Data Privacy and Security

An ACLU application for cy pres funding

ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties guaranteed by the Constitution and the laws of the United States.

Since litigating *ACLU v. Reno* (1997), which helped establish the free and open internet that many now take for granted, the ACLU has been the country's leading nonprofit organization protecting free speech, privacy, and other civil liberties at the intersection of law and technology. As technology has advanced, we have aggressively sought to ensure that the rights to privacy and freedom of expression have evolved with it—and we have been quite successful. Over the past few years, for example:

- We won what is widely considered the most significant U.S. Supreme Court decision on privacy in the digital age, *U.S. v. Carpenter*. The victory marked the culmination of years of ACLU investigation, litigation, and public education around cell phone location tracking.
- The ACLU-led Community Control Over Police Surveillance campaign has helped to secure privacy-protecting laws or ordinances in 13 communities, including San Francisco's landmark ordinance banning face surveillance and restoring democratic control over other technologies, and Maine's groundbreaking new law on internet service provider privacy.
- We secured a historic settlement agreement with Facebook that prevents advertisers from being able to exclude users from learning about opportunities for housing, employment, or credit based on gender, age, or other protected characteristics.
- We helped to achieve a new policy from U.S. Customs and Border Protection (CBP), stating that officers at the border must have reasonable suspicion of unlawful activity or a national security concern before they can conduct an "advanced" search of the contents of an electronic device.
- Advocacy by the ACLU of California resulted in the first transparency reports by T-Mobile and Amazon, and led Twitter, Facebook, and Instagram to suspend access of user data to Geofeedia, a company that marketed its platform to law enforcement as a tool to monitor activists and protesters.
- A primer by the ACLU of California, *Privacy & Free Speech: It's Good for Business*, includes over 100 case studies and cutting-edge recommendations to help businesses build privacy and free speech protections into their products and business plans.
- We have released several widely covered reports to educate the public and policymakers on privacy issues. For example:

- In June 2019, we released a report on video analytics—all the ways in addition to face recognition that artificial intelligence (AI) can be used to analyze and monitor video surveillance cameras. AI can be used to identify our unique walks, social connections, emotional states, or "suspicious" behaviors. Plugged into our existing "dumb" network of surveillance cameras—the most extensive in the world, per capita—AI could create a truly dystopian future that chills free speech and all but eliminates privacy. We provide concrete recommendations to avoid such an outcome in our report.
- In June 2018, we released a report on malicious software updates, a tactic governments could use—and have tried to use—to help them with surveillance. The report includes recommendations for companies and software developers to protect themselves and their clients from such moves, which threaten everyone's security, since they discourage people from applying legitimate software updates.
- In March 2018, we released a report on municipal Wi Fi service as a means to provide privacy, net neutrality, and wider internet access to communities nationwide. The report explains the public internet option, describes various models for implementing it, and recommends core principles to which municipal Wi-Fi service should adhere.

- ACLU engagement with internet standards-setting bodies has helped to secure privacy- and security-improving advancements to two of the core technologies powering the internet, transport layer security (TLS) and the domain name service (DNS).

ORGANIZATION INFORMATION

1. Name

American Civil Liberties Union Foundation, Inc. [13-6213516]

2. Founding and Development

Since 1920, the ACLU[1] has been devoted to protecting the civil liberties of all people in the United States. We work daily in courts, legislatures, and local communities to defend and preserve the freedoms guaranteed by the U.S. Constitution, state and federal civil rights laws, and international rights treaties by which the United States is bound.

[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.

The ACLU is one of America's largest, oldest, and best-known civil society organizations, with ACLU affiliate organizations in every U.S. state, Puerto Rico, and Washington, D.C. We receive no government funding. Since November 2016, the number of ACLU members has tripled to 1.5 million individuals, our consolidated budget (ACLU plus ACLU Foundation) has nearly doubled, and our staff has increased both in number (40 percent) and in diversity. The ACLU litigates more cases before the U.S. Supreme Court than any other nongovernmental organization and engages in policy advocacy in Congress and every U.S. state. The ACLU is a founding member of the International Network of Civil Liberties Organizations, and we engage with international human rights bodies to advance our values.

