LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol (SBN 194857)
msobol@lchb.com
Melissa Gardner (SBN 289096)
mgardner@lchb.com
Michael Levin-Gesundheit (SBN 292930)
mlevin@lchb.com
Michael K. Sheen (SBN 288284)
msheen@lchb.com
Jallé H. Dafa (SBN 290637)
jdafa@lchb.com
John D. Maher (SBN 316157)
jmaher@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Nicholas Diamand (*pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500
Facsimile: 212.355.9592

Interim Co-Lead Class Counsel

AHDOOT & WOLFSON, PC
Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore Maya (SBN 223242)
tmaya@ahdootwolfson.com
Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
Henry J. Kelston (*pro hac vice*)
hkelston@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
2600 West Olive Avenue, Suite 500
Burbank, California 91505
Tel: 310.474.9111
Fax: 310.474.8585

Interim Co-Lead Class Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE LOCATION HISTORY LITIGATION

Case No. 5:18-cv-05062-EJD

JOINT DECLARATION OF TINA WOLFSON AND MICHAEL W. SOBOL IN SUPPORT OF MOTION FOR FINAL APPROVAL OF CLASS ACTION SETTLEMENT

Dept: Courtroom 4 - 5th Floor
Judge: Hon. Edward J. Davila
Date: April 18, 2024
Time: 9:00 A.M.

We, Tina Wolfson and Michael W. Sobol, declare as follows:

1. I, Tina Wolfson, am a partner in the law firm of Ahdoot & Wolfson, PC ("AW") and am a member in good standing of the California State Bar.

2. I, Michael W. Sobol, am a partner in the law firm of Lieff Cabraser Heimann & Bernstein, LLP ("LCHB" or "Lieff Cabraser") and am a member in good standing of the California State Bar.

3. We were appointed by the Court as Co-Lead Class Counsel in the consolidated proceedings against Defendant Google LLC ("Defendant" or "Google") in the above-captioned action (the "Action"). Unless otherwise indicated, we have personal knowledge of the matters stated here, and could and would testify competently regarding these matters if called upon to do so. We respectfully submit this Joint Declaration in support of Plaintiffs' Motion for Final Approval of Class Action Settlement.[1]

4. After what is approaching six years of hard-fought litigation, the Parties reached a nationwide class action Settlement by which Defendant agrees to pay $62 million into a non-reversionary cash fund to be used by up to 21 highly qualified, reputable, 501(c)(3) non-profit organizations for the support and defense of class members' privacy rights, and which requires meaningful prospective injunctive relief giving class members greater understanding of, and control over, their Location Information.

5. As explained in our Joint Declaration in Support of Plaintiffs' Motion for Attorneys' Fees and Expenses (Dkt. 351-1), we have been actively and personally involved in every aspect of this litigation since its inception, and (i) diligently investigated and asserted Plaintiffs' legal claims, in consultation with multiple experts; (ii) efficiently negotiated the consolidation of six related cases asserting substantially similar claims; (iii) successfully opposed, in part, Google's second motion to dismiss the claims in full after the Court dismissed the case in its entirety in response to Google's first such motion; (iv) engaged in comprehensive discovery and litigated roughly 20

[1] All capitalized words and terms are defined in the Class Action Settlement and Release Agreement ("Settlement Agreement" or "SA") (Dkt. 328-1) (Section II) unless otherwise defined herein.

discovery disputes through motions, regular hearings, and joint reports before Magistrate Judge Nathanael Cousins; (v) conducted significant research and discovery in preparation for the anticipated class certification motion; and (vi) engaged in multiple mediation and settlement conference sessions with Defendant, obtaining significant information regarding the Class claims in connection with such mediation; among many other tasks, all of which have been reflected in the quarterly time reports submitted *in camera* to this Court since 2019. As a result of this work, Plaintiffs and Class Counsel had a thorough understanding of the relative strengths and weaknesses of the claims asserted at the time the Settlement was reached.

6. Given the substantial risks of this ligation, we believe that the Settlement is very clearly in the best interests of the Settlement Class. As discussed below, we believe the Settlement is not only fair, reasonable, and adequate, but an excellent outcome that will advance Class Members' privacy interests.

SUMMARY OF SETTLEMENT TERMS AND CY PRES PROPOSALS

7. The Settlement Class. The Settlement Class is defined as "all natural persons residing in the United States who used one or more mobile devices and whose Location Information was stored by Google while 'Location History' was disabled at any time during the Class Period (January 1, 2014 through December 4, 2023).

8. Monetary Relief. The Settlement creates a non-reversionary cash Settlement Fund of $62 million to pay for the costs of Notice and Settlement administration, any Court-awarded attorneys' fees and expenses, and Class Representative Service Awards, with the balance (the "Net Settlement Fund") distributed to Court-approved *cy pres* recipients. SA ¶¶ 32, 39-42.

9. Class Counsel estimate that approximately $42.6 million in cy pres funding would be made available to support the work of these organizations if the requested attorneys' fees and other expenses are approved in full.

10. The proposed *cy pres* recipients must be "independent 501(c)(3) organizations with a track record of addressing privacy concerns on the Internet (either directly or through grants)," and as a condition of receiving any award, were required to provide a proposal "demonstrating and committing that they shall use the funds to promote the protection of internet privacy." SA ¶ 41.2.

11. Class Counsel vetted proposals from potential *cy pres* recipients, ultimately receiving proposals, at the time of this filing, from 21 organizations with a track record of work specifically targeted to promote and protect Class members' privacy interests, providing education, advocacy, and security against privacy violations in the future. True and correct copies of the proposals received from these organizations are attached hereto as Exhibits A through U to this Declaration, respectively:

A. American Civil Liberties Union Foundation (Speech, Privacy, and Technology Project)

B. American Civil Liberties Union Foundation of Northern California (Technology and Civil Liberties Program)

C. Berkman Klein Center for Internet & Society at Harvard University

D. Center for Democracy & Technology

E. Center for Privacy & Technology at Georgetown Law

F. Connect Safely

G. Data & Society Research Institute

H. Electronic Frontier Foundation

I. Electronic Privacy Information Center (EPIC)[2]

J. Fordham University Center on Law and Information Policy

K. Free Press

L. The Future of Privacy Forum Education & Innovation Foundation

M. The Internet Archive

N. The Markup

O. MIT Internet Policy Research Initiative

P. National Cyber Security Alliance

[2] EPIC updated its initial proposal for consideration as a *cy pres* recipient, and its revised proposal replaced the less detailed proposal on the Settlement Website on or around February 28, 2024. The document attached to Mr. Frank's Declaration as Exhibit 8 is the outdated, initial, version of EPIC's proposal.

Q. New York University Information Law Institute

R. Privacy Rights Clearinghouse

S. The Rose Foundation for Communities and the Environment

T. UCLA Institute for Technology, Law & Policy

U. Yale Law School Information Society Project

12. Each proposed recipient is an independent 501(c)(3) organization with a track record of addressing privacy concerns on the Internet (either directly or through grants).

13. Both parties' counsel examined each of these organization's past work, their proposed future projects, and evaluated the nexus between the organization and the claims and the class at issue here. In order to make practical proposals regarding specific allocations to particular entities that satisfied the nexus requirement, counsel also closely examined each organization's size, existing capacity, budgets, and other indicia of their ability to put funds from this Settlement to use so as to advance class members' interests effectively and efficiently.

14. In accordance with the terms of the Settlement, the Parties present the Court with their joint proposal for allocation of the Net Settlement Fund among suitable recipients in Exhibit A to Plaintiffs' Motion for Final Approval of Class Action Settlement, filed concurrently.

15. As a condition of receiving any portion of the Settlement Fund, each Approved *Cy Pres* Recipient shall provide a report to the Court and the Parties every six months regarding how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used. SA ¶ 41.4. Class Counsel will ensure that such reports are posted on the Settlement Website.

16. Non-Monetary Terms. As detailed in Exhibit C to the Settlement, the Settlement requires Google to implement a several business practice changes for a period of at least three years, including, for instance, sending a notification, after the Settlement's Effective Date, to all Google users with Location History or Web & App Activity settings enabled, explaining how those features collection Location Information, instructing those users how to disable the settings, and directing them to new web pages, the content of which was negotiated at length by Class Counsel. SA Ex. C at ¶¶ 4, 6. Google also is required to maintain a policy under which (a) Location Information stored through Location History and Web & App Activity is automatically deleted by

default after a period of at least 18 months when users opt into these settings for the first time, and (b) users can set their own auto-delete periods. And all of the Settlement's meaningful injunctive relief extends for at least three years.

17. Negotiations that led to the Settlement's non-monetary terms predated the public announcement of Google's settlements with various state attorneys general in late 2022 and early 2023. These negotiations extended for months, and included several iterations and revisions of written proposals and counterproposals, and consultation with experts.

CONCLUSION

18. The Settlement is the product of extensive arm's-length negotiations over many months, including three full-day mediation sessions (on March 15, May 2, and May 24, 2022) and numerous additional discussions facilitated by experienced mediator Professor Eric D. Green, Esq.; a settlement conference with Magistrate Judge Joseph C. Spero on January 19, 2023; and strenuous direct negotiations between the parties. Through formal discovery and information exchanged during the settlement negotiation process, Plaintiffs and Class Counsel obtained significant information regarding the Settlement Class's claims and developed a thorough understanding of the relative strengths and weaknesses of the claims at the time the Settlement was reached.

19. Based on our experience and knowledge regarding the factual and legal issues in this matter, and given the substantial benefits to privacy rights provided by the Settlement, it is our opinion that the proposed Settlement is not only fair, reasonable, and adequate, but an excellent outcome that is in the best interests of the Settlement Class.

We declare under penalty of perjury that the foregoing is true and correct. Executed on this 25th day of March 2024, by Tina Wolfson in Burbank, California, and Michael W. Sobol in Brooklyn, New York.

