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

In re Google Location History *Cy Pres* Award Proposal

October 25, 2023

BACKGROUND

1. NAME

Electronic Privacy Information Center (EPIC)

2. FOUNDING AND HISTORY

EPIC's Organizational History

EPIC was founded in 1994 to focus public attention on emerging privacy and civil liberties issues. That year, we launched the Internet's first online petition, the effort to stop the NSA's ill-conceived Clipper Chip encryption scheme. A letter to the President, signed by 42 leading technology experts and legal scholars, attracted the support of more than 50,000 Internet users. The petition was delivered to the White House, and the Clipper Chip proposal was eventually withdrawn. Since that time, EPIC has played a leading role in a wide range of civil liberties and privacy issues in the United States and around the world.

Our mission is to secure the right to privacy for all in the digital ecosystem through public education, advocacy, and expert analysis. We host some of the most comprehensive resources on internet privacy and security at epic.org and our monthly newsletter, the EPIC Alert, is one of the oldest and longest-running electronic newsletters on the Internet. Throughout EPIC's history, our work has focused on lifting veil on data collection practices, advocating for comprehensive privacy protections, and facilitating dialogue between advocates, experts, and decisionmakers. Our research has helped to focus discussions among policymakers and civil society about the impact of new technologies on privacy and human rights.

EPIC routinely engages in research and advocacy to promote privacy and educate the public and policymakers about emerging privacy issues. Our work is cited and relied upon by lawmakers, regulators, scholars, and privacy professionals around the world. EPIC's staff is frequently invited to testify as experts in legislative hearings and forums. We also participate in most agency rulemakings concerning data protection issues and privacy statutes including the Privacy Act, the California Consumer Privacy Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Federal Trade Commission Act, and many more. The donations, awards, grants, and other income that we receive go directly to further our work to establish stronger privacy and data security protections for internet users.

EPIC has long supported the establishment and enforcement of a comprehensive privacy and data protection framework in the United States. We believe that there should be strict limits on when user

data can be collected, processed, used, and retained by online platforms and other entities. Over the last three decades, we have been on the front lines defending users from privacy violations online. We filed landmark complaints with the Federal Trade Commission about Facebook and Google's deceptive privacy practices, supported rulemaking efforts by privacy regulators in California and Colorado, and have authored "friend of the court" briefs in numerous cases concerning civil and constitutional privacy rights. Most recently, we lead an amicus to defend California's new Age-Appropriate Design Code against a challenge from the tech advocacy group NetChoice.

EPIC's Recent Work on Location Data Protection

As part of its efforts to safeguard privacy, EPIC has done extensive work to strengthen protections for location data. In 2017, we highlighted many of the privacy issues with Google's Web & App Activity tracking in a complaint to the FTC. In particular, we explained why Google's secret purchase-tracking algorithm was an unfair trade practice and highlighted the fact that "there appear[ed] to be no mechanism by which Google users [could] opt out of purchase tracker other than by disabling location tracking entirely. Accordingly, we argued that "The need for Google users to opt out of location tracking to avoid in-store purchase tracking [was] misleading because a reasonable consumer would have no reason to know that the latter relies on the former."

In January 2022, attorneys general from the District of Columbia, Texas, Washington, and Indiana sued Google, alleging that the company used dark patterns to repeatedly nudge users to provide more location data. This lawsuit targeted some of the problematic data collection settings we had raised in our 2017 complaint, demonstrating EPIC's vigilance and early detection of Google's unfair and deceptive location data practices.

Over the last few years, we have seen how users have been put at risk by the exposure of sensitive location data in the aftermath of the Supreme Court's decision in *Dobbs*. That's why we worked with worked with a coalition of over 70 organizations to send a letter to Sundar Pichai, the CEO of Google, in June 2022, calling on the company to end its collection and retention of users' location data. We explained that because "law enforcement officials routinely obtain court orders forcing Google to turn over its customers' location information," Google should not "allow its online advertising-focused digital infrastructure to be weaponized against people seeking abortions."

