver process that would allow people in certain states to use their mobile driver's licenses (mDLs) at TSA checkpoints before the agency goes through a full rulemaking process, and before significant technical standards for mDLs have been published.
- Published analysis on DHS's Privacy Impact Assessment on ICE's broad use of surveillance technologies with minimal oversight.
- Submitted an open letter to MLB team owners, vendors, and the professional sports industry writ large, urging them to put an end to the use of facial recognition and other biometric technology at sporting events. The letter went live during a protest outside the Phillies stadium.
- Filed a petition urging Attorney General Merrick Garland to investigate whether federal funding of acoustic gunshot detection tools, particularly ShotSpotter, complies with Title VI of the Civil Rights Act.
- Submitted comments to U.S. Customs and Border Protection urging the agency to reverse course on its plan to collect social media handles from current visa holders.
- Published a blog post analyzing the Office of the Director of National Intelligence (ODNI) report on the Intelligence Community's (IC) purchase of commercially available information (CAI). The partially declassified report was released in response to EPIC's FOIA request. The report found that the IC is collecting increasing amounts of CAI but does not know how much CAI it is collecting, what types, or even what it is doing with that data.

- Submitted a letter to the Senate Homeland Security and Government Affairs Committee and Judiciary Committees in opposition to S.1631, The Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act. The bill would expand the government's counter-drone authority.
- Published a blog post explaining the TSA'S 1:1 pilot facial recognition program and analyzing the drawbacks of facial recognition for identity verification without clear, overarching regulations of this technology.
- The New Jersey Supreme Court ruled that law enforcement cannot do an end run around the Wiretap Act when they want to force social media companies to provide users' communications. The opinion agreed with EPIC's amicus brief in the case.

Key Staff

- Jeramie Scott, Director of EPIC's Project on Surveillance Oversight
- Megan Iorio, Senior Counsel
- Jake Wiener, EPIC Counsel
- Tom McBrien, EPIC Law Fellow
- Chris Baumohl, EPIC Law Fellow

AI AND HUMAN RIGHTS PROJECT

Project Overview

Artificial Intelligence (AI) and automated decision-making (ADM) systems are being used by a myriad of private sector and government entities, in contexts ranging from law enforcement investigations and sentencing in the criminal justice system to education and hiring. Not only are these systems being used to make life-altering decisions, but they are also often deployed in opaque and unaccountable ways that can exacerbate biases and harm individuals. Yet despite this, the use of these systems is largely unregulated in the United States. In response to this growing problem, EPIC established an AI and Human Rights Project to advocate for transparent, equitable, and commonsense AI policies and regulations.

Recent Work

We have seen a rapid increase in the pace of AI deployment and development over the last year, and privacy is a key focal point in the debates around rules to promote fair, accountable, and transparent automated systems that respect individual rights and equity. Data privacy is essential to AI policy, and our work strives to recognize and center that. Without meaningful data minimization or disclosure rules, companies have an incentive to collect and use increasingly more (and more sensitive) data to train AI models. The excuse for collecting this data indiscriminately—driven by cycles of competition and evolution with AI systems—threatens to undermine the core purpose of privacy and data protection frameworks, which are to secure individuals' rights to be free from unchecked data collection and use.

There was recently a major milestone in the collective effort to ensure that our government establishes AI policies that put people over profits and meaningfully rein in big tech. President Biden signed a sweeping Executive Order on "Safe, Secure, and Trustworthy Artificial Intelligence." EPIC issued a press release, and, alongside coalition partners and other groups, was in attendance to commemorate this important step and set the stage for the important work ahead. EPIC is proud to be part of the broad civil rights and digital justice coalition that has engaged with the White House on this important effort. This Order builds on the principles established last year in the Blueprint for an AI Bill of Rights. We need strong, clear rules around the use of AI by law enforcement to address one of the most significant threats to digital civil rights in this generation. Prior to the Executive Order EPIC sent a letter to the White House urging the Biden-Harris Administration to prioritize building agency workforce and resources for AI oversight and accountability.

In September, building on two years of state contracting research, EPIC published a report on the oft-forgotten world of government AI procurement. Across the country, state and local governments are experimenting with AI tools that outsource important government decisions to private companies, all without public input or oversight. These systems assign children to schools, inform medical decisions about patients, impact policing decisions about where to patrol and whom to target, and determine who receives public benefits. And they are all developed and operated by private companies like Deloitte, Thomson Reuters, and LexisNexis. EPIC's report *Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making* not only highlights the variety of AI systems embedded in state government, but also the major companies behind many of the most common government AI systems.

In the last six months, we also:

- Testified before the New York Assembly Standing Committees on Labor and Science & Technology, describing the breadth of increased worker surveillance and exploitation through the use of AI and offering the legislators clear paths forward to address the resulting harms.

