Google Location History Litigation Cy Pres Award Proposal
October 24, 2023 (updated)

BACKGROUND

The Electronic Frontier Foundation was founded in response to a basic threat to speech and privacy. Several informed technologists became aware of the increasing precarity of digital liberties after the U.S. Secret Service misinterpreted a cybersecurity threat and nearly ruined an innocent small games book publisher, Steve Jackson Games. EFF's founders formally unveiled the Electronic Frontier Foundation in July of 1990, and announced they were representing Steve Jackson Games and several of the company's bulletin board users in a lawsuit against the United States Secret Service.

The Steve Jackson Games case turned out to be an extremely important one in the development of a proper legal framework for cyberspace. For the first time, a court held that electronic mail deserves at least as much protection as telephone calls. We take for granted today that law enforcement must have a warrant that particularly describes all electronic mail messages before seizing and reading them: The Steve Jackson Games case established that principle.

For over thirty years, EFF has been at the forefront of internet privacy. We have added new strategies and areas of expertise. For example, in 2022, EFF exposed Fog Data Science, a shadowy company that sells geolocation information of hundreds of millions of Americans to law enforcement agencies. We found that Fog Data Science provides law enforcement with easy and often warrantless access to the precise and continuous geolocation of hundreds of millions of Americans, collected through a wide range of smartphone apps and then aggregated by intermediary data brokers. We worked with the Associated Press for an exclusive story, which was carried by hundreds if not thousands of subscribers in English, Spanish, French, German, Polish, Chinese, and Japanese. It also generated significant secondary attention via requests for interviews at other media outlets, and an op-ed in Slate. Lawmakers from Oregon and California cited our investigation in their comments to the Federal Trade Commission urging them to investigate Fog Data Science's practices.

EFF also stays nimble to respond to emerging threats. While we have long promoted medical digital privacy, this issue became especially urgent in 2022 when the Supreme Court reversed its protection of abortions, and digital data became a key way in which governments can try to identify people seeking reproductive care. EFF created a principled guide for platforms to respect user privacy and rights to privacy in their bodily autonomy, called on nonprofit organizations to remove trackers from their websites, and worked with legislators on commonsense privacy legislation to protect not only health-related data but the full range of consumer data that could be weaponized against abortion seekers.

We have prevailed in lawsuits against the world's largest entertainment companies, major electronics companies, the federal government and the FCC, among others. (A collection of our legal victories is available at: https://www.eff.org/victories.)

CURRENT GOALS

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

Our expert team of attorneys, activists, and technologists will advance internet privacy through the following organizational goals:

- Demand widespread adoption of privacy laws and protection of end-to-end encryption.
- Prevent suspicionless, dragnet-style digital surveillance using geofence warrants.
- Challenge cyberstalking through demands to companies and policymakers.
- Foster a fair digital ecosystem that centers users by diluting tech giants' control, and advocate for decentralization that promotes competition and innovation.
- Push for better policies related to government transparency, e.g. Freedom of Information Act (FOIA) requests and litigation.
- Deliver practical digital security advice through our Surveillance Self-Defense (SSD) project.
- Guide the development of new security standards.
- Establish new—and strengthen existing—collaborations with partner organizations advancing internet privacy.

CURRENT PROGRAMS

As technology has become increasingly intertwined with even seemingly mundane aspects of our lives, EFF has been instrumental in advancing internet privacy globally. EFF continues to take on critical cases, challenge tough opponents, and achieve landmark victories. EFF also conducts ground-breaking investigations into privacy-invading technology, advocates for meaningful policy change in both the private and public sectors, creates privacy-enhancing tools, and educates the public on how to protect themselves from unnecessary surveillance. Privacy has been at the heart of EFF's work since our inception, and will continue to guide our programs going forward. EFF's current programs center on the following six interrelated issue areas:

Digital Privacy - EFF's approach to privacy enables autonomy, anonymity, security, and the right to a life free from prying eyes. This allows for free association and expression, while also taking into account legitimate law enforcement concerns. National and local governments must put legal checks in place to prevent abuse of state powers, and international bodies should consider how a changing technological environment shapes security agencies' best practices.

Security - Computer security—and the lack of it—is a fundamental issue that underpins much of how the internet does and doesn't function. EFF works on a wide range of security issues, including standing up

for encryption both in the U.S. and internationally, deploying cryptographic protocols, like HTTPS Everywhere and Certbot; offering legal assistance to researchers through our Coders' Rights Project; delivering practical security advice to activists through the Surveillance Self-Defense project; directly auditing open source codebases; and working on the development of new security standards.

