For over 100 years, the American Civil Liberties Union (ACLU) has been our nation's guardian of liberty, working on all fronts to defend and preserve the individual rights and liberties guaranteed by the Constitution and the laws of the United States.

BACKGROUND

1. NAME

American Civil Liberties Union Foundation (ACLU)

2. FOUNDING AND HISTORY

Since litigating *ACLU v. Reno* (1997), which helped establish the free and open internet, the ACLU[1] has been a leader in ensuring that as technology advances, rights to privacy and other civil liberties also evolve. The ACLU's Speech, Privacy, and Technology (SPT) Project—based in New York, with offices in San Francisco and Washington, D.C.—formalizes our commitment to ensuring that civil liberties are enhanced rather than compromised by new advances in science and technology.

We have been particularly successful in our recent work to protect digital and locational privacy. For example:

- The ACLU has spearheaded the challenge to warrantless location tracking by means of cellphones, culminating in our win before the U.S. Supreme Court in *Carpenter v. United States*, in which the court held that law enforcement must obtain warrants before demanding cellphone companies to hand over information about where their customers have been and when. *Carpenter* is widely considered the most consequential Supreme Court Fourth Amendment decision in the digital age, and we have been working to expand protections against warrantless surveillance in other contexts. For example, we, the ACLU of Virginia, along with eight Federal Public Defender offices, filed an amicus brief in *United States v. Chatrie*, the first "geofence" search case to reach a federal court of appeals. In the brief, the ACLU asserts that police should not be able to exploit the evidence they acquired from a geofence warrant, a novel and invasive surveillance technique that enables law enforcement to search for and locate

[1] The "ACLU" comprises two related entities with a shared mission: the American Civil Liberties Union, a 501(c)(4) nonprofit organization, and the ACLU Foundation, a 501(c)(3) nonprofit organization. The former engages primarily in lobbying, and the latter engages primarily in litigation, public education, and other nonlegislative advocacy. Although this application mentions some (c)(4) work to show the breadth of our program, the entity making the request is the ACLU Foundation, and any funding would be used entirely for (c)(3) work.

unknown numbers of people in a large area without reason to believe they were engaged in criminal conduct.

- The ACLU helped bring automated license plate readers to public consciousness through a massive, coordinated public records request spanning local law enforcement in 38 states and numerous federal agencies that informed a groundbreaking report.
- The ACLU helped expose and challenge law enforcement's secrecy about the use of international mobile subscriber identity-catchers, or IMSI-catchers (of which Harris Corporation's "Stingray" is the best-known example). These devices can pinpoint the locations of suspects and innocent bystanders alike, as well as interfere with local cell service. We discovered that some local law enforcement agencies concealed stingray use through confidentiality agreements with the manufacturer, equivocal applications to judges, and coordination with federal law enforcement.
- The ACLU's early and thoughtful positions on COVID-19-related digital "proximity tracing" informed all major media on the topic, helping to render it a virtual nonstarter. Our numerous reports and media appearances set clear guideposts for any future proximity-tracking approach.
- We won an en banc 4th Circuit decision holding that Baltimore Police Department's aerial surveillance program, which put the daytime movements of virtually all Baltimore residents under surveillance for 12 hours a day over six months, was unconstitutional.
- We have filed amicus briefs in numerous cases where criminal defendants have challenged government access to their location information in violation of the Fourth Amendment, including cases involving real-time cellphone tracking, so-called geofence warrants, wi-fi–derived location information, automated license plate reader data, and IMSI-catchers.
- We have worked in courts to defend and enforce privacy statutes that restrict abuses by private corporations, including Maine's unique internet service provider privacy law and Illinois' unique Biometric Information Privacy Act.
- Last year, we published thousands of pages of previously unreleased records about how Customs and Border Protection, Immigration and Customs Enforcement, and other parts of the Department of Homeland Security are sidestepping our Fourth Amendment right against unreasonable government searches and seizures by buying access to, and using, huge volumes of people's cellphone location information quietly extracted from smartphone apps.
- This January, we exposed one of the largest government surveillance programs in recent memory: a huge database of 145 million-plus financial transactions assembled through overly broad, and illegal, subpoenas to money transfer companies issued by the Arizona attorney general. The database gave virtually unfettered access to this information to thousands of officers from hundreds of law enforcement agencies across the country. Our exposé followed records requests

submitted by the ACLU and ACLU of Arizona, and we published more than 200 of the resulting documents online.