/s/ *Tina Wolfson*
Tina Wolfson

/s/ Michael W. Sobol
Michael W. Sobol

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Tina Wolfson, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 25th day of March 2024, at Burbank, California.

/s/ Tina Wolfson
Tina Wolfson

Exhibit A

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.

Exhibit B

ACLU Foundation of Northern California
Technology and Civil Liberties Program
Proposal for Google Location History Litigation Cy Pres Award
October 5, 2023

The American Civil Liberties Union Foundation of Northern California is deeply grateful for the invitation to submit this proposal for *cy pres* funds from the Google Location History Litigation. We are excited to share three potential funding opportunities, ranging from one to three years of funding, which would support us to continue and expand our work to promote the protection of internet privacy. We welcome questions or further requests for information.

ORGANIZATION INFORMATION

Organization History, Programs, and Goals

The American Civil Liberties Union Foundation of Northern California (ACLU of Northern California) is a 501(c)(3) nonprofit organization and the largest state-based affiliate of the ACLU.[1] Founded in 1934, the ACLU of Northern California has been a leading champion of civil liberties and civil rights for more than ninety years and been unwavering in our commitment to fight for fairness, equality, and justice for all people.

We have worked throughout our organization's history to ensure that fundamental rights are protected as technology advances and have been a national leader in privacy and technology work since the dawn of the digital age in the 1960s. The ACLU of Northern California helped spearhead the passage of the California constitutional right to privacy in 1972 and has played an instrumental role in the seminal California privacy cases and the development of California law that leads the nation in safeguarding and promoting internet privacy.

In 2004, the ACLU of Northern California created the Technology and Civil Liberties Program—the first dedicated ACLU legal program at a state affiliate to defend and promote privacy and support social justice in the digital age. The Technology and Civil Liberties Program has consistently been on the vanguard of cutting-edge legal work in the courts, with companies, and in communities to build on the inalienable constitutional privacy rights guaranteed to all Californians, and to safeguard and promote internet privacy rights for people in this state and far beyond. We work to build a world where technology is helping, not harming, people and supporting a just and equitable society.

[1] The ACLU Foundation of Northern California and the American Civil Liberties Union Foundation are separate legal entities and have independent boards and budgets. A *cy pres* award to the American Civil Liberties Union Foundation goes to the national entity, based in New York City. A *cy pres* award to the ACLU Foundation of Northern California goes to the California state office based in San Francisco and would support the internet privacy work of the Technology and Civil Liberties Program as detailed in this proposal.

The Technology and Civil Liberties (TCL) Program is one of six legal-policy programs at the ACLU of Northern California, and TCL program staff work on intersectional internet privacy projects with colleagues in our other program teams: Gender, Sexuality & Reproductive Justice, Immigrants' Rights, Democracy & Civic Engagement, Criminal Justice, and Racial & Economic Justice. Across issue areas, we employ decades of experience with integrated advocacy, using impact litigation, legislation,[2] community organizing, and public education to ensure that constitutional rights—to free speech, to privacy, to due process—don't just exist on paper, but also in practice. We are longtime champions of the full range of civil rights and liberties, and our work advancing internet privacy is intersectional by design.

Cy Pres Awards

The ACLU of Northern California has received prior *cy pres* awards to help develop and support its extensive internet privacy work, as well as *cy pres* awards for other areas of organizational work. The following are past *cy pres* awards for internet privacy and other related technology and privacy work of the Technology and Civil Liberties Program.

- *In re Google LLC Street View Electronic Communications Litigation* (2023), $1,006,583 to the American Civil Liberties Union Foundation (ACLU National). ACLU National then selected affiliates for subgrants to support internet privacy work, including a $250,000 subgrant to ACLU Foundation of Northern California.
- *Doe v. Twitter* (2016), $302,914.26 for a statewide project to create awareness about online privacy issues and educate consumers and businesses about online privacy issues and safeguards that can be implemented to protect privacy rights.
- *UCAN v. Bank of America* (2007), $305,034.25 to develop and implement a public campaign to educate consumers, policymakers, and businesses about internet privacy rights of people in California and the privacy implications presented by new and emerging technologies.
- *Rockers et al. v eBay, Inc., et al.* (2007), $40,683.06 to develop and implement a public campaign to educate consumers, policymakers, and businesses about privacy rights of internet users in California and the privacy implications presented by new and emerging technologies.
- *UCAN v. Capital One* (2006), $203,619.18 for the California National ID Initiative, a statewide public education and research project to educate Californians about informational privacy threats posed by issuance of new state and national identification documents, and to make significant progress with legislation designed to address some of these threats.

Charity Ratings

The ACLU Foundation of Northern California is rated as a Four-Star Charity with a charity score of 100% from Charity Navigator and a Gold Transparency rating from GuideStar.

[2] Legislative work is done by the ACLU of Northern California, a separate 501(c)4 organization, and is included here only to relay this component of our integrated advocacy approach. No *cy pres* funds would be used for legislative work.

GRANT PROPOSAL

Project Director
Nicole Ozer is the Technology and Civil Liberties Program Director for the ACLU of Northern California and has led the organization's cutting-edge work to defend and promote internet privacy and other rights in the modern digital world since 2004. Nicole sets the strategic vision for the Technology and Civil Liberties Program and its statewide team of lawyers working in the courts, in communities, with companies, and policymakers to promote internet privacy for people in California and far beyond.

From her position at the ACLU of Northern California, Nicole developed and led the ACLU's national internet privacy campaign, Demand Your dotRights. This multi-year public education campaign connected the dots on internet privacy and government surveillance and led to many internet privacy advances, including the first location information privacy transparency reports by AT&T and Verizon and the passage of the landmark California Electronic Communications Privacy Act (CalECPA). Nicole is a nationally recognized expert on internet privacy issues and regularly speaks at local, state, and national conferences and academic events and in the media.

Nicole graduated magna cum laude from Amherst College, studied comparative civil rights history at the University of Cape Town, South Africa, and earned her J.D. with a Certificate in Law and Technology from the University of California, Berkeley School of Law. Before joining the ACLU of Northern California, Nicole was an intellectual property attorney at Morrison & Foerster LLP in San Francisco.

Nicole spent the spring of 2019 on sabbatical as a Visiting Researcher at the Berkeley Center for Law and Technology and as a Non-Residential Fellow at the Stanford Digital Civil Society Lab. During her sabbatical, Nicole co-authored *Integrated Advocacy: Paths Forward for Digital Civil Society*. More information about Nicole's academic and legal publications is available at https://www.aclunc.org/staff/nicole-ozer-esq-sheher.

Nicole has been honored with the Privacy Award by the Berkeley Center for Law & Technology and the James Madison Freedom of Information Award by the Society of Professional Journalists. The Recorder recognized Nicole as a Woman Leader in Tech Law in both 2023 and 2018 and recognized the Technology and Civil Liberties Program as a finalist for Top Tech Litigation Department of the Year in 2023. The Daily Journal recognized Nicole as a top Artificial Intelligence Lawyer in 2019 and San Jose Magazine selected her as one of 20 "Women Making a Mark" in Silicon Valley.

Program Requests - Issues, Approach, Goals & Objectives, Activities, Funding, Timeline
We live in a digital world and people of all ages must rely on internet technology to communicate, connect, mobilize, and obtain necessities like housing, employment, and health care. For many people– especially Black and Brown and Indigenous communities, immigrants,

disabled people, and others that society may be trying to marginalize—our lives are increasingly shaped by the way technology is built and whether internet privacy is protected, or personal information is collected, used, and shared.

Defending and expanding internet privacy is critical because new technology can provide unprecedented power to invade personal lives, undermine fundamental rights, exacerbate injustice, and endanger people and democracy. As such, internet privacy now intersects with all social justice and civil rights issues of our time.

The ACLU of Northern California Technology and Civil Liberties Program is a national leader in using integrated legal strategies and coordinating work in the California courts, with companies, and in communities, to maximize the ability to defend and promote internet privacy not just for Californians, but also better protect these rights for people across the country and around the world.

The Technology and Civil Liberties Program has two long-term privacy goals, namely to: 1) ensure that all personal information gets the privacy protection it deserves; and 2) end deployment of dragnet internet surveillance practices by law enforcement and better protect vulnerable community members.

The ACLU of Northern California respectfully requests a *cy pres* award to both continue and expand the organization's important internet privacy work. The award would support both litigation and other integrated advocacy that build on our successful, decades-long efforts to advance internet privacy.

We seek *cy pres* funding to support the work of the ACLU of Northern California Technology and Civil Liberties Program for the following goals and objectives:

(1) continue to work on important internet privacy cases and support new litigation and other legal strategies utilizing California state constitutional law to better protect internet privacy;
(2) create more awareness and understanding about privacy issues and build stronger intersectional relationships to promote internet privacy;
(3) educate the public about how personal information is commonly collected, retained, used, and disclosed and how people can better protect their internet privacy;
(4) educate businesses about internet privacy issues and safeguards that can be implemented to better protect privacy rights.

Below are three possible funding options, ranging from one to three years of *cy pres* funding.

One-Year Proposal - $750,000 *Cy Pres* Award

If selected for a $750,000 *cy pres* award, we would be able to address the following goals and engage in the following activities:

(1) Work on critical internet privacy cases in state and federal court and support new impact litigation and other legal strategies utilizing California law to better protect internet privacy.

