EXHIBIT D

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

June 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 one of nine recipients 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 to promote 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 first 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 first 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 encompasses 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.

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:

- Published in-depth analysis of important consumer privacy issues including models for state comprehensive privacy protection, an examination of calls to ban or regulate TikTok, a review of current gaps in sector-specific federal privacy protection, and a series of posts about the proposed data minimization standard that the FTC should adopt to protect privacy online.
- Filed an amicus brief arguing that courts must recognize individuals' concrete interest in the use of their personal information for advertising purposes and hold that victims of misappropriation and violations of the right to publicity have standing to sue.
- Filed comments to the FTC supporting the Commission's enforcement against educational technology company Chegg for failing to secure millions of users' data, and the establishment of access, deletion, and data minimization requirements in the settlement.
- Filed an amicus letter brief urging the California Supreme Court to overturn a lower court decision that imported a restrictive federal standing test into a California state case concerning violations of the Fair Credit Reporting Act.
- Submitted comments to the Colorado Attorney General to strengthen proposed rules implementing the Colorado Privacy Act.

- Successfully advocated as amicus to the Illinois Supreme Court in *Cothron v. White Castle*, where the court found that individuals seeking redress under the state biometric privacy law can sue for each instance when their rights were violated.
- Submitted comments to the National Telecommunications and Information Administration to inform its ongoing review of "Privacy, Equity, and Civil Rights" online, encouraging the agency to maintain its focus on harmful commercial data practices.
- Tracked amendments to and implementation of new privacy regulations in California and Colorado.
- Led a coalition amicus brief defending the constitutionality of California's Age Appropriate Design Code, a landmark bill that requires online companies to design their services with children's privacy in mind.
- Submitted comments to the EU Commission on its review of vision for regulations and guidance related to the metaverse.
- Supported the rollout of the new White House National Cybersecurity Strategy, which includes important policy recommendations for new data protection legislation that would set clear limits on the collection and use of personal information.
- Collaborated with NYU Tech Law & Policy Clinic to file a complaint with the Consumer Financial Protection Bureau about Rocket Money for deceptive practices that violate the Dodd-Frank Act and the Fair Credit Reporting Act.
- Filed comments urging the Consumer Financial Protection Bureau to strengthen financial data rights through rulemaking and specifically prohibit third parties from collecting, using, or retaining personal information beyond what is reasonably necessary to provide a product or service the consumer has requested
- Petitioned the Consumer Financial Protection Bureau to publish an advisory opinion clarifying that credit header data is not exempt from the Fair Credit Reporting Act, promulgate rules, and increase enforcement actions against data brokers.
- Led a coalition of civil society groups in advocating for the FTC to adopt a strong commercial surveillance rule through biweekly meetings, building on extensive comments filed in Fall 2022.

Key Staff

- John Davisson, EPIC Senior Counsel and Litigation Director
- Calli Schroeder, EPIC Senior Counsel and Global Privacy Counsel
- Ben Winters, EPIC Senior Counsel
- Sara Geoghegan, EPIC Counsel
- Suzanne Bernstein, 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

We have continued to pursue important work over the last six months to address unchecked government surveillance that impacts the privacy of Internet users. A large focus of our surveillance oversight work in 2023 is on proposed reforms to Section 702 of the Foreign Intelligence Surveillance Act (FISA), which is the authority under which the U.S. Intelligence Community conducts much of its surveillance of Internet communications and other data stored or handled by U.S. providers. This authority will sunset at the end of 2023 unless reauthorized by Congress, and EPIC is taking the opportunity to provide expert input and support the broader coalition of civil society groups advocating for necessary reforms.

EPIC has long called for Congress to amend Section 702 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. In November 2022, we submitted comments to the Privacy and Civil Liberties Oversight Board's (PCLOB) Oversight Project examining Section 702, recommending that the Board urge Congress to prohibit "abouts" collection and warrantless backdoor searches. EPIC's Jeramie Scott was then invited to speak on these points before the PCLOB in January 2023. We have continued these efforts and are advocating for Congress to either enact serious reforms to Section 702 or let it sunset, as they did with Section 215 of the PATRIOT Act, another post-9/11 surveillance authority. In the last six months we have also:

- As an invited panelist before the Privacy and Civil Liberties Oversight Board (PCLOB), called on PCLOB to investigate the scope of use of Section 702 authorities in cybersecurity investigations.
- Published in-depth analysis of emerging Section 702 reform proposals, including an initial overview, a deep dive on proposed limits to close the "backdoor search" loophole, an overview of ways to strengthen the amicus curiae process in the FISA Court, and a discussion of meaningful avenues for individual judicial redress.
- Launched a coalition-led website, along with a parallel EPIC campaign page, to educate the public about the need for significant reform of Section 702 authorities.
- Tracked and updated the public on important intelligence surveillance developments, including the publication of a significant opinion of the Foreign Intelligence Surveillance Court about FBI misuse of Section 702 data, the release of the national intelligence surveillance transparency report, and more.

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:

- Pursued release of a report from the Office of the Director of National Intelligence on government purchases of sensitive data.