In 2010, our longstanding Technology and Liberty Project became the Speech, Privacy, and Technology (SPT) Project, formalizing our commitment to these issues and recognizing their interdependence. SPT is dedicated to protecting and expanding the freedoms of expression, association, and inquiry; expanding the right to privacy and increasing the control that individuals have over their personal information; and ensuring that civil liberties are enhanced rather than compromised by new advances in science and technology. SPT is headquartered in New York City, with additional staff in San Francisco and Washington, D.C.

3. Current Goals

Although the ACLU works on a wide range of civil rights and liberties (see Current Programs below), digital privacy is one of only six organization-wide goals, along with criminal justice reform, immigrants' rights, LGBT equality, reproductive freedom, and voting rights.

SPT's current goals are:

- Reforming the third-party doctrine and ending warrantless electronic searches;
- Enabling secure and private communications;
- Ending dragnet surveillance;
- Improving cybersecurity through engagement with internet standards-setting bodies; and
- Ensuring that biometric- and AI-driven surveillance technologies are implemented with democratic oversight and in ways that respect civil rights and liberties.
- Ensuring that traditional free speech rights evolve with our increasingly digital lives; and
- Protecting journalists, sources, and press freedom.

4. Current Programs

In addition to SPT, the ACLU has 13 other teams organized around advancing our rights and liberties within specific, sometimes overlapping areas. These teams include our Capital Punishment Project, Criminal Law Reform Project, Disability Rights Program,

Human Rights Program, Immigrants' Rights Project, LGBT & HIV Project, National Security Project, Prisoners' Rights Project, Project on Freedom of Religion and Belief, Racial Justice Program, Reproductive Freedom Project, Voting Rights Project, and Women's Rights Project.

GRANT PROPOSAL

5. Project Director

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

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

6. Request Range

We request funds totaling between $750,000 and $1.5 million. The budget we include under Use of Funds (#12) below assumes a grant roughly in the middle of this range, which we could scale up or down accordingly. Funding at the low end would support substantial privacy and security work by the ACLU and ACLU of California, the largest state-based affiliate and a leader on data privacy, surveillance, and digital security issues. Funding at the high end would ensure that our privacy and security work is fully funded and robust, greatly support complementary work by the ACLU of California, and enable the national ACLU to hire additional staff to coordinate and expand our work on ensuring that advances in AI and machine learning do not further erode privacy rights.

7. Summary

For the first time in human history, it is technologically and financially feasible for governments and corporations to record and store nearly complete records of human lives—our communications, our movements, our associations, and more. For the most part, the law has not kept pace with these profound changes.

Our work is aimed at bridging that gap, and we have had successes. In three recent cases—including *Carpenter*, in which the ACLU was counsel—the Supreme Court has recognized that advances in surveillance technology require a reconsideration of the Fourth Amendment. For the first time in a generation, Congress is seriously considering new privacy legislation to protect consumers from the abuses of large technology companies. And the public has woken up to these threats, demanding a say over the deployment of new surveillance technologies, and even calling for a moratorium on some, like facial recognition.

At the same time, rapid advances in artificial intelligence and machine learning are presenting grave new threats to privacy and related rights. The increasing adoption of AI in both public and private decisions means that engaging with algorithmic systems is crucial to protecting civil rights and civil liberties in the 21st century. The ACLU is uniquely well-positioned to address these issues. It is the only organization that possesses deep expertise on both the impacts of digital systems and surveillance on

liberty, and the impacts of big-data driven tools on equality. ACLU attorneys and technologists also work at the intersection of these technology-driven concerns, seeking to protect the rights of those often most harmed by the hasty adoption of new systems—members of groups already marginalized by discrimination and exclusion. Additional resources will allow us to grow this work and provide guidance and direction to partner organizations.

Initial areas of focus will include facial recognition tools, predictive policing, surveillance by private vendors in public schools, and employers' use of software in hiring.

All of SPT's privacy goals and the ACLU's organization-wide digital privacy priority reflect a commitment to protecting the privacy and security of data. While the ACLU's commitment to digital privacy and security is enduring, the areas in which we expect to focus our efforts over the next two years are described below under #11, Major Goals and Objectives of Project.

8. Approach

The ACLU is approaching data 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, most of our most impactful successes over the past few years in protecting data privacy and security have resulted from work on two or more fronts.