- Since August, we have helped temporarily block state laws in Arkansas and Texas that would essentially "card" users to access certain websites. We filed amicus briefs with other leading privacy organizations in both cases and have explained to the public why such measures rob users of anonymity, pose privacy and security risks, and could be used to block some people from being able to use some internet services at all.

The ACLU is also recognized on other cutting-edge privacy issues, including facial recognition, biometrics, and various artificial intelligence (AI) and "big data"-driven surveillance approaches. The ACLU work in these areas combines the expertise of litigators, communications and policy experts, technologists, data scientists, and others.

3./4. CURRENT GOALS & PROGRAMS

The ACLU currently has four strategic goals around digital privacy shared by our legal department (primarily SPT[2]) along with teams in our Communications, Analytics, National Political Advocacy, and Affiliate Support departments. All four of these goals touch upon internet privacy and security, as well as locational privacy.

The goals are to:

- Bring the Fourth Amendment into the 21st century by reforming or eliminating the third-party doctrine and ending warrantless and overbroad electronic searches;
- Defend secure communications and expand right to communications privacy;
- Ensure that artificial intelligence-enabled and biometric surveillance technologies are meaningfully constrained by law and policy; and
- Ensure that advances in AI, big data, and automated decision-making do not undermine civil rights and civil liberties.

5. CY PRES EXPERIENCE

The ACLU has a long history of being approved for cy pres funding. Most recently, we received $1,006,582.88 from the Google Street View settlement (2023). Other recent cy pres awards include:

- $221,518.98 from Everi Digital via Angeion Group (2022);
- $12,199.96 from Amcor Rigid Plastics (2021); and
- $407,315.57 from Nesbitt's Fair Credit Reporting Act settlement fund (2018).

[2] SPT has goals related to free speech and technology in addition to those listed above, and the ACLU has 14 legal teams working on other sometimes overlapping issue areas. We anticipate using any cy pres award solely for the work described in this application.

6. EXTERNAL RATINGS

The American Civil Liberties Union Foundation has a four-star 99% rating from Charity Navigator, an "A" grade from CharityWatch, and is accredited by the BBB Wise Giving Alliance. We also participate in the Combined Federal Campaign, the world's largest annual workplace charity program.

GRANT PROPOSAL

7. PROJECT DIRECTOR

Ben Wizner, director of the ACLU Speech, Privacy, and Technology Project

bwizner@aclu.org / (212) 519-7860.

Brief bios of Ben and other key staff for the proposed work follow.

8./9. SUMMARY OF REQUEST AND APPROACH

All funds would be used to support the internet privacy and security work of the ACLU's Speech, Privacy, and Technology Project. We would also expect to share the award to support complementary work by a handful of ACLU affiliates, were we to receive an award at the high end of our funding request range.

The practices at issue in the Google Location History Litigation illustrate a problem the ACLU has long addressed: the leaking—and in some case, siphoning—of data users wrongly assume to be private, inaccessible, or "safe." It is perhaps the most fundamental challenge in applying the protections of the Fourth Amendment to the digital age. Because there are so many weak links in this chain, the ACLU approaches internet privacy and security through a multifront approach—combining litigation, records requests, public education, advocacy before companies and internet standards-setting bodies, and separately funded state and federal lobbying—precisely because we have found this approach to be most successful. Indeed, our most impactful successes over the past few years have resulted from work on two or more fronts. For example:

- This June, we revealed that the FBI has continued to force state and local law enforcement agencies to sign nondisclosure agreements (NDAs) if they want to use the FBI's cell site simulators (sometimes known as stingray devices), which enable users to track cellphone users' locations. The troubling NDAs prohibit the disclosure of their use to the public and to the courts and even require withholding of information about the devices, their functionality, and deployment from defendants and their lawyers in criminal cases, which undermines people's constitutional right to mount a defense. We also published the documents behind our findings, which we obtained through a Freedom of Information Act request and related litigation. This is merely the latest exposé in over a decade of ACLU work documenting location-tracking technologies and their abuse by law enforcement.