International - EFF's international team advocates for privacy, free speech, and an open internet around the world. We expose mass and unwarranted surveillance and educate unlawfully targeted users on how to protect themselves and their colleagues. EFF uses individual cases to highlight the effect of technology on human rights and defend technologists from persecution and detention wherever they live.

Transparency - EFF holds governments accountable to the public through federal and state freedom of information laws, the courtroom, and our megaphone. We showcase technologies and policies that help the transparency process, such as tools that make it easier to file and track public records requests, websites dedicated to whistleblowing, or open government initiatives to improve access to information.

Creativity and Innovation - EFF works to protect and strengthen fair use, innovation, open access, net neutrality, and your freedom to tinker. Our digital future depends on our ability to access, use, and build on both information and technology. We challenge patent and copyright trolls in public and in court; argue in Congress for more balanced copyright and patent laws; and urge governments, funders, and educational institutions to adopt open access policies so established players do not silence the next generation of creators.

Free Speech Online - EFF fights for free expression offered by new technology—overcoming the legal, structural, and corporate obstacles blocking people around the world from speaking their minds and accessing information and ideas. We should be able to use new technologies to publish our ideas; criticize those in power; gather and report the news; and make, adapt, and share creative works. These rights are especially important for those in vulnerable communities, who must be able to safely meet, grow, and make themselves heard without being silenced or drowned out by the powerful.

EFF's 2022 Annual Report

CHARITY NAVIGATOR RATING

EFF has had a 100%, 4-star rating from Charity Navigator for the past 10 years.

CY PRES AWARD HISTORY

EFF's 42 *cy pres* awards since 2010 have provided $17.4 million for our general operating expenses.

Date Received	Case Name	Amount Received ($)
12/20/2010	Visa check/Master Money Antitrust Litigation Settlement	20
04/22/2011	Solvay Pharmaceuticals Litigation	210,606
12/15/2011	Weller v. Internet Brands, L.A.S.C.	50,000
12/19/2011	Google Buzz	1,022,399
05/25/2012	Valentine v. NebuAd, Inc.	197,989
06/30/2013	Classmates.com Consolidated Litigation Settlement	69,109
07/23/2013	Lagarde v. Support.com, Inc.	100,000
10/03/2013	Francisco Marenco v. Visa Inc.	65,260
11/01/2013	Intelius "Identity Protect" Class Action	4,223,839
02/14/2014	Dawn Fairchild v. AOL, LLC	37,500
10/09/2014	Netflix Cy Pres Award	497,661
02/13/2015	Grannan v. Alliant Law Group. P.C.	50,836
03/24/2015	Sabol v. Hydroxatone	71,758
07/24/2015	Francisco Marenco v. Visa Inc.	1,664
10/26/2015	Craigslist Settlement	1,000,000
03/08/2016	Martin v. Dun & Bradstreet Inc.	44,224
04/08/2016	Byanooni v Merrill Lynch	17,375
08/12/2016	Chapa v. TruGreen, Inc.	82,550
08/26/2016	Wheelock v Hyundai Motor	9,413
09/30/2016	McCabe et al, vs. Six Continents	125,870
11/23/2016	Capital One TCPA Class Settlement	1,809,938
12/31/2016	Bank of America TCPA Settlement	187,212
03/29/2017	Fraley v. Facebook Case	846,771
07/25/2017	Couser v Comenity Bank	5,983
09/26/2017	Home Depot Data Breach	971,169
01/22/2018	Computershare Inc- Ossola v. American Express Co.	96,856
01/30/2018	Ashley Madison Website Data Breach	472,671
05/21/2018	Khoday v Symantec	92,086
05/30/2018	Gehrich TCPA Settlement	402,727
06/01/2018	Zepeda v Paypal	328,084
06/10/2019	Cottage Health Settlement	239,170
06/28/2019	Opperman v. Kong	154,977
02/12/2020	Ossola v. American Express	12,676
05/13/2020	Slovin v. Sunrun	100,273
10/23/2020	Kieu Phan vs UKA's Big Saver Foods	316,565
09/08/2021	Flaum v. Doctors Associates, Inc.	1,033,469
03/22/2022	Carrier IQ	277,338
04/13/2022	Buchanan v. SiriusXM Radio	92,319
12/27/2022	Muransky v Godiva	292,139
02/07/2023	Pine v. A Place for Mom	208,743
07/14/2023	Lopez v Volusion	1,335
07/20/2023	Wang v. Wells Fargo	1,566,973
TOTAL		**17,387,547**

Grant Proposal

PROJECT DIRECTOR

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in Bernstein v. Dept. of Justice, the successful First Amendment challenge to the U.S. export restrictions on cryptography.