- Testified in the Maryland Senate Finance Committee to provide expert input on the states proposed biometric information privacy law.
- Filed comments urging the FTC investigate the use of police endorsements as a tool by companies to promote their home surveillance products, including security cameras.
- Filed a brief as amicus curiae in the New Jersey Supreme Court arguing that police should be required to seek a wiretap order to obtain a prospective disclosure order for Facebook users' future communications.
- Argued as amicus in the Fourth Circuit that school officials cannot search a students' cell phone in coordination with police officers without a warrant.
- Filed comments calling on the General Services Administration to implement stricter protections on contractor access to data for fraud prevention services and consider abandoning behavioral analytics techniques.
- Published an analysis of government use of COVID-19 Relief funds to drive police purchases of new surveillance technologies.

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.

A new focus of our work in 2023 is to respond to the rapid deployment of Generative AI systems – which are both overhyped in terms of their capabilities and in terms of the "longterm" concerns raised by those who have developed them. EPIC has already begun work to contribute an independent and well-researched voice to the policy discussion around these emerging AI systems. In the last six months, we:

- Organized a private roundtable of domain experts and EPIC members about the policy considerations around Generative AI harm.
- Published a blog post about the information manipulation concerns related to ChatGPT.
- Published *Generating Harms: Generative AI's Impact and Paths Forward*, a report detailing the wide variety of harms that new generative A.I. tools like ChatGPT, Midjourney, and DALL-E pose today.

Our recent report recognizes that while Generative AI systems are new, many of the harms they can cause track longstanding threats to privacy, transparency, racial justice, and economic justice imposed by other emerging technologies and business practices. To illustrate these challenges and potential paths forward, the report includes numerous case studies, examples, and research-backed recommendations. The report also includes an Appendix of Harms, designed to provide readers with a common lexicon for understanding the various harms that new technologies like GAI can produce.

We have also worked over the last six months to promote and support the development of commonsense AI policies by the White House and federal agencies. EPIC published a series of four blog posts breaking down the AI Risk Management Framework (RMF) released by the National Institute of Standards. This framework was congressionally directed and is one of the latest entrants into a crowded field of helpful optional guidelines for AI users and regulators.

- Published a blog post on the Map section of the RMF
- Published a blog post on the Govern section of the RMF
- Published a blog post on the Measure section of the RMF
- Published a blog post on the Manage section of the RMF

In furtherance of the goal to strengthen existing consumer protection and civil rights laws, EPIC has also provided expert testimony and submitted comments to federal and state agencies:

- Submitted comments in support of the Equal Employment Opportunity Commission's Draft Strategic Plan that is focusing on enforcing discrimination through hiring via automated decision-making systems.
- Led a coalition on extensive comments to the California Privacy Protection Agency on how to draft regulations pursuant to the California Privacy Rights Act.
- Recommended that the Administrative Conference of the United States consider the administrative burdens exacerbated by the adoption of automated decision-making systems.

Key Staff

- Ben Winters, Senior Counsel
- Enid Zhou, Senior Counsel
- Tom McBrien, EPIC Law Fellow
- Grant Fergusson, EPIC Equal Justice Works 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 International Privacy Program, we have worked with our international coalition partners to advocate for enhanced privacy protections in the pending transatlantic data transfer framework.
- 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:
    - Urged the FCC to take action to block unwanted telemarketing and scam text messages, and to better protect consumers from malicious URLs.
    - Supported the FTC's proposed rule combating government impersonation fraud calls and urged the agency to expand its efforts to combat other impersonation scams.
    - Urged the FCC to set strong privacy and security rules before pressing cell phone carriers to expand collection of precise handset location data.
    - Supported updated data breach notification requirements by the FCC but cautioned the agency against using a vague harm standard that would limit notifications.
    - Successfully advocated for the FCC to impose limits on artificial and prerecorded calls to residential lines.
    - Successfully advocated for the FCC to consider including more extensive details of privacy practices in its "Broadband Nutrition Label" requirements.
    - Called on the FCC to use its broad authority to better protect consumers from data breaches caused by inadequate data security.
- Under a new initiative this year, we have begun to provide litigation support to other advocacy organizations working on cases involving emerging Internet privacy issues.
- As part of our work to protect location privacy, we have called on the FCC to severely limit, if not outright prohibit, the use of geolocation information for its suicide hotline program, 988.
- We are also deepening our work and focus on defending reproductive privacy and health privacy in the aftermath of the Supreme Court's *Dobbs* decision that overturned *Roe v. Wade* and undid fifty years of precedent protecting the constitutional right to privacy. Over the last six months, we have:
    - Urged the White House to ensure that federal policing funds are not used to fuel surveillance of individuals seeking reproductive health services.

- Argued as amicus in *Colorado v. Seymour* that the CO Supreme Court should find that "reverse keyword search" warrants are unconstitutional and would have especially chilling impacts on reproductive health in the wake of *Dobbs*.
- Urged the Department of Health and Human Services to scrap plans to create database to track recipients of free HIV PrEP medication.
- Supported the FTC's enforcement action against an online counseling company broke health privacy promises and used sensitive health data for ad targeting.

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

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.