Aside from closely scrutinizing Google's location data practices, we also strive to stop other apps and entities from collecting and selling location data without users' consent. In 2017, through a security researcher's investigation, we learned that a popular weather app was not only tracking the locations of users who had already expressly opted out of location tracking, but also misleading users by sending their personal location data to third-party companies for targeted advertising.

Soon after this discovery, in 2018, EPIC brought the first location data tracking lawsuit under the D.C. Consumer Protection Procedures Act against AccuWeather International, Inc., alleging that the company engaged in unlawful and deceptive practices in tracking users' locations. Following our lawsuit, AccuWeather overhauled its app and changed its location tracking practices, including by separating location service controls for functional purposes and for advertising purposes. We were pleased to see these changes and believe they are necessary to put users in control of their own cell phone location data.

Also in 2018—on the same day that the complaint in this case was filed—EPIC sent a letter to the FTC about Google's location tracking practices. EPIC explained that "Google is not permitted to track users after they have made clear in their privacy settings that they do not want to be tracked. This privacy violation affects all Android users and iPhone users who use Google Maps or search. EPIC urges the Commission to enforce its Order and hold Google accountable."

In another case, *EPIC v. DOJ*, No. 18-1814 (D.D.C.), we sought the public release of information detailing the Department of Justice's collection of cell site location information (CSLI) through § 2703(d) court orders. As CSLI can reveal the most intimate details of an individual's everyday life—from religion to political beliefs to health conditions—EPIC was interested in learning more about the DOJ's use of cell site location information for law enforcement investigations. In our initial FOIA request, we explained that we sought to "determine the use, effectiveness, cost, and necessity in the collection and use of cell site location information so that the public, lawmakers, and the courts may have a better understanding of the use of this investigative technique."

Months later, as a result of our lawsuit, the DOJ agreed to provide a detailed breakdown of the total number of applications, orders, and warrants for cell phone location data under § 2703(d) from five U.S. Attorney's Offices between 2016 and 2019. As prosecutors currently do not release any comprehensive or uniform data about their surveillance of cell phone location data, we compiled the information we received from the DOJ in a comparative table for each district. Interestingly, we found that the U.S. Attorney's Office for the District of Rhode Island and the U.S. Virgin Islands—two of the smallest offices in the country—had sought warrants for location data information during the specified period of time. Moving forward, we intend to continue to push for more transparency and hold both private companies and federal agencies accountable for the improper or overbroad collection of location data.

3. CURRENT GOALS

EPIC's overarching goal is to be a coalition leader and driving force for the development of policy standards that legislators, regulators, and companies adopt and rely upon to protect privacy online. Specifically, we are pursuing a number of specific goals across our project areas to advance privacy protections in the digital ecosystem:

- To support the establishment of strong, comprehensive privacy standards in the United States that minimize the collection and use of personal data and include heightened protections for particularly sensitive categories of personal data, including location, health, communications, and children's data.
- To research and advocate for human rights-based safeguards on the development and use of artificial intelligence systems in commercial settings, including transparency, accountability, accuracy, and non-discrimination requirements.
- To identify and seek to end abusive business practices of data brokers, adtech firms, and other platforms that collect and monetize our personal data and increasingly enable law enforcement to conduct backdoor surveillance.
- To promote the development of privacy-enhancing technologies and business practices that support, rather than erode, individual privacy protections.

4. CURRENT PROGRAMS

EPIC pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. EPIC participates in many of the most significant cases, rulemakings, and other regulatory proceedings concerning online privacy. EPIC also obtains records under the federal open government laws and seeks to maximize transparency about government data collection policies and systems. EPIC also leads and participates in civil society dialogues, roundtables, panels, and other forums that serve the public interest. We frequently testify before state and federal legislatures and agencies about emerging privacy and civil liberties issues.

Consumer Privacy Advocacy

When consumers make a purchase online, browse the internet, or scroll through social media, they expect that companies will use their information solely for the purposes of the transaction. All too often, companies misuse, sell, or fail to protect consumers' personal information. EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the federal and state agencies to address emerging privacy issues and to safeguard the privacy rights of consumers. EPIC has also long advocated for the establishment of a strong, comprehensive privacy law in the United States and for robust enforcement.