Ms. Cohn has been named to *The NonProfit Times 2020 Power & Influence TOP 50* list, honoring 2020's movers and shakers. In 2018, Forbes included Ms. Cohn as one of America's Top 50 Women in Tech. The National Law Journal named Ms. Cohn one of 100 most influential lawyers in America in 2013, noting: "[I]f Big Brother is watching, he better look out for Cindy Cohn." She was also named in 2006 for "rushing to the barricades wherever freedom and civil liberties are at stake online." In 2007 the National Law Journal named her one of the 50 most influential women lawyers in America. In 2010 the Intellectual Property Section of the State Bar of California awarded her its Intellectual Property Vanguard Award and in 2012 the Northern California Chapter of the Society of Professional Journalists awarded her the James Madison Freedom of Information Award.

Bios of EFF staff and board members.

PROJECT REQUEST

Our personal data and the ways private companies harvest and monetize it plays an increasingly powerful role in modern life. The protection of consumer privacy is foundational to EFF's work—from surreptitious data collection, malware installed on personal devices, smart meters, and the Internet of Things—EFF fights in the courts and Congress to maintain privacy rights in the digital world. We work with a wide range of partners to support the development of privacy-protecting policies and technologies. EFF requests general operating support of our organization for our work to promote the protection of internet privacy.

Goals and Objectives

Ongoing/Long Term

- Pass comprehensive data privacy legislation by educating the public and decision-makers.
- Support solutions that protect individual digital privacy and human rights by identifying and educating the public and decision-makers about emerging threats and best practices.
- Push standards among technology developers that center user privacy, including through creation of public interest technology and protocols.

1-3 Years (2024 – 2026)

- Push for the phasing out of third party tracking cookies, while preventing the implementation of other equally invasive technologies that may emerge.
- Educate the public on vulnerabilities in electronic health records systems.
- Call for more transparency in data collection and universal opt-out tools for internet-connected devices (such as cars) and guide the development of new privacy standards.
- Promote student privacy and access to information by addressing problematic content blockers and rapidly evolving artificial intelligence (AI) tools.
- Achieve ten or more legal and legislative victories organization-wide each year.

Activities

1. Maintain and update EFF's public interest technologies and resources:
    a. Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser seeking to track you, it's like you suddenly disappeared. Available to the public for free, Privacy Badger was the first add-on to specifically focus on blocking tracking in advertisements, instead of just the ads themselves. EFF's open-source technology has also inspired other widely used privacy tools, including the Brave browser and Safari's tracker blocking.
    b. Surveillance Self-Defense (SSD) guide provides vital information on how to use secure technology and develop careful practices. It includes tutorials for installing and using security-friendly software, and information on making a security plan, strong passwords, protecting metadata, and much more. SSD is available in 12 languages, in whole or in part.
    c. CertBot is EFF's free, open-source software tool to help websites encrypt their traffic and keep their sites secure, aims to build a web that is more structurally private, safe, and protected against censorship. In 2022, we released Certbot 2.0, and nearly 3 million new certificates were issued. Overall, there are 3.3 million installations maintaining 20 million certificates for 29.6 million domains.
    d. Encourage global privacy control (GPC) protocol to extend to other contexts, such as internet-enabled appliances and cars. Background: GPC allows users to tell companies they want to opt out of having their data shared or sold. It is simple, easy to deploy, and works well with existing privacy tools. For example, Privacy Badger sends the GPC signal to every company you interact with alongside the Do Not Track (DNT) signal. Like DNT, GPC is transmitted through an HTTP header and a new Javascript property, so every server your browser talks to and every script it runs will know that you intend to opt out of having your data shared or sold.

2. Actively engage on a range of ongoing privacy-promoting lawsuits. For example, in 2022 EFF filed a lawsuit against the Sacramento Municipal Utility District (SMUD) and Sacramento Police Department on behalf of the Asian American Liberation Network and other residents to fight an illegal data sharing practice that specifically targeted Asian Americans. The public utility searched entire zip codes' worth of private energy usage data and disclosed it to the local police department without a warrant or any individualized suspicion of wrongdoing, creating a mass surveillance program that invades the privacy of entire communities.