Many important internet privacy cases are litigated in California state and federal courts, and the ACLU of Northern California regularly works on these cases. For example, recent work has included:

- *Meza v. Superior Court* (California Supreme Court) - filing an amicus letter in support of petition for review to the California Supreme Court about internet privacy and better protecting people's location information from government "geofence warrants," dragnet law enforcement demands to technology companies for people's location information to discover who was in a particular place at a particular time.
- In *Re Ricardo* (California Supreme Court) - filing an amicus brief in the successful California Supreme court case defending internet privacy of young people enmeshed in the criminal justice system.
- *EFF v. Superior Court* (California Supreme Court) - filing an amicus letter in support of petition for review to the California Supreme Court to better protect internet privacy by ensuring transparency about government use of cell site simulators to obtain location information and monitor where people go and what they do.
- *ACLU v. DOJ* (Northern District of California) - successfully litigating, in partnership with ACLU National, to enforce our freedom of information act request to seven federal agencies and obtain records to reveal how the government was attempting to undermine internet privacy through widespread surveillance of social media platforms.
- *Liapes v. Meta* (First District Court of Appeals) - filing an amicus brief, in partnership with ACLU National, related to the internet privacy implications of discriminatory ad targeting.
- *In re Eshelman* (Northern District of California) - successfully defeating a subpoena attempting to pierce the internet privacy of an individual who was targeted by a pharmaceutical tycoon for critical commentary.
- *hey Inc. v. Twitter* (Ninth Circuit Court of Appeals) - filing an amicus brief to protect individuals from use of a federal foreign discovery statute to pierce their internet privacy.

There are many other internet privacy cases currently moving through the California courts, including related to the sharing of personal information with data brokers and other third parties, challenges to children's internet privacy and other California laws, and cases related to internet privacy and viewing records. The funds would be used to continue to defend and promote the internet privacy rights of people in important cases.

The funds would also be used to develop new litigation work and other legal strategies utilizing California state constitutional privacy law and statutory law to better protect internet privacy. It would support the extensive legal research and writing, factual investigations, and expert technologist support needed for cutting-edge work in the courts to promote internet privacy.

We have a strong constitutional right to privacy in California and the ACLU of Northern California has played an instrumental role in the seminal California privacy cases including *White v. Davis*, *People v. Blair*, *Burrows v. Superior Court*, *Hill v. NCAA* and *Sheehan v. San Francisco 49ers.*

Today, in the aftermath of the Supreme Court decision in *Dobbs* and many states actively attacking reproductive and LGBTQ rights, it is more critical than ever to fully utilize state privacy law to protect people. The ACLU of Northern California has helped spearhead an important academic symposium on this issue that will be held at Berkeley Law on October 27, 2023. Leading academics and practitioners, including the Technology and Civil Liberties Program Director and the senior staff attorneys, will come together to discuss the current state of the law and discuss potential new and creative ways to utilize constitutional privacy law.

The funds will support the Technology and Civil Liberties Program to build off the learnings and momentum of this academic symposium and have the resources necessary to develop new cutting-edge litigation and other legal work to utilize California state constitutional privacy and statutory law to better protect internet privacy.

(2) Create more awareness about internet privacy issues and strengthen intersectional relationships to more effectively defend and promote internet privacy.

To better defend and promote internet privacy, it is important to create more public awareness and builder greater connection with racial justice, economic justice, and other issues to more effectively discuss the impact of internet privacy issues on people's lives and strengthen intersectional and collaborative work.

The ACLU of Northern California has already been able to do some impactful work in this area. We organized a remote convening in October 2022, bringing together 55 organizational and community leaders working on racial justice, youth justice, gender, sexuality and reproductive justice, immigrants' rights, environmental justice, and economic justice. This day-long convening of presentations and breakout conversations facilitated robust discussion about emerging issues and strategies for addressing internet privacy on new terrain and supported new intersectional relationships. We also started to develop an intersectional public narrative that has already been employed by diverse groups working on internet privacy campaigns. But much more can and should be done.

ACLU of Northern California recognizes the need to build on this existing work and support the intersectional education, partner engagement, organizing, and strategic communications. The funds would enable us to:

- Better communicate about how internet privacy affects people through narrative change and strategic communications on internet privacy. It would provide the funding needed for focus groups and message testing to inform more effective public narratives and public education materials on internet privacy and intersectional engagement.

- Diversify and strengthen coalitions to support internet privacy**.** It would support the team's travel, attendance, and participation at diverse events and coalition meetings to build and maintain needed relationships. It would support the partner engagement and coalition organizing needed to diversify and strengthen internet privacy coalitions.

(3) Educate the public about how personal information is commonly collected, retained, used, and disclosed on the internet and how to better protect the privacy of their personal information.

Making sure that people better understand how personal information is collected, retained, used, and disclosed and how to better protect the privacy of their personal information is foundational to better protecting internet privacy.

The funds would allow us to:

- Research, draft, and publish at least four new easy-to-understand internet privacy education materials on topics such as:
    - Internet Privacy and Health Apps and Services
    - Internet Privacy and Location Information
    - Internet Privacy and Digital Payments
    - Internet Privacy & Learning What Information Has Been Collected and Shared About You
    - Internet Privacy & Government Demands for Your Personal Information
    - Internet Privacy and Student Information

- Give presentations at local, state, and national conferences to educate a diverse cross-section of the public, including young people and people of color, about how to access resources about internet privacy issues and how to better protect their privacy.
- Research and draft materials for both online distribution and offline publication, including newspapers, social networking sites, and our own blog, to highlight internet privacy issues and educate the public about how to better protect their privacy.
- Continue to meaningfully serve as a privacy resource for the legal and technical community; analyze emerging privacy issues and develop new policy papers; support corporate advocacy by diverse partners; and participate in academic symposia, events, and educational activities to advance privacy issues hosted by public agencies, law schools, technology centers, and clinics in California and around the country.

(4) Increase awareness and accountability among businesses on internet privacy issues and protections that should be implemented to better protect internet privacy rights.

Educating and effectively pushing companies to better protect internet privacy rights is also essential. The funds would allow us to:

- Research, draft, and publish an extensive update of the ACLU of Northern California's pioneering business primer, *Privacy & Free Speech, It's Good for Business*. With its more

than 150 real-life business case studies and internet privacy resources on information collection, retention, use, and disclosure, it is the most comprehensive resource of its kind to help companies better safeguard internet privacy (available online at www.aclunc.org/business/primer).

Many people have already utilized the business primer, and it has been the focus of presentations for the business, legal, and technical community at high-level conferences around the country such as South by Southwest, Defcon, Gartner, and the RSA Computer Security Conference. The business primer has also been cited by the Federal Trade Commission.

The funds also would allow us to:

- Research, draft, and publish at least four new internet privacy materials for business on topics such as:
  - Internet Privacy and Health Apps and Services
  - Internet Privacy and Location Information
  - Internet Privacy and Digital Payments
  - How Your Business Can Comply with Internet Privacy Law and Why It Matters
  - How Your Business Can Use Internet Privacy Law to Protect People from Government Demands
  - Internet Privacy and Student Information
- Meet with companies, both well established and start-ups, to discuss emerging technology and business models and push for incorporation of more effective internet privacy protections into product and business plan design and help prevent privacy invasions.

Timeline for all activities – to be completed within 1 year of receiving the *cy pres* award.

Two-Year Proposal - $1.5 Million *Cy Pres* Award

A *cy pres* award of $1.5 million would provide the additional support needed to implement the activities that were developed in Year 1 as well as fund important new projects to further deepen and expand the internet privacy work.

(1) Continue to engage in the existing cases and support the implementation of the new litigation and legal strategies developed in Year 1 to utilize the California constitutional right to privacy.

The funds would support the extensive legal research and writing, factual investigations, and expert technologist support needed to continue to work on existing cases and implement the cutting-edge litigation and other legal strategies using California constitutional law and other laws developed during Year 1.

(2) Continue to create more awareness about internet privacy issues and strengthen intersectional relationships to more effectively defend and promote internet privacy.

The funds would support continued, consistent work on narrative change and strategic communications work on internet privacy, including:

- Utilize the public narrative work developed in Year 1 and regularly use in public materials and press opportunities. Provide strategic support to also facilitate its effective use by diverse partners for their own internet privacy work.
- Continue to travel, attend, and participate in diverse events to build and maintain needed relationships.
- Continue partner engagement and organizing to diversify and strengthen internet privacy coalitions.
- Organize and host a follow-up intersectional convening to continue to support greater cross-organization work on emerging issues in internet privacy.

(3) Continue to educate the public about how personal information is commonly collected, retained, used, and disclosed on the internet and how to better protect the privacy of their personal information.

The funds would support promotion of the materials produced in Year 1 and continued, consistent work to educate the public about internet privacy and how to better protect the privacy of their personal information.

- Widely promote the new easy-to-understand internet privacy education materials produced in Year 1.
- Continue to give presentations at local, state, and national conferences to educate a diverse cross-section of the public, including young people and people of color, about how to access resources about internet privacy issues and how to better protect their privacy.
- Continue to research and draft materials for both online distribution and offline publication, including newspapers, social networking sites, and our own blog, to highlight internet privacy issues and educate the public about how to better protect their privacy.
- Continue to meaningfully serve as a privacy resource for the legal and technical community; analyze emerging privacy issues and develop new policy papers; support corporate advocacy by diverse partners; and participate in academic symposia, events, and educational activities to advance privacy issues hosted by public agencies, law schools, technology centers, and clinics in California and around the country.

(4) Continue to increase awareness and accountability among businesses on internet privacy issues and protections that should be implemented to better protect internet privacy rights.

The funds would support the promotion of materials produced in Year 1 and the continued, consistent work to educate and push businesses to better protect internet privacy.

- Promote the internet privacy update to the business primer, online through our website, social networking sites, our own blog, and online marketing. Offline through presentations at local, state, and national business conferences and events.
- Continue to maintain and update the primer by researching, drafting, and publishing new real-life internet privacy case studies as they develop.
- Prepare and meet with at least six companies, both well-established and start-ups, to discuss emerging technology and business models and help them integrate more effective internet privacy protections into product and business plan design and help prevent privacy invasions.