Surveillance Oversight

EPIC's Project on Surveillance Oversight 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. We also advocate for much needed reforms to the laws that authorize government surveillance for criminal and national security purposes, many of which were written long before the digital era and do not adequately address the problems we see today.

AI and Human Rights Project

Through its AI and Human Rights Project, EPIC seeks to promote the adoption of transparent, equitable, and commonsense AI policies that respect human rights. New technologies have emerged that create the promise of significant advancement across many different scientific and technological fields, but the deployment of these new AI systems presents significant risks. EPIC has particularly focused on advocating for a robust regulatory architecture governing the deployment of AI systems.

5. EXTERNAL RATINGS

EPIC has been awarded the Gold Star of Transparency from Guidestar, and Charity Navigator has given EPIC a score of 93.98, earning EPIC a 4-Star rating.

6. CY PRES EXPERIENCE

EPIC has been a recipient of *cy pres* awards for over a decade. This following list highlights awards received in just the last 12 months:

Case Name	Award Amount	Date Received
***Krakauer v. Dish Network*, 14-2184 (M.D.N.C.)**	$700,000	Scheduled Q4 2023
In re: iPod Nano Cases	$263.86	10/2023
Hawkins et al. v. Startek	$615.00	9/2023
Gaston v. FabFitFun	$16,294.67	08/2023
Sherman v. Brandt Industries USA	$23,529.92	06/2023
Chicago Car Care, Inc. v. A.R.R. Enterprises, Inc.	$255.02	05/2023
Fabricant v. AmeriSave	$439,505.22	04/2023
In re: Lenovo Adware Litigation	$87,625.15	02/2023
In re: Google Street View	$1,006,582	12/2022
Able Home Health, LLC v. Willamette Valley Toxicology LLC	$4,213.79	12/2022
In re Google Plus Profile Litigation	$378,028.51	09/2022

Other relevant *cy pres* awards include:

Case Name	Award Amount
In re: Vizio, Inc. Consumer Privacy Litigation	$12,358
Abramson v. American Advisors Group, Inc	$3,942
Dolemba v. Champion Roofing, LLC	$1,779
William Harrison v. The Irvine Company LLC	$353,408
Craftwood Lumber Co. v. Senco Brands, Inc.	$10,857
Lopez v. Superior Health Linens, LLC	$84,367
West Loop Chiropractic & Sports Injury Center, Ltd., et al. v. North American Bancard, LLC	$4,273

GRANT PROPOSAL

7. PROJECT DIRECTOR

Alan Butler, Executive Director and President of EPIC.

Mr. Butler joined EPIC in 2011 and served as Interim Executive Director during 2020. Prior to his appointment as Executive Director, Mr. Butler managed EPIC's litigation, including the Amicus Program, and filed briefs in emerging privacy and civil liberties cases before the U.S. Supreme Court and other appellate courts. Mr. Butler has argued on behalf of EPIC in privacy and open government cases in the U.S. Court of Appeals for the D.C. Circuit, the Third Circuit, and the Supreme Courts of New Mexico and New Jersey. Mr. Butler has authored briefs on behalf of EPIC in significant privacy cases, including an amicus brief in *Riley v. California* that was cited in the Supreme Court's unanimous opinion upholding Fourth Amendment protections for cell phones. He has also authored briefs on national security, open government, workplace privacy, and consumer privacy issues. Mr. Butler is also Chair of

the Privacy and Information Protection Committee of the ABA Section on Civil Rights and Social Justice.

He is co-author of the most recent edition of Communications Law and Policy: Cases and Materials and has also published several articles on emerging privacy issues, including: Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after Riley v. California, Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance, and When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy. Mr. Butler is a graduate of UCLA School of Law and Washington University in St. Louis, where he earned a B.A. in Economics. He is a member of the DC Bar and the State Bar of California.