- Were featured in President Obama's article "What I'm Reading on the Rise of Artificial Intelligence" for the "Zero Trust AI Governance" framework developed by EPIC, the AI Now Institute, and Accountable Tech.
- Submitted comments to the Federal Election Commission to support Public Citizen's petition for rulemaking to address the ongoing threat of disinformation ahead of the 2024 elections.
- Published a blog post on Generative AI and upcoming elections highlighting how GAI can exacerbate the issues of election misinformation and disinformation.
- Joined a letter urging Senate Majority Leader Chuck Schumer to include climate considerations while considering how to regulate AI technologies.
- In a follow-up piece to EPIC's May report *Generating Harms*, published a non-exhaustive list of Generative AI tools on the market broken down by type of content generated.
- Published a chart outlining and comparing the state AI laws proposed in 2023.
- Testified before the Massachusetts State Legislature in support of House Bill 64 and Senate Bill 33, *An Act establishing a commission on automated decision-making by government in the Commonwealth.*
- Submitted comments to the Office of Science and Technology Policy (OSTP) concerning the National Artificial Intelligence Strategy, calling on the administration to center risks, rights, and responsibilities in its approach to AI.
- Commended the National Telecommunications and Information Administration's inquiry into AI accountability measures in comments.
- Urged the OSTP to consider the full range of workplace surveillance harms in comments submitted to the Administration.
- Urged the FCC to explicitly data from telecommunications relay services (TRS)—services made available for individuals with hearing or speech disabilities—from being used to train AI data sets without consent.

Key Staff

- Ben Winters, Senior Counsel
- Enid Zhou, Senior Counsel
- Tom McBrien, EPIC Law Fellow
- Grant Fergusson, EPIC Equal Justice Works Fellow
- Maria Villegas Bravo, EPIC Law Fellow

OTHER PROJECTS

Overview and Recent Work

The three key program areas outlined above have comprised a significant part of EPIC's work in 2023, but we will have also continued our efforts on other projects and issues. For example:

- As part of our Telephone Subscriber Privacy Project, we have advocated for the Federal Communications Commission (FCC) to bring enforcement actions against service providers when they neglect to follow through on their commitments to reduce robocalls. In the last six months, we have:
    - Alongside partners, urged the Federal Communications Commission to reduce the tide of illegal phone calls consumers face by helping legitimate callers understand when their calls are being mixed with illegal traffic.
    - Filed an amicus brief alongside the National Consumers League urging the Ninth Circuit to hold carriers liable when they fail to sufficiently protect consumers from SIM swap attacks, which can allow a fraudster to wipe out a person's entire life savings.
    - Joined the National Consumer Law Center in calling on the FCC not to proceed with its proposed modified rules and instead enforce the stronger, existing rules regarding consent to receive texts and prerecorded telemarketing calls.
    - Submitted comments urging the FCC to expand its focus on caller ID authentication to include curtailing short-term rentals of phone numbers which can bypass caller ID authentication rules.
- We have continued to expand our work on health privacy and reproductive privacy in recent months, and recently we have:
    - Filed a complaint with the FTC urging the Commission to investigate Grindr's privacy practices after Grindr failed to safeguard users' sensitive personal data and apparently violated the Health Breach Notification Rule (HBNR).
    - Submitted comments to the Senate Committee on Health, Education, Labor, and Pensions urging them to protect health data and patient privacy.
    - Commended the FTC's rulemaking to expand the scope of HBNR-covered entities, and suggested further steps the agency could take.
    - Submitted comments in support of the FTC taking enforcement action against genetic testing company Vitagene for unfair and deceptive trade practices involving genetic and health information.

  - Praised the Department of Health and Human Services' new reproductive health safeguards for the HIPAA Privacy Rule and called on the agency to expand those protections.
- Filed comments urging the UK Information Commissioner's Office (ICO) to make updates to its draft biometric data guidance. The guidance is meant to instruct organizations using biometric systems and vendors of these systems on good practice and legal obligations.
- Published analysis on *Acheson Hotels v. Laufer* and its potential impact on the difficulty of establishing informational standing.
- Submitted an amicus brief in *Bride v. Snap* urging the Ninth Circuit to reinforce previously established limits on Section 230 and to allow a lawsuit against an anonymous messaging company to be decided on its merits.
- Called on the Consumer Financial Protection Bureau (CFPB) to strengthen protections for consumers.
- FTC updated safeguards rule to require data breach reporting, adopts EPIC recommendations.
- Urged the Federal Communications Commission to prioritize privacy and cybersecurity in its rulemaking on deploying Next Generation 911 (NG911) technologies.

Threats to individual privacy from corporate and government surveillance intensify each day, and EPIC will be working to curb the myriad of data abuses that harm consumer privacy and threaten democracy.

Key Staff

- Enid Zhou, EPIC Senior Counsel
- Megan Iorio, EPIC Senior Counsel and Director of the Amicus Project
- Chris Frascella, EPIC Law Fellow
- Tom McBrien, EPIC Law Fellow
- Calli Schroeder, EPIC Senior Counsel and Global Privacy Counsel
- Sara Geoghegan, EPIC Counsel
- Suzanne Bernstein, EPIC Law Fellow
- Maria Villegas Bravo, EPIC Law Fellow

CONCLUSION

The work of promoting the protection of Internet privacy has never been more important than it is right now. Policymakers in the United States and abroad are hard at work writing the rules that will govern our digital lives for many years to come. And EPIC plays an important role raising public attention to emerging privacy issues, conducting expert research and analysis to inform policy and enforcement actions, and supporting a broad and diverse coalition of civil society groups working to secure the right to privacy for all individuals online. We are grateful for the support provided through the *In re Google Street View* award fund and we are confident that the funds are being put to good use to serve the interests of individual impacted in the case who deserve better privacy protection.