(5) Develop new projects to deepen and expand our work and public knowledge about internet privacy issues by researching, drafting, and publishing two new white papers:

- White paper on internet privacy and cashless payments

The funds would allow our team to investigate and detail the internet privacy implications related to the rise of digital ordering and payment. This white paper would build on an initial investigation that we conducted with Berkeley Information School and law students during the 2022-2023 school year to identify the proliferation of no-cash policies in local stores.

The rise of digital ordering and payments at restaurants and other businesses is moving all of the internet privacy issues related to information collection, retention, use, and disclosure to the offline world.

When restaurants and other businesses make being able to order or pay digitally the only option (and needing to own a smartphone in order to do this), it also has significant implications for access and equity. Many people do not have a smartphone, including more than 40 percent of people over the age of 65, and 25 percent of people who make less than $30,000 per year. People with disabilities and the unhoused are also less likely to own a smartphone. These are some of our most vulnerable communities.

- White paper on internet privacy and advertising implications on vulnerable communities

The funds would allow our team to investigate and detail the internet privacy implications of targeted advertising on communities, with an emphasis on discussing how Black and Brown communities, immigrant communities, people with fewer economic resources, and people seeking reproductive and gender-affirming care can be disproportionately affected.

Timeline for all activities – to be completed within 2 years of receiving the *cy pres* award.

Three-Year Proposal - $2.25 Million *Cy Pres* Award

A *cy pres* award of 2.25 million would provide the additional support needed to implement the activities that were developed in Year 1 and started in Year 2, as well as fund additional projects to further deepen and expand the internet privacy work.

(1) Continue to engage in existing cases and continue to support the implementation of the new litigation and legal strategies started in Year 2.

The funds would support the extensive, consistent, multi-year legal research and writing, factual investigations, and expert technologist support needed to work on cutting-edge litigation promoting internet privacy.

The funds would also support a follow-up convening on state constitutional privacy work to continue to build and expand new and creative litigation and other legal strategies.

(2) Continue to create more awareness about internet privacy issues and strengthen intersectional relationships to more effectively defend and promote internet privacy.

The funds would enable us to continue to build on the work from Years 1 and 2, and to support the intersectional education, partner engagement, organizing, and strategic communications needed to better communicate about how internet privacy affects people and diversify and strengthen coalition efforts to protect internet privacy.

(3) Continue to educate the public about how personal information is commonly collected, retained, used, and disclosed on the internet and how to better protect the privacy of their personal information.

The funds would enable us to continue to build on the work from Years 1 and 2 and consistently continue to educate the public about internet privacy issues and how to better protect the privacy of personal information. Activities include:

- Continue to promote the new easy-to-understand internet privacy education materials produced in Year 1 and update/develop new materials as necessary.
- Continue to give presentations at local, state, and national conferences to educate a diverse cross-section of the public, including young people and people of color, about how to access resources about internet privacy issues and how to better protect their privacy.
- Continue to research and draft materials for both online distribution and offline publication, including newspapers, social networking sites, and our own blog to highlight internet privacy issues, and educate the public about how to better protect their privacy.
- Continue to meaningfully serve as a privacy resource for the legal and technical community; analyze emerging privacy issues and develop new policy papers; support corporate advocacy by diverse partners; and participate in academic symposia, events, and educational activities to advance privacy issues hosted by public agencies, law schools, technology centers, and clinics in California and around the country.

(4) Continue to increase awareness and accountability among businesses on internet privacy issues and protections that should be implemented to better protect internet privacy.

The funds would enable us to continue to build on the work from Years 1 and 2 and continue to consistently educate and push businesses to better protect internet privacy, as well as deepen the work with an additional focus on the venture capital community. Activities include:

- Continue to promote the internet privacy update to the business primer, online through our website, social networking sites, our own blog, and online marketing. Offline through presentations at local, state, and national business conferences and events.
- Continue to maintain and update the primer by researching, drafting, and publishing new real-life internet privacy case studies as they develop.
- Expand education and outreach to the venture capital community. As initial public offerings have slowed, businesses are now less likely to become public companies before impacting the internet privacy of many people. It has therefore become critical to engage more effectively with the venture capital community so that more internet privacy protective practices are encouraged and supported by the private investors who are working with these companies.

(5) Deepen work and better protect internet privacy though technology research and interactive public education tools.

Damaging internet privacy practices are often hidden. It can be hard to discover what is really happening to personal information, and to effectively identify and communicate the potential implications. Using both technology research and developing creative, interactive technology tools to cut through these challenges has been an incredibly effective strategy. Funds would allow us to:

- Retain the expert technology support needed to conduct independent app and website privacy audits and other technical projects to continue to identify emerging internet privacy issues and engage in cutting-edge legal work.
- Work to develop a new, creative, interactive, technology tool to educate and protect internet privacy. We have a proven track record of being able to develop important technology tools like this when we have the resources available. For example, our ACLU of Northern California Facebook Quiz About Facebook Quizzes[3] educated the public in a clear and interactive way what personal information—including political affiliation, religion, sexual orientation, and pictures—that Facebook apps were collecting about them and also about their Facebook friends.

[3] Chris Conley, ACLU of Northern California blog post (August 26, 2009), https://www.aclunc.org/blog/take-our-quiz-see-what-do-facebook-quizzes-know-about-you; New York Times article about the quiz (August 27, 2009), https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2009/08/27/27readwriteweb-what-facebook-quizzes-know-about-you-75429.html

Our tech quiz walked people through what was happening to their personal information, why, and how to better protect their internet privacy.

Our tech quiz also publicly blew the whistle on the larger Facebook "privacy app-gap"—the internet privacy hole that Cambridge Analytica[4] exploited as part of its shadowy voter-profiling work that used information from tens of millions of Facebook profiles during the 2016 election.

Timeline for all activities – to be completed within 3 years of receiving the *cy pres* award.

Benefit /Target Population for Project

The ACLU of Northern California is based in California, but the internet has no borders. We develop and implement our internet privacy work to benefit people far and wide, with a particular focus on how to support people who may be disproportionately affected by internet privacy threats, including people of color, people with fewer economic resources, immigrants, activists, and, now increasingly, people seeking reproductive and transgender healthcare in states that are criminalizing these rights.

Working in deep partnership and in support of diverse local, state, and national organizations and community activists, our ACLU of Northern California work on internet privacy has built the awareness, knowledge, and momentum necessary to develop stronger laws and corporate practices and give people the power to better control their internet privacy. This work has required companies all over the world to develop privacy policies, notify people about data breaches, and stop the collection and sharing of personal information. Our extensive corporate advocacy work has led to new international policies by large technology companies like Facebook and Twitter to protect the internet privacy of billions of people around the world.

Through the ACLU's California affiliate network, our print and electronic newsletters, social media, and other distribution channels, we reach hundreds of thousands of people with our educational messaging and materials. Our materials also are often distributed by the national ACLU network of blogs and social networking feeds, and these communications can reach more than 1 million people.

With this *cy pres* funding, we can continue and expand this important internet privacy work.

EVALUATION

We agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocation to the ACLU of Northern California has been used and how remaining funds will be used.

[4] Nicole Ozer and Chris Conley, ACLU blog post (March 23, 2018), https://www.aclu.org/news/privacy-technology/after-facebook-privacy-debacle-its-time-clear-steps-protect

We will evaluate the success of the grant based on achievement of each of the deliverables detailed in the proposal's goals and objectives, activities, and timeline for Year 1, Year 2, and Year 3. For example, in Year 1, achievement of activities delineated in (1)-(4), such as researching, drafting, and publishing at least four new easy-to-understand internet privacy education materials for people and for businesses, by the end of that grant year. For Year 2, achievement of activities delineated in (1)-(5), and for Year 3, achievement of activities delineated in (1)-(5).

Related to the overall success of the grant in enhancing and promoting internet privacy, the ACLU of Northern California Technology and Civil Liberties Program also sets long-term goals, annual goals, and short-term goals, and conducts annual evaluations to measure progress on all our priority work, including internet privacy.

As detailed in the proposal above, the *cy pres* award will support developing, publishing, and promoting a variety of new materials on internet privacy for people and businesses as well as presentations at diverse local, state, and national conferences, events, and academic symposia to better protect internet privacy.

Exhibit C

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY
1557 Massachusetts Avenue, Cambridge, MA, 02138 P +1.617.495.7547 F +1.617.495.7641
w: cyber.harvard.edu e: hello@cyber.harvard.edu t: @BKCHarvard

October 5, 2023

Deborah De Villa, Esq.
Ahdoot Wolfson Attorneys
2600 W. Olive Avenue | Suite 500
Burbank, California 91505

Michael Sobol, Esq.
Lieff Cabraser Heimann & Bernstein, Attorneys at Law
275 Battery St, Floor 29
San Francisco, CA 94111

RE: Google Location History Litigation, No. 5:18-cv-05062-EJD (N.D. Cal.)

Dear Ms. De Villa and Mr. Sobol:

The Berkman Klein Center for Internet & Society ("BKC" or "the Center") is honored to be considered as a potential recipient of *cy pres* funds in the above case. As the scope and sweep of our current and future work show below, we can make full use of *cy pres* funds from either category.

Please find the additional information requested for the Court below:

Organization Information

(1) Name of organization
Berkman Klein Center for Internet & Society
The President and Fellows of Harvard College
1557 Massachusetts Avenue
Cambridge, MA 02138

(2) Discuss the founding and history of the organization.

Since its founding in 1996, Harvard's Berkman Klein Center for Internet & Society (BKC) has

housed rigorous scholars whose research has been fundamental to our collective understanding of the digital space, and whose creative thinkers have turned ambitious ideas into concrete impact. Originally founded at Harvard Law School, BKC has grown into Harvard's only university-wide, interfaculty initiative devoted to studying the Internet. Once controversial and novel, many of the insights derived from those at BKC are now well accepted and even foundational to continuing work in academia, private industry, and civil society. By closely examining the existing architecture of the digital world—and in imagining better systems of governance—BKC leaders are among those who have helped positively shape the trajectory of the digital world.