8. SUMMARY OF PROJECT REQUEST

All funds from this award would be used to carry forward EPIC's mission of securing the right to privacy for all online. The proposed award would provide general support for our staff attorneys working across our program areas, enable us to expand our capacity by bringing on a staff technologist and staff investigator, and help us improve our outreach and education work through an annual EPIC-hosted convening of entities, experts, and practitioners working to improve privacy protections online.

EPIC is uniquely positioned to serve the interests of class members in this case because we are the largest and most well-established non-profit in the country focused exclusively on protecting privacy online. As such, we can act as an expert voice for stronger privacy protections and build the coalition and frameworks necessary to ensure that these policies are converted to practice. Tackling issues at the intersection of emerging technologies and threats to user privacy requires both a detailed comprehension of the laws and core frameworks of privacy and data protection and an understanding of the technological systems and standards that underlie modern devices and information systems. These complex concepts need to be put in the context of everyday users to identify the privacy harms that result from data abuses, and also need to be situated in the broader context of policy priorities and goals at the local, state, and national level. EPIC has spent nearly three decades building the expertise, capacity, and reputation necessary to carry this important work forward.

This funding will allow us to carry forward important goals that we believe are necessary to strengthen privacy and security protections for Internet users.

Major Goals/Objectives

- Secure the adoption of robust, comprehensive privacy regulations that place the obligation on businesses to minimize the processing of our personal data and prohibit digital discrimination.
- Extend our long track record of investigating, calling public attention to, and highlighting for regulators those personal data practices that violate the privacy of Internet users.
- Publish resources on current privacy concerns, violations, approaches, and victories that will be available for internet users, journalists, policymakers, and any other interested audiences.
- Establish human rights-based safeguards on the development and use of artificial intelligence systems in commercial settings, including transparency, accountability, accuracy, and non-discrimination requirements.
- Further investigate the use of AI and automated decision-making systems in public benefits administration and other government programs.

- Build capacity to produce deeper, more frequent, and more technically sophisticated complaints and educational resources concerning abusive data practices.
- Organize an annual convening of civil society organizations focused on privacy and data protection.

Goal: Secure the adoption of robust, comprehensive privacy regulations that place the obligation on businesses to minimize the processing of our personal data and prohibit digital discrimination.

Context/Approach: EPIC has increasingly bolstered its position as an expert resource for lawmakers and regulators considering the adoption of privacy rules. We have submitted extensive comments as part of the privacy rulemakings in California and Colorado, testified before state legislatures in support of comprehensive privacy regulations, provided expertise on emerging tech issues to state legislators, filed amicus briefs in cases concerning critical privacy questions, shared research and recommendations with federal regulators focused on data protection, and much more.

In August 2022, the FTC announced that it would conduct its first-ever rulemaking on commercial surveillance and data security. EPIC has long called on the FTC to use its rulemaking authority to safeguard privacy and civil rights, including with our 2021 white paper *What the FTC Could Be Doing (But Isn't) to Protect Privacy*, and our 2022 report, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*. We were thrilled to see this development at the Commission and have already played an active role in the rulemaking, including by submitting a 230-page comment in November 2022 and convening a working group of peer organizations engaged in the process.

Activities: EPIC will craft model language, draft policy white papers, and circulate side-by-side comparisons of potential privacy legislation and regulations to inform the policymaking process. We also plan to build a supplementary toolkit to further demonstrate the positive impacts that a data minimization framework would have on harmful commercial surveillance practices. In addition, we will produce impactful advocacy pieces and events that raise awareness of the harms of commercial surveillance and how a privacy law can lead us towards a better future online. We will continue to hold biweekly coalition working group meetings on sufficient rulemaking mechanisms, provide testimony and comments on the FTC's draft rule after it is issued, and monitor the FTC's implementation of a final rule. We will also prioritize convening and collaborating with civil society groups in our existing coalition meetings, in new groups, and at our proposed annual forum.

Timeline: Ongoing, Year 1 to Year 3

Goal: Extend our long track record of investigating, calling public attention to, and supporting robust enforcement to stop data practices that violate the privacy of Internet users.