- In November, we submitted 47 pages of comments in response to the Federal Trade Commission's call for input from the public about "whether new rules are needed to protect people's privacy and information in the commercial surveillance economy." With the ACLU's broad expertise touching upon privacy, commercial speech, and algorithmic discrimination, among other areas—within and beyond SPT—our positions are unusually detailed, informed, and weighty. We note support for "FTC rulemaking to rein in commercial surveillance, not by burdening users with the impossible task of managing their own data as it flows through the complex web of advertisers, data brokers, government agencies, and other parties who buy and sell it for their own benefit, but by changing the paradigm and demanding that companies collect and use consumer data in service of consumers. Strong rules that go beyond the "notice-and-choice" paradigm are the only way to address the serious harms that consumers experience under the current abusive system of commercial surveillance."

No other organization combines the expertise, programmatic capacity, and 50-state reach the ACLU has on these issues. An award at or near the request level below would support a significant part of our internet privacy and security work for up to three years.

10./11. FUNDING REQUEST AND USE

We respectfully request a $9 million cy pres award. This funding would support ongoing and robust internet privacy and security work by the ACLU over three years, including by hiring additional technologists to work alongside lawyers to advance this work.

We expect to regrant approximately one sixth of an award to several state-based ACLU affiliates to build the capacity of their existing programs to improve internet privacy and security. Among the affiliates we anticipate might receive funding are the ACLU of Colorado, the ACLU of Illinois, the ACLU of Massachusetts, the ACLU of New Jersey, the New York Civil Liberties Union, and the ACLU of Washington. (Please note that the ACLU of California, an undoubted leader in this area, is submitting a separate cy pres application at the invitation of counsel.)

The need to engage technologists in the public interest is clear. Technological advances have been far outstripping controls on their use, whether legal, practical, or financial. Few policymakers—let alone the public—understand the underlying technologies. And those who do understand the technologies disproportionately work for the very government and corporate actors most interested in exploiting weaknesses in our digital security. As a result, technological capability has been driving policy. The result is a proliferation of overbroad watch lists, dragnet surveillance programs, location and behavioral tracking, and colossal data-mining schemes.

ACLU technologists will advise our legal and policy work, inform and empower the public on technology issues, and seek technical solutions to problems hard to solve through legal or policy channels. This project will also help solidify a genuine career path for technologists who wish to work in the public interest—a field the ACLU helped to pioneer over a decade ago with the support of the Ford Foundation. We have had at least one technologist on staff since 2012 and have served as a critical pipeline for numerous tech

fellows from various privacy-related disciplines, including cryptography, genetics, and cybersecurity. Capacity-building made possible by an award would steer promising young technologists toward protecting the privacy and security of the internet we all depend upon.

12. TARGET POPULATION

The primary target population consists of all "U.S. persons"—that is, U.S. citizens, wherever in the world they reside, as well as any individual residing within the United States. However, aspects of our work will likely benefit the privacy and security of non-U.S. internet users as well.

EVALUATION

13. REPORTS

Should it receive a cy pres award, the ACLU agrees to provide a report every six months to the court and the parties informing them of how any settlement fund monies have been used and any remaining funds will be used.

14. EVALUATION

The success of the grant will be assessed in an ongoing basis at SPT's biweekly meetings, and as part of a formal look back/look forward process SPT engages in every year. It will also be assessed as part of a formal look back/look forward process the ACLU engages in for our organizational priorities. We will evaluate project success primarily by looking at whether we achieved tangible new protections for internet privacy and security. Such protections could be heightened legal standards to access users' data; deployment of more private and secure protocols at the internet infrastructure level; wider adoption of corporate best practices for data retention and storage; improved agency regulations; or other constraints of law, policy, or practice that preserve users' privacy and security. We will also gauge the success of the ACLU's public education efforts through blog posts, op-eds, and earned media.

15. PUBLICATION

Our project focuses on policies, legal standards, and technical solutions for data privacy and security rather than the data itself. We expect to promulgate court victories, positions on best practices, and/or new technical standards, and to educate the public and businesses about risks to privacy and security and how to mitigate them. This information will be disseminated through the ACLU's blog, our extensive social media reach, and media coverage, and any changes to agency policies or legal standards will be published in the Federal Register (or state counterparts) or court opinions. Depending on circumstances and funding level, we may also publish a report or white paper on a relevant privacy/security issue.