9. Support

At the low end of our requested support range, funds would help the ACLU continue critical efforts on data privacy and security, including litigation; public records requests and lawsuits; work with internet standards-setting bodies; and advocacy to encourage best practices by companies. At the high end, support would enable us to grow and enhance our work considerably, most notably through the addition of staff to coordinate and expand our work on the unique threats to privacy posed by AI and machine learning. Rapid advances in facial recognition technologies have been the most visible manifestation of this development, but, as our recent report on video analytics demonstrates, there will be many others, and it is imperative that we impose legal and ethical restraints on these emerging technologies.

10. Enhancements to Internet Privacy and Security

We expect our multifront efforts to enhance internet privacy and security, as well as other digital privacy and security, in complementary ways.

Litigation can lead to protective new legal standards. For example, our win in *Carpenter* requires law enforcement agencies to obtain warrants based on probable cause before requesting historical cell phone location data and sets the stage to extend this requirement to other sensitive digital information, such as prescription drug information. However, litigation–and even public records requests—can help achieve policy changes even apart from the legal outcome of a case. For example, the U.S. Department of

Justice and U.S. Department of Homeland Security (DHS) formalized new policies requiring probable cause warrants before using cell-site simulators following ACLU litigation. Likewise, CBP's reasonable suspicion standard for forensic device searches follows ACLU litigation. Together these policies protect the privacy of thousands of people's data—as well as their security, since numerous recent breaches illustrate the government's failure to keep its own surveillance data safe. Other policy changes we are pursuing—such as a warrant requirement for law enforcement to access data from prescription drug databases—could benefit millions of additional individuals.

Advocacy before internet standards-setting bodies can have a huge impact. For example, potentially many millions of people worldwide benefit from the contributions of the ACLU to the latest revision of transport layer security 1.3 (TLS 1.3), DNS privacy, and secure email.

Public education can not only inform, but also mobilize individuals and businesses to act. ACLU videos on privacy and technology have been viewed millions of times, for example, and the ACLU of California's primer *Privacy and Free Speech: It's Good for Business* offers numerous concrete recommendations to help companies protect their customers and bottom lines.

Engagement with companies—often alongside the other avenues of work—carries the potential to benefit millions of people at once. For example, advocacy by the ACLU and ACLU of California have led to Google's commitment not to sell face surveillance technologies to governments and to Microsoft's call for legislation governing it, as well as the introduction of transparency reports by T-Mobile and Amazon and major social media platforms suspending Geofeedia's access to user data.

11. Major Goals and Objectives of Project

Our data privacy and security work currently falls within four major areas, each with its own goals and objectives.

REFORMING THE THIRD-PARTY DOCTRINE AND ENDING WARRANTLESS ELECTRONIC SEARCHES

A central pillar of our privacy work has been to bring the Fourth Amendment into the 21st century by reforming or eliminating the "third-party doctrine," which denies constitutional protection to data shared with a third party. We struck a major blow to the doctrine in June 2018, when the Supreme Court ruled in *Carpenter* that law enforcement must obtain warrants before demanding that cell phone companies hand over information showing where their customers have been and when. In addition to recognizing the need to protect the highly sensitive location data on cell phones, the decision provides a path forward for safeguarding other sensitive digital information in future contexts. We have since been involved in litigation to establish more widely that law enforcement needs warrants to mine sensitive personal location data beyond just historical cell phone records. The court made clear that the third-party doctrine does not automatically apply to all digital information held by companies, and that certain kinds of records that are

particularly sensitive and private are protected by the Fourth Amendment. Our strategy going forward is threefold.

First, we will continue to push to expand the *Carpenter* rule to real-time cell phone tracking and other forms of location data. We have already engaged on this issue in a few cases—including one in which the Supreme Judicial Court of Massachusetts recently delivered a sweeping opinion—and we expect to become involved in more.

Next, we will need to push beyond location records into other kinds of sensitive data, including records generated by in-home "internet of things" devices and personal health and biometric data that are stored by private companies. For example, we are participating as a friend of the court to challenge the Drug Enforcement Agency's attempts to access a New Hampshire's prescription drug database records without a warrant, which state law requires. We were previously involved in two unsuccessful efforts to establish a warrant requirement in similar cases in Oregon and Utah, both of which were decided before the Supreme Court's *Carpenter* decision. We believe the current case presents a good opportunity to expand our win in *Carpenter* to another type of highly sensitive and pervasive digital data.

Over the longer term, we aim make new inroads against other anachronistic doctrines that simply no longer hold water in the digital age, such as the so-called "border-search exception" to the Fourth Amendment's warrant requirement.