Context/Approach: In just the past few months, EPIC has submitted multiple complaints and comments to the FTC and DOJ focused on protecting privacy. EPIC 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). Alongside Fairplay, CDD, and Common Sense Media, EPIC urged the FTC to require an independent audit of a face-scanning parental consent tool. EPIC also submitted comments to both the FTC and the DOJ on the latest Merger Guidelines recommending that both agencies require that data consolidation and privacy be considered in the review of future mergers. EPIC also filed a complaint in December with the

Consumer Financial Protection Board highlighting the ways that financial technology company Rocket Money deceptively obtains, impermissibly uses, unlawfully shares the personal data of its customers.

Activities: We will continue our support of clearer guidelines and more robust enforcement mechanisms of privacy protections. This work includes but is not limited to filing amicus briefs, submitting complaints, authoring and signing onto petitions, and working directly with enforcement bodies.

Timeline: Ongoing, Year 1 to Year 3

Goal: Publish resources on current privacy concerns, violations, approaches, and victories that will be available for internet users, journalists, policymakers, and any other interested audiences.

Context/Approach: EPIC regularly publishes blog posts, white papers, reports, news interviews, and other resources for internet users, journalists, and policymakers. In 2020, EPIC released *Grading on a Curve: Privacy Legislation in the 116th Congress,* which provided an overview of the elements of a privacy law as well as a scoring system for legislation. We published The State of State AI Laws: 2023, an analysis of the various state AI laws that have been introduced, passed, or gone into effect in the 2023 legislative session. As public education is a key part of EPIC's mission, we endeavor to publish timely resources for lawmakers, journalists, advocates, and members of the public who are interested in key developments in tech policy. This post serves as a follow-up to our widely popular 2022 round-up and has already received coverage, including on an episode of Tech Policy Press's *Sunday Show*.

Activities: EPIC will continue to research and publish analysis, white papers, reports, web resources, and updates in our monthly newsletter. With this funding, we would also build our capacity to monitor the compliance of large tech companies and data controllers with applicable privacy regulations and make that information and analysis available through EPIC's website.

Timeline: Ongoing, Year 1 to Year 3

Goal: Establish human rights-based safeguards on the development and use of artificial intelligence systems in commercial settings, including transparency, accountability, accuracy, and non-discrimination requirements.

Context/Approach: In addition to scrutinizing government use of AI and informing the public of abuses, EPIC strives to protect all those who are discriminatorily screened and scored by advocating for oversight and enforcement. When we discovered that Airbnb was developing an opaque algorithm to generate risk assessment scores and determine the "trustworthiness" of potential renters, we filed a complaint with the FTC and urged the agency to investigate Airbnb's unfair trade practices. In another instance, we sent comments to the Consumer Financial Protection Bureau recommending the agency revise its regulations on the use of AI and machine learning systems by financial institutions to comply with the Universal Guidelines for AI and the OECD AI Principles. EPIC is also currently working with the Rose Foundation on a project on the CCPA to develop model privacy and algorithmic risk assessments to educate consumers and promote best practices for entities processing personal data.

Activities: We will be tracking uses of AI in sectors ranging from education and hiring to housing and credit scoring. As we continue to identify examples of screening and scoring in everyday life, we will act to notify regulatory agencies of potential abuses.

Timeline: Ongoing, Year 1 to Year 3

Goal: Further investigate the use of AI and automated decision-making systems in public benefits administration and other government programs.

Context/Approach: In 2022, we launched our new Screening and Scoring Project, which aims to investigate instances of screening and scoring in everyday life and intervene where possible to better protect the public from algorithmic harm. This coincided with the publishing of our report *Scored and Screened in D.C.*, the result of a 14-month investigation that highlights the breadth of algorithmic tools used by the D.C. government and aims to improve transparency and accountability around taxpayer-funded systems that are often used against those taxpayers. We have published two more pivotal reports on AI in 2023 alone: *Generating Harms: Generative AI's Impact & Paths Forward*, and *Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making*. The former provides an assessment of the harms that Generative AI poses with respect to misinformation, data security, labor manipulation, the environment, and more. In addition to contextualizing potential harms with real-world case studies, the report provides tangible recommendations for legislatures, executives, and companies. The latter highlights how state and local governments are experimenting with AI tools that outsource important government decisions to private companies, all without public input or oversight.