SPEECH, PRIVACY, AND TECHNOLOGY PROJECT (SPT) KEY STAFF

BEN WIZNER, DIRECTOR

Ben Wizner is the director of SPT. For more than 20 years, he has worked at the intersection of civil liberties and national security, litigating numerous cases involving airport security policies, government watch lists, surveillance practices, targeted killing, and torture. He appears regularly in the global media, has testified before Congress, and is an adjunct professor at New York University School of Law. Since July of 2013, he has been the principal legal advisor to National Security Agency whistleblower Edward Snowden. Ben is a graduate of Harvard College and New York University School of Law and was a law clerk to Stephen Reinhardt of the U.S. Court of Appeals for the 9th Circuit. Ben has roughly tripled SPT's size during his tenure, as well as overseen the ACLU's participation in nearly every major Supreme Court case involving privacy rights in the digital age.

ESHA BANDHARI, DEPUTY DIRECTOR

Esha Bhandari is deputy director of SPT, where she works on litigation and advocacy to protect freedom of expression and privacy rights in the digital age. She also focuses on the impact of big data and artificial intelligence on civil liberties. She has litigated cases including *Sandvig* v. *Barr*, a First Amendment challenge to the Computer Fraud and Abuse Act on behalf of researchers who test for housing and employment discrimination online, *Alasaad* v. *Wolf*, a constitutional challenge to suspicionless electronic device searches at the U.S. border, and *Guan* v. *Mayorkas*, a First Amendment case on behalf of journalists questioned about their work by border officers. She argued *United States* v. *Hansen*, a First Amendment case, before the Supreme Court.

Esha was previously an Equal Justice Works fellow with the ACLU Immigrants' Rights Project, where she litigated cases concerning a right to counsel in immigration proceedings and immigration detainer policies. Esha is a graduate of McGill University, where she was a Loran scholar and received the Allen Oliver Gold Medal in political science; the Columbia University Graduate School of Journalism; and Columbia Law School, where she received the Robert Noxon Toppan prize in constitutional law and the Archie O. Dawson prize for advocacy. She served as a law clerk to Amalya L. Kearse of the U.S. Court of Appeals for the 2nd Circuit. Esha is also an adjunct professor of clinical law at New York University School of Law, where she co-teaches the Technology, Law, and Policy Clinic.

NATE WESSLER, DEPUTY DIRECTOR

Nathan Freed Wessler is a deputy director with SPT, where he focuses on litigation and advocacy around surveillance and privacy issues, including government searches of electronic devices, requests for sensitive data held by third parties, and use of surveillance technologies. In 2017, he argued *Carpenter v. United States* in the U.S.

Supreme Court, a case that established that the Fourth Amendment requires law enforcement to get a search warrant before requesting cellphone location data from a person's cellular service provider. Nate is one of is one of the nation's leading attorneys on privacy and surveillance issues.

Nate was previously a staff attorney with SPT and legal fellow in the ACLU National Security Project (NSP). Prior to that, he served as a law clerk to Helene N. White of the U.S. Court of Appeals for the 6th Circuit. Nate is a graduate of Swarthmore College and New York University School of Law, where he was a Root-Tilden-Kern public interest scholar. Before law school, he worked as a field organizer in the ACLU's Washington Legislative Office.

DANIEL KAHN GILLMOR, SENIOR STAFF TECHNOLOGIST

Daniel Kahn Gillmor is a senior staff technologist for SPT, focused on the way our technical infrastructure shapes society and impacts civil liberties.

As a free software developer and member of the Debian project, he contributes to fundamental tools that shape the possibilities of our information-rich environment. As a participant in the Internet Engineering Task Force, he fosters the creation of new generations of networking and cryptographic protocols designed and optimized for privacy and security He is an anti-surveillance advocate for privacy, justice, free speech, and data sovereignty. Daniel is a graduate of Brown University's computer science program.

JENNIFER GRANICK, SURVEILLANCE AND CYBERSECURITY COUNSEL

Jennifer Granick fights for civil liberties in an age of massive surveillance and powerful digital technology. As the surveillance and cybersecurity counsel with SPT, she litigates, speaks, and writes about privacy, security, technology, and constitutional rights. Granick is the author of the book *American Spies: Modern Surveillance, Why You Should Care, and What To Do About It*, published by Cambridge Press, and winner of the 2016 Palmer Civil Liberties Prize.