BKC is Harvard's center for connecting faculty who study Internet & new technologies. Chris Bavitz leads Lumen, which uniquely collects and studies online content removal requests, providing transparency and supporting analysis of the Web's takedown "ecology"; Jonathan Zittrain and James Mickens co-lead the Institute for Rebooting Social Media, which addresses social media's most urgent problems including privacy breaches, content governance, and misinformation; and Cass Sunstein and Oren Bar-Gill have just launched the Artificial Intelligence and the Law effort, bringing together a team of faculty to research algorithms and consumer protection.

BKC's commitment to world-class scholarship has been coupled with a desire to build a digital sphere that serves the public interest. Early BKC projects, such as Creative Commons, Global Voices, and the Digital Media Law Project allowed people to rethink sharing and content amplification online; harness the potential of the web to translate crucial underreported news directly from global citizen journalists; and create resources to help citizen and professional journalists alike navigate a nascent but quickly growing and complexifying field. The success of these projects, as well as more recent BKC community-incubated organizations like the Integrity Institute (a think-and-do tank for trust and safety workers in tech) and the Edgelands Institute (a multi-disciplinary organization explores how the digitalization of urban security is changing the urban social contract) has hinged on BKC's ability to serve as a trusted convener, hosting practitioners, policymakers, technologists, artists, and academics for iterative dialogue on emerging issues in technology and society, and to create an entrepreneurial environment to develop research-based solutions and coalitions.

The Center's programs are world-renowned for bringing together those who seek to use their extraordinary talents in the service of global public interest, and who wish to contribute to a collaborative network committed to generosity, curiosity, and action. We are dedicated to serving undergraduate students through tenured faculty at Harvard and from academic institutions around the world, as well as people from the full range of career stages, disciplines, sectors, national origins, and lived experiences. Our capacity and field-building efforts have resulted in an active network of thousands, where active appointees and alumni work in companies, governments, civil society, and academic institutions as well as leadership roles that direct rigorous research,

frontline community consultations, and civic-minded advocacy. To date, BKC has welcomed more than 500 people into its community of fellows, staff, faculty, and affiliates from more than 40 countries; hosted more than 1,000 events, workshops and conferences; produced more than 700 videos and podcasts; contributed more than 10 million lines of code to GitHub; and published more than 250 reports, papers, and books in our publication series.

(3) Describe the organization's current goals.

A diverse, interdisciplinary community of scholars, practitioners, technologists, policy experts, and advocates, we seek to tackle the most important challenges of the digital age while keeping a focus on tangible real-world impact in the public interest. The beneficiaries of this work include the Internet & society community broadly construed including students, practitioners, public sector stakeholders, technology leaders, policy-makers, academics, and the broader public.

(4) Provide a brief description of the organization's current programs.

Select examples of established programmatic initiatives in these areas include the following:

Privacy Tools
The Privacy Tools Project advances a multidisciplinary understanding of data privacy issues and builds computational, statistical, legal, and policy tools to help address these issues in a variety of contexts. By leveraging advances in computer science, social science, statistics, and law, the Privacy Tools project aims to further the tremendous value that can come from collecting, analyzing, and sharing data while more fully protecting individual privacy. This effort seeks to translate the theoretical promise of new technical measures for privacy and data utility into definitions and measures of privacy and data utility, as well as practical computational, legal, and policy tools for enabling privacy-protective access to sensitive data in a variety of contexts.

Recent work of the Privacy Tools Project has included efforts to bridge the understanding of legal and technical privacy concepts relevant to statistical agencies such as the US Census Bureau, as well as an NSF-funded collaboration to pilot co-design of law and computer science to ensure the adoption of sociotechnical systems that provide adequate data protection for individuals, groups, and society. Members of this team are also a part of the Data Co-ops project at Georgetown University to develop technical and legal tools for re-envisioning the information ecosystem. In addition to contributing to data publishing infrastructure around the world, the ideas developed in this project aim to benefit society more broadly as it grapples with data privacy issues in many other domains, including public health and electronic commerce.

Institute for Rebooting Social Media
In 2021, the Center launched the Institute for Rebooting Social Media ("RSM") in recognition of the fact that the relationship between consumers and powerful social media platforms is in need

of a reset. This three-year research initiative at the Center has focused on addressing social media's most urgent problems, including misinformation, privacy breaches, and content governance. RSM has brought together participants from academia, industry, government, and civil society in time-bound collaboration to spur real practical legal, technical, and policy changes in the state of our online social media. RSM participants have explored the development of new legal, governance, and technical structures to build consumer trust, alter today's paradigms around the capture and monetization of user data, re-examine principles of liability of social media platforms, and mitigate the current risks and harms to consumers and society at large. The RSM initiative combines efforts to advance scholarship through public writing and analysis, expand the field of students and professionals engaged on these issues in the public interest, and build tangible prototypes. Projects furthering these objectives of fostering a safer, privacy-respecting digital consumer environment, such as the Integrity Institute, have been nurtured and developed through RSM and its predecessor Assembly Program at the Center.

Cyberlaw Clinic

The Harvard Law School Cyberlaw Clinic, founded at the Berkman Klein Center, provides innovative, hands-on training to Harvard Law School students who, together with their clinical supervisors, offer legal and policy research, guidance, and representation to a variety of real-world clients. Clinic clients include individuals, start-ups, institutional entities, and research projects. Students enhance their preparation for high-tech practice and technology policy work, including public interest tech, earning course credit by working on real-world litigation, client counseling, advocacy, and contractual projects. Privacy within business, non-profit, and research contexts has been a significant area of focus for the Clinic. Data and information privacy and security are foremost among the concerns, and the Clinic's attorneys and students frequently address novel questions concerning the practical application of privacy and data security laws and crafting of privacy policies. The Clinic also works with clients and collaborators to inform the development of the law regarding privacy, vis-à-vis both private actors and the government. For example, last fall, the Cyberlaw Clinic submitted an extensive comment on an Advance Notice of Proposed Rulemaking by the Federal Trade Commission related to commercial surveillance and data privacy. The comment was submitted on behalf of various Berkman Klein Center projects and associates, including the Data Nutrition Project, the Lumen Database, the Risk Assessment Tool Database project, and the Youth and Media Project project. The comment provided concrete recommendations on achieving end-to-end data transparency from data collectors and processors for consumers.

Youth and Media

Our Youth and Media project ("YaM") focuses on the digital lives of youth and engages in research, advocacy, and development initiatives around youth privacy and digital technology. While digital technologies indeed provide creative, educational, and revolutionary possibilities for youth, data about young people is collected, stored, and searched at an unprecedented rate

and without material oversight. Neither youth nor their parents have control over how this information is handled by third parties, as data is frequently gathered, accessed, disclosed, copied, and sold without consent or knowledge. Meanwhile, online reputation has an increasingly large sway over a young person's future social, academic, and professional prospects.

The data privacy issues for youth are further complicated in educational settings, where increasingly powerful, innovative digital and AI-driven products and services offer schools new platforms and tools to shape, improve, and expand learning experiences, even in the face of continually shrinking budgets. However, these benefits are accompanied by critical privacy concerns, especially around the collection and use of student data. Our YaM team engages youth in participatory research to gather evidence-based insight on these digital privacy issues, advises government policymakers and non-governmental organizations on youth privacy considerations, develops educational tools, and works with multi-stakeholder initiatives to develop approaches that balance transparency and privacy considerations. This team has developed privacy and other learning resources, available in over 35 languages, and conducted one of the largest qualitative research projects on youth issues — with a special focus on privacy and social media — on the Internet in the U.S. The YaM projects' research insight into the digital lives of youth informed recent comments by the Cyberlaw Clinic to the Federal Trade Commission in connection with its proposed rulemaking on commercial surveillance and data security rulemaking.

Lumen

Lumen uniquely collects and studies online content removal requests, providing transparency and supporting analysis of the Web's takedown "ecology." Lumen seeks to facilitate research about different kinds of complaints and requests for removal – legitimate and questionable – that are being sent to Internet publishers, platforms, and service providers and, ultimately, to educate the public about the dynamics of this aspect of online participatory culture. Initially focused on requests submitted under the United States' Digital Millennium Copyright Act, Lumen now includes complaints of all varieties, including those concerning trademark, defamation, and privacy, both domestic and international. Currently, the Lumen database contains millions of removal requests and grows by more than 20,000 notices per week, from companies such as Google, Twitter, YouTube, Wikipedia, Reddit, Medium, Github, and WordPress. Because of recent dramatic increases in notice volume, in 2014 the project upgraded to a more robust website that provides more granular data and API access for notice submitters and researchers.

Digital Self-Determination

The Berkman Klein Center studies and advises governments on digital self-determination, an emerging concept by which we consider how data serves individuals. The focus remains firmly on the people impacted by data rather than the data systems or human power structures. BKC is a founding partner in the International Digital Self-Determination Network along with the national

government of Switzerland; the Centre for Artificial Intelligence and Data Governance at Singapore Management University; the Global Tech Policy Practice at the Technical University of Munich School of Social Sciences and Technology; and The GovLab at New York University. In collaboration with this network, the Center connects different actors from around the world to consider how to apply Digital Self-Determination in real-life settings in order to ensure that people everywhere are legally, socially, and technically empowered to participate in the digitally connected world. BKC's current work on digital self-determination research addresses educational systems and the support and use of student data by studying the dynamics of involved stakeholders like edtech providers, school administrators, and teachers. From this research, the project has made recommendations for stakeholders that clarified data ownership, access, persistence, and use.