Activities: We will continue to conduct research and produce educational resources about the opaque use of these technologies and the need for AI oversight.

Timeline: Ongoing, Year 1 to Year 3

Goal: Build capacity to produce deeper, more frequent, and more technically sophisticated complaints and educational resources concerning abusive data practices.

Context/Approach: Although EPIC has a long history of informing regulators and the public about abusive commercial data practices, there are far more such practices than we can fully investigate today. To grow our capacity to produce impactful complaints and educational resources, we seek to hire (1) a staff technologist to further EPIC's ability to understand and explain emerging data practices, and (2) a staff member with investigative reporting experience who can help develop complaints against businesses violating user privacy.

Activities: By augmenting the expertise of EPIC's staff with these hires, we can both expand and optimize our investigative capabilities and technological expertise.

Timeline: Year 1

Goal: Organize an annual convening of civil society organizations focused on privacy and data protection.

Context/Approach: As of today, there is no all-inclusive annual meeting of groups that work to secure the collective human right to privacy.

Activities: Host an annual event with panels and social events to encourage knowledge-sharing and collaboration among privacy organizations. EPIC seeks to continue and build upon our ongoing collaboration with our peer groups in civil society. This forum will be an ideal setting for organizations to inform each other about our ongoing work, share strategies and challenges, and identify priorities for privacy protection each year.

Timeline: Annual, Year 1, Year 2, Year 3

9. APPROACH

See "*Context/Approach"* under each goal in Section 8.

10. FUNDING REQUEST

We request an award of $7.5 million to support EPIC's important digital privacy work over 3 years ($2.5 million per year). We have provided a year-by-year budget so that this project can considered as a one year $2.5 million, two years $5 million, or full three years $7.5 million award.

PROJECT EXPENSES	Year 1	Year 2	Year 3	Total
Salaries and wages	$2,100,000	$2,100,000	$2,100,000	$6,300,000
Consultants and professional services – (Technologist and Investigative Specialists)	$150,000	$150,000	$150,000	$450,000
Conferences and Travel – Including Privacy Convening Forum	$130,000	$130,000	$130,000	$390,000
Communications, Subscriptions, and Research	$10,000	$10,000	$10,000	$30,000
Other indirect expenses (i.e., rent/occupancy, utilities, maintenance, office supplies and equipment and professional dues)	$110,000	$110,000	$110,000	$330,000
TOTAL	$2,500,000	$2,500,000	$2,500,000	$7,500,000

For further context, EPIC's operating budget for 2024 is $3,487,500, all of which is directed toward protecting the privacy and security of internet users. EPIC directs 83% of revenue to program activities—a top-tier standard for non-profit management.

11. USE

This funding will be used to support and expand EPIC's Consumer Privacy Project and to support EPIC's overall work to secure privacy on the internet. With this funding, we would also be able to expand our staff by hiring a technologist and a privacy violations investigator. And we would use this funding to support a forum for convening experts on privacy rights on the internet. As of now, there is no central coordinating event for civil society organizations focused on privacy and data protection; the proposed forum would fill a necessary gap in collaboration and the sharing of expertise.

12. TARGET POPULATION

EPIC's overall organizational constituencies include the general public, users of digital products and services, journalists focused on emerging privacy and civil liberties issues, state and federal lawmakers, and state and federal regulators.

We also know that the impacts of online surveillance systems are especially harmful for marginalized communities, fostering discrimination and inequities in employment, government services, healthcare, education, and other areas of life.

Our *Scored and Screened in D.C.* report highlighted the breadth of algorithmic tools used by the D.C. to sort residents into winners and losers based on data about health, finances, location, gender, race, and other personal information. These screening systems perpetuate existing disparities and deepen inequities.

As noted in Section 2, EPIC recognizes that users' sensitive location data has only become further imperiled in the aftermath of the Supreme Court's decision in *Dobbs*, and that is why we worked with over 70 coalition partners to call on the CEO of Google to end the company's collection and retention of users' location data.