We are currently engaged in litigation to establish a warrant requirement for device searches at the border, led by our case *Alasaad v. Nielsen*, in which we recently moved for summary judgment. We will also continue to file amicus briefs in criminal appeals involving this issue, and to advocate against increased vetting of visitors' social media accounts through our continuing Freedom of Information Act (FOIA) litigation.

ENABLING SECURE AND PRIVATE COMMUNICATIONS

Government efforts to ensure that companies do not deploy encryption that the government cannot circumvent are expanding in the United States and elsewhere. The government has shifted its strategy from demanding new legislation requiring backdoors in encryption to arguing that providers are already obligated to develop new surveillance capabilities under existing laws. For example, since November 2018, we have been litigating to unseal court records in a possible replay of 2016's *FBI v. Apple* litigation, this time with the FBI moving to hold Facebook in contempt for its refusal to undermine the security of its own service, Facebook Messenger.

The ACLU expects to be at the forefront of litigation, cybersecurity advocacy (see below), and separately funded legislative efforts to defend encryption and other means of ensuring communications security. We have been building our relationships with key tech companies to strengthen our coalition in preparation for what may be a major fight this year. At the same time, we will work to ensure that rampant government hacking is not adopted as the answer to more widespread encryption.

We will also monitor the proliferation of law enforcement requests to Amazon and other purveyors of in-home assistants like Alexa and Google Home for audio recordings

captured by those devices. While the machines purportedly do not capture ambient communications, we believe it is only a matter of time before law enforcement seeks to force purveyors to surreptitiously turn on cameras and microphones—if they have not done so already. With or without a warrant, this is would be an exceedingly dangerous development.

In addition, we will increase our public education around the risks of such devices and other cutting-edge technologies through our "Free Future" blog, other social media channels, reports, and media outreach.

IMPROVING CYBERSECURITY THROUGH ENGAGEMENT WITH INTERNET STANDARDS-SETTING BODIES

Much of modern speech and assembly happens on the internet. When people use online systems to communicate, they leak significant amounts of data by default to the invisible parties that operate the networks. This opens the door to silent, widespread surveillance that has troubling civil liberties implications for freedom of speech, privacy, and freedom of association. A major focus of ACLU technologists is reducing that leakage through standards bodies like the Internet Engineering Task Force, which set expectations about how machines across the globe talk to each other.

Our technologists will continue their work on a variety of priority projects, including making encrypted email more widely accessible; securing group chats, which pose more security risks than one-on-one messaging; and improving privacy protections for DNS, which connects users with the network services they use, such as www.aclu.org or www.cnn.com.

ENSURING THAT BIOMETRIC- AND AI-DRIVEN SURVEILLANCE TECHNOLOGIES ARE IMPLEMENTED WITH DEMOCRATIC OVERSIGHT AND IN WAYS THAT RESPECT CIVIL RIGHTS AND LIBERTIES

For years, a great surveillance machine has been growing up around us. The United States already deploys more surveillance cameras per capita than any other nation, but most of the footage is never reviewed. However, technologies that simply collect and store information in case it might be needed—so called "dumb" surveillance—are rapidly evolving into "smart" technologies that actively watch people, often in real time, and analyze our activities for suspicious patterns.

In fact, significant advances in AI and related technologies threaten to fundamentally transform the surveillance landscape and all but eliminate public anonymity. At this stage, our primary push-back has taken the form of public education (such as our recently released report on intelligent video analytics), demands for transparency and meaningful public control, and legislation.

We will continue to partner with ACLU affiliates in pushing for corporate accountability and policies preventing sale of face surveillance technology to law enforcement, as well as continue legislative advocacy to help achieve local legislation banning law

enforcement use of surveillance technologies and to prevent bad legislation from advancing at the federal level. We will also be developing litigation strategies and watching for litigation opportunities, just as we did for several years in the line of cell phone-location tracking cases that culminated in the *Carpenter* decision.

We are also pushing back through FOIA requests against the deployment of biometric surveillance techniques by DHS and other federal agencies and will consider litigation if appropriate opportunities arise.

12. Use of Funds

We expect to apply a grant near the middle of our range ($1,170,000) as follows:

SALARIES/BENEFITS:

New data surveillance/AI counsel: $150,000;

Other ACLU privacy/surveillance attorneys: $618,000;

ACLU of California privacy/surveillance attorneys: $205,000.