BKC Policy Practice

Bringing together governmental, nonprofit, and private sector organizations to discuss the most pressing questions around emerging digital technologies, the BKC Policy Practice creates a space for learning, knowledge-sharing, and capacity-building. Participating organizations work with small, agile teams – composed of Harvard faculty, staff, BKC community members, students, and outside expert collaborators – to identify key challenges and create actional outputs such as UNICEF's Case for Better Governance of Children's Data report and the United States' National Action Plan on Responsible Business Conduct.

BKC Research Sprints

Since 2020 the BKC Research Sprint program has engaged international cohorts of early career academics and tech professionals to learn from international experts about a social technology issue tied to current events and related to data issues, surveillance, and/or AI. They then co-create outputs such as research reports, policy briefs, practitioner guidelines for participatory stakeholder engagement processes, technology oversight recommendations, Wikipedia entries, web dashboard mockups, and explainer infographics. We have held research sprints on privacy-related topics including surveillance of vulnerable populations, data co-operatives, transparency and takedown notices with Lumen, privacy in schools during the COVID-19 pandemic, and Digital Self-Determination.

Fellows and Affiliate Programs

The Berkman Klein Center's vibrant fellows and affiliate programs incorporate the work of leading privacy scholars. Members of our current fellows and affiliates class who write and advise on privacy and surveillance concerns include security technologist Bruce Schneier, Youth and Media scholars Leah Plunkett and Sandra Cortesi, privacy tools post-doctoral fellow Alexandra Wood, privacy scholar Neil Richards, digital labor scholar Ifeoma Ajunwa, and migration and surveillance scholar Petra Molnar.

(5) Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.

The Berkman Klein Center has been fortunate to receive prior court approvals as a *cy pres* beneficiary in connection with the following other class action suits:

- *Cy Pres Recipient Lundy et al. v. Meta Platforms Inc., No. 3:18-cv-06793* US District Court, Northern District of California, 2023 (proposed, pending final hearing)
- *Mounts v. Wells Fargo Bank*, Court of Appeals of the State of California, 2017
- *In re: Ashley Madison Customer Data Security Breach Litigation*, US District Court, Eastern District of Missouri, 2017
- *Nader v. Capital One*, US District Court, Central District of California, 2014
  Fraley v. Facebook, Inc., US District Court, Northern District of California, 2013
- *In re: Netflix Privacy Litigation*, US District Court, Northern District of California, 2012
- *Lanchester v. Washington Mutual Bank*, Superior Court of the State of California, 2012
- *In re: Google Buzz Privacy Litigation*, US District Court, Northern District of California, 2011
- *Raymond et al v. CarsDirec*t, Superior Court of the State of California, 2011

These past awards have been instrumental in supporting the creation and expansion of our privacy and related initiatives around digital technologies that advance the public interest, and have played a pivotal role in the Berkman Klein Center's outreach and public dissemination of our work in this area.

Grant Proposal

(6) Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?

Yes, Charity Navigator's most recent assessment gives Harvard University a 4-star rating out of 4 with a score of 96/100.

(7) Identify the organization's principal investigator or project director.

BKC Faculty Director, Jonathan Zittrain, will serve as the principal investigator. Since 2014, the board of directors has been led by Jonathan Zittrain, George Bemis Professor of International Law at Harvard Law School, Professor of Public Policy at the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and Director of the Harvard Law School Library. His research interests include the ethics and governance of artificial intelligence; battles for control of digital property; the

regulation of cryptography; new privacy frameworks for loyalty to users of online services; the roles of intermediaries within Internet architecture; and the useful and unobtrusive deployment of technology in education.

(8) Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

While the particular issues and projects BKC develops depend on the current issues, technologies, and social context of the time, we have always had a perennial focus on privacy, data autonomy and protection, and surveillance. Today the power of data to transform so many aspects of society, the negative impacts we see social media having on society, and the rise of a new form of AI in Large Language Models (LLMs) makes these perennial issues all the more salient. We feel an urgent need to contribute to conceiving and establishing a balance between the value of innovation and the prioritization of the highest social good, based on sound research, savvy social understanding, and creative approach.

As can be seen from our work described in section (4), we tackle hard problems with multiple complementary approaches: studying, connecting and convening, and educating and advising. The goals of this multiprong approach are to create new paths for (a) studying how to enable the safe use and protection of data, (b) convening faculty, students, fellows, and the public in broad and impactful conversations and (c) to advise in governmental, civil, and commercial stakeholders, to train the next generation of privacy experts, and to educate the public.

We will bring together our projects to create new, dynamic synergies that will increase their collective impact. And by bringing projects together, the work of the individual efforts will be enhanced. Thus, our activities will reflect both these collaborative and individual approaches.

The Center will welcome fellows and affiliates who are addressing issues of data, surveillance, and privacy, some of whom will work on projects independently while others may be embedded in existing Center projects. The Cyberlaw Clinic enrolls a cohort of HLS students every academic year and will continue to do so, with students working with clients on a wide range of privacy-related projects each academic year.

Projects like Privacy Tools, Youth and Media, and Digital Self Determination are leading research, education, policy, and development work, combining different methods of social science research, with a shared commitment to engage in efforts with a real-world impact. Youth and Media, for instance, is studying privacy in the context of newer (e.g., AI and generative AI) and more immersive technologies (e.g., virtual and augmented reality) with the aim of supporting youth, parents, educators, and policy-makers in better understanding privacy – by providing them with a set of tools (learning experiences, visualizations, and other educational resources)

and guidelines – and raise awareness about some of the major privacy challenges of living in a digital world. The Digital Self Determination project is looking to expand its work on privacy in educational systems and through its participation in the International Network for Digital Self Determination, to support governments in understanding approaches and creating policies that support the best use of data for data subjects' autonomy. The Center will surely continue to examine the online takedown ecosystem, as it has with the Lumen database project for many years, balancing a desire for notice transparency with an interest in respecting privacy.

This research would inform our advisory work. Berkman Klein is commonly asked to advise national, state, and regional governments and civil society, which we do through our Policy Practice. With this support, we will be able to expand our work with these organizations and will be able to engage experts from the aforementioned BKC research projects, early career scholars, and practitioners, an integration we have sought to resource. Similarly, Youth and Media will be able to expand and update their data and privacy resources for students, parents, and educators.

The Research Sprints will be able to expand and redefine its programs around new research focused on current issues and do so by bringing in expertise from projects such as Privacy Tools and other privacy- and surveillance-focused projects by faculty directors and associates.

We propose a three-year project. Every year we anticipate continued academic research from the Privacy Tools and Youth and Media project, the Cyberlaw Clinic's continued student education, litigation, client counseling, and advocacy on privacy issues, and educational efforts developed by the Research Sprint program on data, privacy and/or surveillance. In the first year we anticipate additional research production by Privacy Tools, Lumen, Youth and Media, and Digital Self Determination project, and continued advisory work by the Policy Practice. We will also build synergies between our projects and with our collaborators that will express themselves outwardly by year two and throughout year three.

(9) Explain why the organization is approaching the issue and/or opportunity in this way.

By resourcing existing projects more, connecting them with other projects, and creating new synergies across efforts, we will be able to both expand our privacy work and, more importantly, increase its impact on decision-makers and the public.

(10) Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

The Berkman Klein Center has the capacity to make full and productive use of $6,500,000 over the course of three years to deliver on the initiatives described. Settlement funds would be used to cover staffing, stipends for relevant fellows, honorariums for contributors to privacy work, and the cost of convenings via facility, food, travel, and other related expenses.

(11) Will the money be used to continue an existing project or create a new project?

The money would be used to continue and expand existing projects, to build connections between projects and with our community and broader networks.

(12) What target population will your organization's project benefit?

Our project will benefit the general public, governmental, civil, and commercial privacy stakeholders, young people and educators, higher ed students within and outside of the US, and the privacy and security communities.

Evaluation

(13) Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes, we agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how the remaining funds will be used. Harvard University has historically treated *cy pres* awards as gifts to the University and that all decisions regarding research and activities supported by such funds will be made solely by the University in accordance with its established policies and procedures.

(14) Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

For the research and scholarly aspects of this project, success is measured by external evaluations of the depth, quality, novelty, relevance, and robustness of the work. We rely in large part on the existing academic networks to help us improve our privacy work, both within and outside of our extended networks and via the informal review in internal discussions and formal review of academic publications.

Programs such as the research sprints, fellowships, workshops, and key events include formal survey evaluations by participants, as well as multiple informal touchpoints. Program teams use

these measures formatively throughout the programs and at the end of programs to determine what might be done differently in the next iteration.

Another measure is the uptake and influence of our privacy research within academic communities. This depends not only on the quality of the work but also its communication. Our communications staff tracks the reach and influence of our work through metrics, such as the number of times reports are downloaded and visits to web pages hosting materials. We also seek to quantify our reach into these communities by tracking the number and type of application and attendance at our sprints, convenings, and partner engagements.

Reaching advocacy and policy audiences is of critical importance to us. We share our findings and recommendations beyond academia, For our reports, policy briefs, and other outputs targeted at civil society organizations, private companies, and governments, we engage with our networks of public interest organizations, practitioners, and policymakers in evaluating the impact and influence of this work. Then we measure press mentions and appearances in both mainstream and relevant niche outlets, social media engagement across platforms, and in-person interactions such as speaking opportunities at conferences.

(15) Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Yes, we intend to use the results of the project in publications, conference papers, and/or presentations. The involved BKC faculty and researchers publish books, in peer-reviewed academic journals, technical reports, technical reports, op-eds and other online writing. They present at relevant conferences and give presentations to a wide range of audiences. In addition, we share our findings, interpretations, and recommendations to policy and technology stakeholders, educational audiences, and the public.

Please do not hesitate to contact me at 617-384-9123 if you have questions or if there is any additional information that would be helpful.