EPIC also recently filed a petition urging Attorney General Merrick Garland to investigate whether federal funding of acoustic gunshot detection tools–a form of automated decision-making system–complies with Title VI of the Civil Rights Act. Substantial evidence shows that ShotSpotter disproportionately deploys its sensors in predominantly Black neighborhoods, replicating historically biased policing practices. On top of these problematic deployment practices, ShotSpotter systems are also riddled with inaccuracies.

Additionally, EPIC recently 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. The complaint follows from EPIC's long history of advocacy before the FTC calling for enforcement action against companies that violate users' privacy and abuse personal data. In 2010, EPIC filed a complaint about Google Buzz that led to the FTC's first consent decree with the company.

In 2023, EPIC joined three peer organizations in calling on the FTC to investigate new research indicating that YouTube and Google are tracking and targeting ads at viewers of "made for kids" videos—an apparent violation of the Children's Online Privacy Protection Act and Google's 2019 settlement with the FTC.

EVALUATION

13. REPORTS

EPIC will provide a report to the Court and the parties every six months to update both on the use of Settlement Funds and on how EPIC intends to allocate remaining funds for the duration of the provision.

14. EVALUATION

The success of EPIC's project work will be evaluated on both a short-term, continuous basis and through longer-term evaluations. EPIC hosts two weekly all-staff meetings in which current, upcoming, and completed work is reviewed. We also have weekly internal meetings specific to our consumer privacy work and a variety of bi-weekly and monthly coalition meetings. All of these venues will include conversations that evaluate our progress toward the aforementioned goals and next steps. In addition to these routines, EPIC has annual staff retreats in which we review progress made in the prior year, analyze our successes relative to our objectives, and plan for the next year.

Some key metrics we already use—and will continue to use—to measure the success of our work include:

- The adoption of data minimization rules and other key elements of effective data protection by federal and state policymakers;
- The adoption of legally-binding, human rights-centric safeguards on the use of AI and automated decision-making systems;
- The volume, depth, and reach of the complaints and educational resources EPIC produces;
- The quantity and reach of privacy- and AI-related enforcement actions initiated by regulators at EPIC's urging; and
- The level of participation in and collaborative outputs of EPIC-organized coalition events.

Another way we will measure progress towards our public education goals is by monitoring aggregate traffic to the EPIC website. By using privacy-protective tools to monitor page views, time on page, and bounce rate, we will be able to keep track of not only the number of people who have seen our work but also identify the content that users appear to find most engaging and useful. Additionally, we will be able to assess the public's engagement with our work by the number of people who sign up for relevant EPIC events. Finally, we can measure our reach by tracking press reporting and media citations to our work.

15. PUBLICATION

EPIC aims to make our work both accessible and digestible for all audiences. Multiple times per year, EPIC posts in-depth reports on pressing developments in the digital privacy sphere. As noted in Section 8, our latest reports have addressed screening and scoring tools, the harms posed by generative AI, and the government procurement of automated decision-making systems. The additional research and advocacy efforts made possible through a *cy pres* award will inform multiple reports that EPIC publishes over the next several years.

We also regularly publish analysis in shorter white papers and posts. Our Analysis blog, in particular, is an essential forum for sharing our work with lawmakers, journalists, and the public. One recent series of posts from EPIC staff broke down the importance of data minimization for policymakers and the public and explained the role it should play in the FTC's forthcoming commercial surveillance rulemaking. EPIC also publishes op-eds, such as this recent one in *Bloomberg Law*, which allow us to further widen the reach of our work.

We will also prioritize developing educational resources such as pamphlets, policy one-pagers, and technical reports that can be used by lawmakers and members of the public. And we will continue to create living resources like scorecards that provide viewers with up-to-date, side-by-side comparisons of relevant privacy policies, AI regulations, and the like.

This funding would also provide EPIC with a sufficient budget to create a "Privacy Protection Toolkit" for internet users. With the support of a technologist that we have budgeted for, EPIC will develop this resource on how to best protect one's personal data amid the rapid changes to commercial data practices.