Total Salaries/Benefits: $973,000

OTHER ACLU AND ACLU OF CALIFORNIA COSTS:

Litigation: $5,000

Travel (for data surveillance advocacy): $11,000

Public education on data surveillance: $11,000

Office costs (includes phones, equipment, rent, IT): $57,000

Administrative overhead (includes time dedicated to this surveillance work by ACLU development, executive, human resources, and finance department staff): $113,000

Total Other Costs: $197,000

TOTAL BUDGET: $1,170,000

We would scale our work up or down accordingly to match any funding above or below this amount.

13. Target Population

Given our focus on the privacy and security of data of, from, or about individuals, 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. persons as well.

14. Individuals Served

While it is impossible to predict with certainty how many individuals will benefit from our work over a year, we expect to achieve at least one concrete change in policy or legal standards that meaningfully improves the privacy or security of more than 1 million individuals, and at least one change to internet standards or business practices that stands to benefit more than 5 million individuals.

15/16. Timeline and Project Completion

Given the ACLU's commitment to data privacy and security, we expect that we will always be looking to advance protections for consumers or defending protections we have already won. That being said, we expect to achieve at least two meaningful improvements to data privacy and/or security within a year of funding.

17. Project Support

The ACLU's Speech, Privacy, and Technology Project's data surveillance work is also funded by the John D. and Catherine T. MacArthur Foundation ($250,000 committed) and the LuEsther T. Mertz Charitable Trust ($150,000 committed), as well as projected grants from the Fritt Ord Foundation ($25,000), New York Community Trust ($30,000), and individual donors ($90,000). In addition, expenses above revenue will be covered by ACLU general funds.

UTILIZATION OF DATA

18. Evaluating Success

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 1) the privacy of consumers' data (such as a new warrant requirement to access patients' prescription information, or wider deployment of encrypted email), and 2) the security of consumers' and/or businesses' data (such as adoption of best practices for data retention and storage). We will also gauge the success of the ACLU's public education efforts through blog posts, op-eds, and earned media.

19. Court Updates

We propose submitting a short narrative report with hyperlinks highlighting our work (and, if funding permits, new ACLU staff) to be submitted six months after receipt of funding, with a longer narrative report (about 5–9 pages) more fully detailing supported activities, challenges/opportunities, and lessons learned to be submitted a month after the cy pres grant period has ended. However, we are open to reporting in a different format and/or frequency at the court's convenience.

20. Project Results

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 dedicated *Free Future* blog, the ACLU's extensive social media channels, and media outreach, 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.

MISCELLANEOUS

21. ACLU Relationship to Firms

Spector Roseman Kodroff & Willis PC: we are not aware of any relationship and have not been in contact with Spector Roseman about the Google Street View case or settlement apart from this application.

Cohen Milstein Sellers & Toll PLLC: Cohen Milstein has co-counseled several cases with the ACLU or ACLU state-based affiliates. For example, the firm recently filed a lawsuit with the ACLU of Maryland to stop the Prince George's County Board of Education from charging fees for summer school, and with the ACLU Women's Rights Project against AT&T for violating the Pregnancy Discrimination Act. Apart from this application, we have not been in contact with Cohen Milstein about the Google Street View case or settlement.

Lieff Cabraser Heimann & Bernstein LLP: The ACLU and ACLU of Michigan filed a lawsuit with Lieff Cabraser in 2012 against Morgan Stanley for violating federal civil rights laws by providing strong incentives to a subprime lender to originate mortgages that were likely to be foreclosed on. The firm may have co-counseled other cases with the national ACLU or state ACLU affiliates of which we are not immediately aware. Lieff Cabraser advised the ACLU of the possible Google Street View case and cy pres pool and invited us to apply.

22. Other Cy Pres Funding

The ACLU has occasionally received cy pres funding to advance our privacy work, most notably $716,000 through the Google Buzz privacy litigation settlement (2011–2012) and $70,000 from the Digital Trust Foundation (2015–2016) as part of the *Lane v. Facebook* settlement.

23. Google/Alphabet Support

The ACLU has received over $2.5 million from Google/Alphabet primarily through employee giving, employer matches, and employee-driven donations, but neither Google nor Alphabet has otherwise been a significant ACLU donor.