Sincerely,

Elisabeth Sylvan, Ph.D.
Berkman Klein Center for Internet & Society at Harvard University

Exhibit D

CENTER FOR DEMOCRACY & TECHNOLOGY

***In re Google Location History Litigation* Cy Pres Award Proposal**
October 5, 2023

I. Organization Information

1. Name of organization & contact details.

Name: Center for Democracy & Technology
Contact: Alexandra Givens, President & CEO
agivens@cdt.org; development@cdt.org
(202) 407 8840

2. Discuss the founding and history of the organization.

The Center for Democracy & Technology (CDT) is a nonpartisan, nonprofit advocacy organization that fights to protect consumers' privacy, civil rights and civil liberties in the digital age. We promote strong privacy and security protections for personal data, work to combat data-driven discrimination, and defend users' rights to free expression and privacy. CDT was founded in Washington, D.C. in 1994 and has operated a second office, in Brussels, since 2014.

Since our founding, CDT has been one of the leading U.S. and global organizations fighting to protect consumers' privacy. CDT's largest program is our Privacy & Data project, which works to protect consumers' interests in areas ranging from internet privacy to artificial intelligence, location data privacy, health privacy, workplace privacy and more.

CDT leads legislative efforts at the U.S. federal level and advocates to federal agencies. We also advocate directly to technology companies to improve their business practices and product designs, and serve as public interest leaders in multistakeholder fora where best practices and standards are set.

3. Describe the organization's current goals.

- Promote strong privacy & security protections for people's personal data
- Combat data-driven discrimination
- Promote responsible governance of AI
- Defend civil liberties by limiting government digital surveillance
- Advance equity and privacy considerations in the use of technology in education and in government services
- Promote solutions to the challenges of online trust & safety that protect individuals' rights to freedom of expression and privacy.

4. Provide a brief description of the organization's current programs.

CDT's **Privacy & Data Program** seeks to improve companies' data practices through legislation, regulatory action, and by changing industry norms. We believe that people's privacy must be protected by clear rules and practices enshrining data minimization, use limitations, and strict protections for sensitive data such as location information. We are a leading voice in the fight for a U.S. federal privacy law, and advocate directly to the Federal Trade Commission, Consumer Financial Protection Bureau, the Commerce Department and other agencies to combat invasive data practices.

Our Privacy & Data Program also advocates directly to companies to improve their business practices and product designs. We engage directly with in-house privacy teams on best practices, and create outside pressure for them to act. We also serve as public interest leaders in the multistakeholder bodies where privacy standards and norms are set, leading the World Wide Web Consortium (W3C)'s Privacy Interest Group, serving on the Internet Architecture Board, and participating in numerous advisory groups and fora. We have specific sub-projects focused on health privacy, student privacy, worker privacy, and disability rights & tech.

CDT's **Security & Surveillance Program** seeks to ensure reasonable checks and balances on governments' ability to access, collect, and store individuals' data. In addition to advocating for policy change, our Surveillance program engages directly with companies to urge their responsible handling of governments' data requests. We push back against overbroad geofence warrants, call on companies to require legal

process before sharing their customers' data, and oppose law enforcement's unfettered access to people's data via commercial data brokers. We were founding members of the Global Network Initiative, a unique body through which companies commit to transparency and assessments of how they protect their users' privacy rights.

CDT also has programs on Free Expression/Online Platform Governance; Equity in Civic Technology; Competition; and Elections & Democracy.

5. **Has your organization ever received a prior *cy pres* award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.**

Cy pres awards are an important source of funding for CDT's consumer advocacy work. We are honored to have been entrusted as recipients of cy pres awards in numerous prior cases. The awards have been unrestricted rather than allocated to a specific project.

2023	• *Quintero v. SANDAG* — $36,973.20
2022	• *In Re Carrier IQ, Inc. Consumer Privacy Litigation* — $275,671
2020	• *Borecki v Raymours Furniture Company, Inc.* — $45,634 • *TD Ameritrade* — $7,380
2019	• *Wahl v. Yahoo! Inc.* — $170.00
2018	• *N.P. v. Standard Innovation Corp.* — $39,780.31
2017	• *Fraley et al v. Facebook* — $10,407.98
2016	• *Byanooni v. Merrill Lynch* — $17,374.91 • *Aboudi v. T-Mobile USA, Inc.* — $408,203.94 • *In Re LinkedIn User Privacy Litigation* — $31,752
2014	• *Manjunath A. Gokare, P.C. v. Fed. Express Corp.* — $5.00 • *In Re Netflix Privacy Litigation* — $497,661
2013	• *Standiford vs. Palm, Inc.* — $365,149.44 • *TD Ameritrade Class Action* — $59,669.97
2012	• *In Re Google Buzz User Privacy Litigation* — $511,199.49 • *Valentine v. NebuAd, Inc.* — $75,000

2011	• "Flash Cookie" Class Action Settlement — $322,795
	  ○ *In Re Quantcast Advertising Cookie Litigation*
	  ○ *In Re Clearspring Flash Cookie Litigation*
	  ○ *Davis, et al. v. VideoEgg, et. al*
	• *Demetria Rodriguez, et. al., vs. NDCHealth Corporation et al.* — $255,007

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?**

Charity Navigator awards CDT 4 out of 4.

II. Grant Proposal

7. **Identify the organization's principal investigator or project director.**

Dr. Nathalie Maréchal, Co-Director, Privacy & Data Program
Eric Null, Co-Director, Privacy & Data Program

8. **Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.**

CDT seeks to expand our Privacy & Data Program to better protect consumers' privacy through legislation, regulation, and improved company practices. Through three lines of work, we seek to: (i) secure robust privacy protections for location information and other sensitive data through comprehensive legislation and regulation; (ii) push companies to improve their data practices and product designs; and (iii) advance affirmative, privacy-protecting approaches to online advertising to displace current behavior-based models. These efforts build on CDT's existing subject matter expertise and strong working relationships with federal policymakers, company decision-makers, and allied consumer groups. The Award would allow us to scale up and expand this work, as described below.

(1) Securing Better Consumer Privacy Protections for Location Information & Other Sensitive Data

Goal: Secure robust privacy protections for location information and other sensitive data by advancing comprehensive privacy legislation and effective regulations.

Context: Recent events have increased public awareness about the sensitivity of location information and the lack of adequate protections for this and other sensitive data. In the wake of the 2022 *Dobbs* decision, investigative reporters showed that they could easily purchase location information revealing where people who visited a Planned Parenthood facility had come from and where they went next. Reports showed that marketing companies are using location data to target ads to people in sensitive locations such as a doctor's office. Law enforcement has purchased commercially-available location data to issue geofence warrants, and more.

CDT has been a leading voice emphasizing the sensitivity of location data and the need for meaningful privacy protections. During the major legislative push that led to the introduction and movement of the American Data Privacy & Protection Act in 2021-2023, CDT contributed legislative recommendations, testified before Congress, and raised public awareness about the risks and need for a strong comprehensive privacy law. The bill's overwhelming bipartisan vote out of the House Energy & Commerce Committee and various state bills show that attitudes are changing — and the FTC's increased enforcement against companies that collect and sell consumer location data shows the potential (and the challenges) for enforcement actions to protect location data too. CDT is eager to build on this momentum, to increase public awareness about the need for strong consumer privacy protections and to secure those protections now.

Activities:

- Advocate for Congress to adopt robust protections for consumer privacy, with a particular focus on (i) protecting sensitive information such as location data, and (ii) ensuring any framework imposes baseline privacy requirements (rather than relying on users' notice & consent, which can easily be worked around or manipulated). Provide public interest feedback and actionable advice on legislative proposals; educate policymakers on the significance of privacy issues;

and support diverse public interest groups from across the political spectrum to engage in the fight for strong privacy protections.

- Serve as a strong consumer voice in existing and anticipated federal agency processes impacting consumer privacy, including Federal Trade Commission (FTC) rulemaking on commercial data practices and Consumer Financial Protection Bureau (CFPB) efforts on commercial data brokers. Develop strategies for other agencies, such as the Federal Communications Commission, to use their authorities to protect location privacy. File comments & support others' submissions to build a strong evidence base for robust, protective rules.

(2) Directly Improving Companies' Data Policies, Practices & Designs

Goal: To push companies to improve their data policies, practices, and designs through direct advocacy and public interest leadership in the multi-stakeholder fora where industry best practices and norms are set.

Context: Given the slow pace of legislative and regulatory efforts, CDT believes consumer advocates must also advocate *directly* for companies to improve their data policies, practices and designs. CDT already does this in several ways, which include engaging directly with in-house privacy and product teams to recommend changes to company data practices, while creating outside pressure for them to act. For example, we successfully convinced Apple and Google to develop a standard to reduce the risk of Bluetooth location trackers (like Airtags) being misused for stalking people, which was the result of two years' direct advocacy by CDT and the National Network to End Domestic Violence.

CDT publishes reports and best practice guides for how companies should protect consumers' data. We also serve as a strong public interest voice in multi-stakeholder fora where standards and norms are set, ranging from internet standards bodies like the IETF (where we are working to make the Apple-Google Bluetooth location tracking proposal become an industry standard) and W3C, to efforts by the World Economic Forum, BBB, BSR, and others. In recent years, we have expanded our strategy to include investors as a tool to shape company behavior, elevating "responsible data practices" as an ESG investment criterion against which companies should be scored.

CDT is eager to build on this work, at a time when rapid advancements in AI and national security debates are increasing public attention on businesses' data practices and thus creating new momentum. Specifically, CDT seeks to hire new staff who can delve more deeply into companies' data practices at the operational level, and to grow our ESG/investor-focused work from a pilot effort to a formal program.