3. Continue advocating for comprehensive data privacy legislation and consumer data privacy laws that avoids federal preemption, ensures consumers have a private right of action, and uses non-discrimination rules to avoid pay-for-privacy schemes. See blog: "EFF's Recommendations for Consumer Data Privacy Laws (June 2019)"

4. Collaborate with grassroots organizations to advance internet privacy policies and practices from the local to federal levels via the Electronic Frontier Alliance, an information-sharing network made up of 76 member groups in 26 U.S. states and Puerto Rico.

5. Demonstrate the relevance of consumer privacy to all tech users through our existing resources (blog, podcast), as well as more emphasis on short videos and infographics. Leverage EFF's media presence and communications to advance advocacy and shape public conversations about internet privacy, including a new emphasis on using videos and infographics to reach new audiences. For example, this Deeplinks blog post: "Is Your State's Child Safety Law Unconstitutional? Try Comprehensive Data Privacy Instead" (October 2023).

APPROACH

Comprehensive data privacy legislation is the best way to hold tech companies accountable in our surveillance age, including for harm they do to children. Comprehensive data privacy legislation would address the massive collection and processing of personal data for online behavioral advertising that is the root cause of many problems online. Also, compared to age verification laws, it is far easier to write data privacy laws that are constitutional. Laws that lock online content behind age gates can almost never withstand First Amendment scrutiny because they frustrate all internet users' rights to access information and often impinge on people's right to anonymity.

Data privacy legislation has many components. At its core, it should minimize the amount of personal data that companies process, give users certain rights to control their personal data, and allow consumers to sue when the law is violated. EFF holds that privacy laws pass First Amendment muster when they have a few features that ensure the law reasonably fits its purpose. First, they regulate the commercial processing of personal data. Second, they do not impermissibly restrict the truthful publication of matters of public concern. And finally, the government's interest and law's purpose are to

protect data privacy; expand the free expression that privacy enables; and protect the security of data against insider threats, hacks, and eventual government surveillance. If so, the privacy law will be constitutional if the government shows a close fit between the law's goals and its means.

New technologies are radically advancing our freedoms, but they are also enabling unparalleled invasions of privacy. For example, cars today collect a lot more data than they used to, often leaving drivers' privacy unprotected. Advertisers, investment companies, and insurance companies are among those who want to actively collect or use vehicle and driver data to deliver and enhance their products. Cars can also collect information not only about the vehicle itself, but also about what's around the vehicle, and that data can reveal a lot about the people inside of the car. Given the sensitivity of this data and what it can reveal about individuals, companies should clearly spell out which data they collect, how that data is used, and offer individuals a meaningful option to opt out of data collection. National and international laws have yet to catch up with the evolving need for privacy that comes with new digital technologies.

As privacy needs evolve, so too should our regulatory regimes. National governments must put legal checks in place to prevent abuse of state powers, and international bodies need to consider how a changing technological environment shapes security agencies' best practices. Above all, we need to respect the rights of autonomy, anonymity, association, and expression that privacy makes possible, without undermining legitimate law enforcement.

FINANCIAL REQUEST and BENEFICIARIES

EFF requests $6 million for general operating support over 2 years or $9 million of general support over 3 years. Funding at $3 million per year represents about 20% of our annual budget for EFF's privacy-focused work discussed in this proposal for the first year. EFF has successfully managed a $6 million multi-year general support grant (2022-2024) with bi-annual reporting requirements, and we are well positioned to leverage the requested funding to amplify EFF's work and outcomes related to internet privacy.

EFF's scope is global, and our organization's work serves all tech users the world over; however, we also focus on work that will particularly benefit vulnerable populations. For example, our lawsuit against SMUD highlights that the illegal data sharing program specifically targeted Asian Americans. EFF also holds that data surveillance is a civil rights problem, and legislation to protect data privacy can help protect civil rights. Lower-income people are often less able to avoid corporate harvesting of their data. See our 5/18/23 blog post "Digital Privacy Legislation is Civil Rights Legislation," which is available in 10 languages.