Granick spent much of her career helping create Stanford Law School's Center for Internet and Society (CIS). From 2001 to 2007, she was executive director of CIS and founded the Cyberlaw Clinic, where she supervised students in working on some of the most important cyberlaw cases that took place during her tenure. For example, she was the primary crafter of a 2006 exception to the Digital Millennium Copyright Act that allows mobile telephone owners to legally circumvent the firmware locking their device to a single carrier. From 2012 to 2017, Granick was civil liberties director specializing in and teaching surveillance law, cybersecurity, encryption policy, and the Fourth Amendment. In that capacity, she has published widely on U.S. government surveillance practices and helped educate judges and congressional staffers on these issues. Granick also served as the civil liberties director at the Electronic Frontier Foundation from 2007 to 2010.

Earlier in her career, Granick spent almost a decade practicing criminal defense law in California. Granick's work is well-known in privacy and security circles. Her keynote,

"Lifecycle of the Revolution" for the 2015 Black Hat USA security conference electrified and depressed the audience in equal measure. In March of 2016, she received Duo Security's Women in Security Academic Award for her expertise in the field as well as her direction and guidance for young women in the security industry. Sen. Ron Wyden (D-Ore.) has called Granick an "NBA all-star of surveillance law."

BRETT MAX KAUFMAN, SENIOR STAFF ATTORNEY

Brett Max Kaufman is a senior staff attorney in the ACLU's Center for Democracy working with SPT and NSP on a variety of issues related to national security, technology, surveillance, privacy, and First Amendment rights. He has litigated cases including *ACLU v. Clapper*, a challenge to the National Security Agency's mass call-tracking program, and *Leaders of a Beautiful Struggle v. Baltimore Police Department*, a challenge to Baltimore's mass aerial surveillance program. He joined the ACLU as a legal fellow from 2012 to 2014, then spent one year as a teaching fellow in the Technology Law & Policy Clinic at New York University School of Law, where he continued to serve as an adjunct professor of law from 2015 to 2022. He returned to the ACLU in 2015 and is also an adjunct lecturer at UCLA School of Law.

Brett is a graduate of Stanford University and the University of Texas School of Law, where he was book review editor of the *Texas Law Review* and a human rights scholar at the Rapoport Center for Human Rights and Justice. After law school, he served as a foreign law clerk to Justice Asher Dan Grunis of the Supreme Court of Israel and later clerked for Robert D. Sack of the Court of Appeals for the 2nd Circuit, and for Judge Richard J. Holwell and (after Judge Holwell's resignation) Judge Lewis A. Kaplan of the U.S. District Court for the Southern District of New York.

JAY STANLEY, SENIOR POLICY ANALYST

Jay Stanley is senior policy analyst with SPT, where he researches, writes, and speaks about technology-related privacy and civil liberties issues and their future. He has authored and co-authored a variety of influential ACLU reports on privacy and technology topics, including digital driver's licenses, digital cash, and the impact of AI and video analytics on privacy. Before joining the ACLU, he was an analyst at the technology research firm Forrester, served as American politics editor of Facts on File's World News Digest, and was a national newswire editor at Medialink. He is a graduate of Williams College and holds an M.A. in American history from the University of Virginia.

American Civil Liberties Union Foundation

"Protecting Internet Privacy and Security" Three-Year Budget

November 1, 2023 - October 31, 2026

	Year 1 (11/1/23 - 10/31/24)	Year 2 (11/1/24 - 10/31/25)	Year 3 (11/1/25 - 10/31/26)	TOTAL
Personnel Costs				
Salaries[1]	1,462,000	1,462,000	1,462,000	4,386,000
Fringe Benefits	380,000	380,000	380,000	1,140,000
Program Costs				
Litigation Costs	75,000	75,000	75,000	225,000
ACLU Affiliate Grants	500,000	500,000	500,000	1,500,000
Professional Services/Contracts	50,000	50,000	50,000	150,000
Office Costs				
Rent & Occupancy Costs	85,000	85,000	85,000	255,000
Office, Equipment & Technology[2]	100,000	100,000	100,000	300,000
Administrative Costs[3]	348,000	348,000	348,000	1,044,000
TOTAL EXPENSES	**$ 3,000,000**	**$ 3,000,000**	**$ 3,000,000**	**$ 9,000,000**

1 Personnel costs include percentages of time spent by the ACLU Speech, Privacy & Technology Project staff, ACLU Communications staff, and ACLU Advocacy staff on internet privacy and security work.

2 Includes IT, web, equipment, phones, legal research, insurance and related costs.

3 Administrative costs are determined by our most recent financial statements and include time dedicated to this project by the Executive, Finance, Development, and Human Resources Departments.