Additionally, in 2023 EFF, the Knight Institute, and Social Justice Legal Foundation filed a lawsuit against San Mateo County on behalf of incarcerated people, their nonincarcerated loved ones, and a collective of artists supporting incarcerated members of the LGBTQ community in response to its 2021 policy that

banned anyone incarcerated in its jails from receiving any physical mail other than attorney communications. Under this policy, senders of mail must route their letters to Smart Communications, a private for-profit company, which scans and then destroys the physical copy. The digital copy is stored for a minimum of seven years, even when the intended recipient is released or found innocent before that time. Incarcerated people are only able to access the digital copies through a limited number of shared tablets and kiosks in public spaces within the jails. This policy invades the privacy of those imprisoned in the jails as well as everyone who corresponds with them through physical mail, including family, friends, and religious and support organizations. In addition to the contents of the mail, Smart Communications also collects a variety of other information not directly included in the mail, including details about the sender. Anyone that San Mateo County provides credentials to can access all of this information. Concerns about this invasive surveillance have led many people to stop corresponding by mail altogether, even though countless studies have shown that letter-writing reduces recidivism and increases successful reentries into society upon release.

Meanwhile, our work to end stalkerware benefits survivors and potential victims of domestic violence. According to President Biden's September 2023 Proclamation on National Domestic Violence Awareness and Prevention Month, "4 in 10 American women and nearly 3 in 10 American men are still impacted by sexual abuse, physical violence, or stalking by an intimate partner at some point in their lifetimes."

Finally, EFF has a long history of defending human rights activists, such as a lawsuit we filed in 2021 representing prominent Saudi human rights activist Loujain AlHathloul against spying software maker DarkMatter Group and three of its former executives for illegally hacking her iPhone to secretly track her communications and whereabouts. The information obtained from the hack while she was in the U.S. later led to Loujain's imprisonment and torture by the Saudi government.

EVALUATION

EFF agrees to provide a report on EFF's privacy activities supported by the Settlement Fund to the Court and the parties every six months for the duration of this grant. EFF's chief development officer Allison Morris, associate director of institutional support Mei Harrison, PhD, and institutional support coordinator Tierney Hamilton will provide oversight and administrative support for the grant, including written reporting. EFF's chief financial officer Kelly Esguerra will generate any required financial reports.

We measure our impact through legal and legislative victories, the efficacy of our activism, media reach, and the wide implementation of our public interest technology tools. Aside from outright legal wins, a key indicator of our success is whether court decisions are consistent with our positions on privacy, free speech, and other Constitutional values. EFF has also fought for many years to end government efforts to undermine encryption and security, and we will continue to do so until comprehensive privacy legislation that preserves encryption becomes law. This is also true of our contributions to global conversations regarding internet privacy standards—a right to privacy should be enshrined into international law. Within the private sector, the voluntary implementation of basic privacy protections by corporations, as

we saw with Google and Apple collaborating on efforts to detect unwanted location trackers which are misused in stalking and abuse, is the kind of response to our activism we hope to see more of.

PUBLICATIONS and PRESENTATIONS

EFF will share the results of our privacy promoting work publicly through several avenues, including publications of our Deeplinks blog, as well as presentations at cybersecurity, human rights, and dozens of other conferences and events throughout the year, including DefCon, Black Hat, and RightsCon, "the world's leading summit on human rights in the digital age" hosted by Access Now. Partial listing of upcoming and past events , such as EFF Executive Director Cindy Cohn and Legislative Director Lee Tien presenting at the October 2023 Berkeley Law Symposium "California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age." According to organizers, "The symposium will bring together leading academics and practitioners to explore the landscape of California's constitutional right to privacy at age 50, highlight how the right is currently used to promote racial justice and other social progress, and discuss new creative and intersectional uses of state constitutional rights to privacy to defend and promote justice in the digital age."

EFF reaches millions of people worldwide. In 2022, we had nearly 20,000 press mentions globally, or an average of 78 per day, along with a following of nearly half a million subscribers to our EFFector newsletter and 28 million page views (for EFF.org, our Action page, and several other websites we host). EFF experts were cited in a range of issues in The New York Times, CNN, NPR, Vice, USA Today, The Guardian, The Washington Post, and dozens of local news outlets. EFF's "How to Fix the Internet" podcast was downloaded in 154 countries. The podcast featured episodes on topics including "Securing the Internet of Things" with guest Window Snyder, founder and CEO of Thistle Technologies. We recently started compiling sizzle reels sampling some of the many TV appearances EFF staff made in 2022 and 2023.

Contacts:

(Pam) Mei Harrison, PhD
Associate Director of Institutional Support
415-436-9333 x128
Mei@eff.org

Cindy Cohn
Executive Director
Cindy@eff.org

Allison Morris
Chief Development Officer
Allison@eff.org