Activities:

- Hire 1-2 experienced data privacy professionals who have managed effective data privacy programs within companies or industry associations, and can boost CDT's efforts to drive best practices in key industries including the data broker, automotive and advertising sectors.
- Develop and advocate for the adoption of privacy-protecting measures, such as basic data hygiene (for example, understand the data they collect, reduce what they collect to what they need, delete data when no longer needed), adopting privacy controls that require opt-in consent for any location data not necessary for the service; improving policies around geotargeting; improving user notices; and improving global controls (see more on this below).
- Hire 1 new professional to lead CDT's work elevating consumer privacy & responsible data practices as a criterion for formal measurement within ESG. This work will focus on urging the leading global ESG benchmarking organizations to include effective measures for data privacy & governance in their benchmarking efforts, working with investors to craft shareholder proposals for introduction during company Annual General Meetings, and providing technical and policy expertise to inform these efforts.

(3) Transforming Online Advertising to Protect Consumer Privacy

Goal: To support the growth & adoption of an online advertising ecosystem that moves away from pervasive tracking and respects users' privacy.

Context: The next few years could serve as an inflexion point for online advertising. New data privacy regulations and growing public dismay at the behavioral-tracking model of online advertising are creating new opportunities for the ecosystem to change. At the same time, work is needed to establish how such change can work in practice – meeting

consumers' needs, and providing a sustainable funding model for journalism, social media sites, and other services that need advertising revenue to survive.

The capabilities for tracking online activity and the protections that users can count on are primarily determined not by legislative bodies, but by industry self-regulation (discussed above) and by the implementation of internet standards by large and small tech companies. Google's Privacy Sandbox and Apple's App Tracking Transparency are particular examples, but new advertising-related proposals are widespread and may reshape how advertising is targeted, distributed and measured. These proposals are often developed and adopted inside companies or inside internet standards bodies like the IETF and W3C where consumer advocates are barely represented. CDT has a unique history as one of the few public interest voices in these fora, and we wish to grow this work at a critical time to advance privacy-preserving advertising that actually serves consumers' needs.

Activities:

- Work to standardize simple global opt-outs, including the Global Privacy Control.
- Support standardization (and improvement) of easy-to-understand privacy labels. These have seen recent uptake in mobile device app stores, but lack standardization or application to settings outside centralized control.
- Support mechanisms to address the priority question of ad measurement. Current privacy debates are stymied by advertisers' claims that they need to share users' data with third parties to measure the effectiveness of ads: advancing privacy-preserving methods for online measurement will help clear the way for stronger legislative protections.

9. **Explain why the organization is approaching the issue and/or opportunity in this way.**

Please see "Context" section for each goal outlined above.

10. **Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.**

Requested Funding Amount: $3 million over 3 years ($1 million per year).

The money will be used to support the salaries of key personnel to conduct the activities described above, with some additional budget for travel and events. While we have broken out the three workstreams for clarity and explanation, they are highly complementary and part of an integrated strategy. For example, our industry-facing advocacy (Workstream 2) is most effective when it is backed by momentum in legislative and regulatory efforts (Workstream 1); and both our legislative/regulatory advocacy and industry-facing advocacy will be most effective if public interest voices have helped craft alternative, privacy-affirming models for advertising (Workstream 3).

		Year One	Year Two	Year Three	
Workstream 1 (Policy)					**W1 Total**
Salary & Benefits	Co-Director, Privacy & Data	$193,558	$193,558	$193,558	**$1,044,271**
	Policy Counsel, Privacy & Data	$96,428	$96,428	$96,428	
Travel & Events		$5,000	$5,000	$5,000	
Overhead		$53,104	$53,104	$53,104	
Total		$348,090	$348,090	$348,090	
Workstream 2 (Industry Advocacy)					**W2 Total**
Salary & Benefits	Senior Counsel, Privacy & Data	$131,215	$131,215	$131,215	**$1,411,231**
	Senior Counsel, Privacy & Data	$131,215	$131,215	$131,215	
	Senior Counsel, ESG	$131,215	$131,215	$131,215	
Travel & Events		$5,000	$5,000	$5,000	
Overhead		$71,765	$71,765	$71,765	
Total		$470,410	$470,410	$470,410	
Workstream 3 (Advertising)					**W3 Total**
Salary & Benefits	Senior Technologist	$143,310	$143,310	$143,310	**$544,498**
Travel & Events		$10,500	$10,500	$10,500	
Overhead		$27,689	$27,689	$27,689	
Total		$181,499	$181,499	$181,499	
		Year 1 Total $1,000,000	**Year 2 Total $1,000,000**	**Year 3 Total $1,000,000**	**Grand Total $3,000,000**

11. Will the money be used to continue an existing project or create a new project?

Grow CDT's existing Privacy & Data Program.

12. What target population will your organization's project benefit?

All people deserve and benefit from increased privacy protections, but the needs are particularly acute for historically marginalized communities, for whom new technologies and data use can drive discrimination and deepen inequality.

CDT prioritizes this lens of equity and justice across our work. Some examples include our focus on the implications of government surveillance for communities of color; the impact of student 'safety' monitoring technology on the privacy and civil rights of LGBTQ+ students, disabled students, and students of color; and the discriminatory effects of targeted advertising and the use of AI in hiring, lending, housing, credit, for historically marginalized communities.

A key way in which CDT works is by partnering with organizations that represent impacted communities to help them engage on tech policy issues. Our collaboration with the National Network to End Domestic Violence to combat abuse of Bluetooth location tracking devices is one example of this; we also have a joint fellow with the American Association of People with Disabilities, and work closely with a wide range of groups focused on racial justice, LGBTQ+ rights, immigrants' rights, workers' rights, reproductive rights, and the rights of older Americans.

We collaborate with these groups to identify problems, develop informed solutions, and increase the big tent of voices calling for stronger protections in how technology is designed and governed. This strategy has allowed CDT to successfully shift the concern of technical considerations from a focus on the owners, operators, and technology itself to a focus on the safety, dignity, and freedom of the users and impacted communities.

III. Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes. CDT has regular processes in place to track and report progress on allocated funds. We are the recipient of numerous foundation grants that require annual or semi-annual reporting, and are accustomed to generating mid-grant financial reports as well as substantive project updates.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

CDT seeks to shape public policy decisions and change company practices to protect people's privacy, civil rights and civil liberties. These changes take time, so in addition to tracking outcomes we look to interim indicators of success.

For our policy work, these indicators include how often policymakers turn to CDT for expert advice, and how frequently our recommendations are reflected in policymakers' talking points, legislation, oversight letters, and executive actions. We also monitor how other public interest organizations cite CDT's work, adopt our arguments, seek advice, and join our advocacy letters.

For our direct-to-industry advocacy, our success indicators include how often companies turn to CDT and whether they act upon our recommendations. For example, whether CDT is invited to serve on companies' advisory councils and to brief internal teams, and how effective we are in those activities.

We actively track press hits, which includes major outlets like the Washington Post, New York Times, CNN, NBC, NPR and the AP. In addition to broad dissemination, we do targeted outreach to policymakers, companies, advocates and impacted communities, speaking at conferences or holding custom briefings.

In addition to routine tracking, each project has a monthly check-in with senior leadership to ensure projects are advancing on track towards their goals.

15. **Does your organization intend to use the results of the project in any publications, conference papers, and presentations?**

Yes. We anticipate publishing reports and shorter public-facing pieces (like op-eds and fact sheets) on topics such as best practices for companies to protect users' privacy, and recommended policy changes. We anticipate filing comments with relevant federal agencies to raise awareness of privacy harms, recommend agency interventions, and create an evidentiary record for change. We hope and expect that we may again be called to provide Congressional testimony.

CDT routinely engages with the press and uses short-form writing (op-eds, blogposts, social media posts) to raise public awareness about privacy harms and ways to address them. We also give presentations and attend privacy-related conferences to advocate for strong privacy policies and protections.

Exhibit E

GEORGETOWN LAW
Center on Privacy & Technology

Proposal for Cy Pres Funding:
In re Google Location History Litigation

Organizational Information

1. Name of organization.
Center on Privacy & Technology at Georgetown Law ("the Privacy Center").

2. Founding and history.

The Privacy Center was founded in 2014 to bring a civil rights and racial justice lens to legal and policy debates about privacy, technology and surveillance in the digital age. We undertake research and advocacy to expose and mitigate the disparate impact of government and corporate surveillance on historically marginalized communities. Situated at Georgetown Law Center, we also have a pedagogical mission to train the next generation of civil rights advocates in a root-causes approach to technology law and policy. Our founding faculty director is David Vladeck, the A.B. Chettle Chair in Civil Procedure at the Law Center, and former director of the Bureau of Consumer Protection of the Federal Trade Commission. We have five faculty advisors -- Anupam Chander, Julie Cohen, Laura Donohue, Laura Moy and Paul Ohm -- each of whom is a nationally or internationally recognized scholar in the field of privacy law. We have a full time staff of seven, led by our Executive Director, Emily Tucker.

Since our founding, we have published groundbreaking research and led coalition-based advocacy that has resulted in pro-privacy policy change in a variety of contexts. For example, our 2016 report, *The Perpetual Line-Up: Unregulated Police Face Recognition in the United States,* was the first report to document the extent of police use of facial recognition technology in the United States. That report, along with four subsequent reports on different aspects and uses of facial recognition technology, helped to create what has essentially become a new field within civil society of organizations working against face recognition specifically, and against algorithmic technology in law enforcement more generally. Since the release of *Perpetual Line-up,* more than two dozen states and municipalities have introduced legislation to regulate or ban law enforcement use of facial recognition, and several members of Congress have also introduced bills to impose limits at the federal level.

In 2022, we released *American Dragnet: Data-Driven Deportation in the 21st Century*, the first report to quantify data-surveillance by Immigration and Customs Enforcement (ICE). After analyzing the responses to hundreds of Freedom of Information Act requests, we were able to estimate the number of people whose personal data has been shared with ICE by state DMVs, by utilities companies, and by data-brokers. As a direct result of our discovery that utilities companies were selling customer information to data brokers, in December 2021 Equifax announced it would no longer sell utilities data to ICE. We also partnered with the immigrant rights organization CASA to research the flows of data created and managed by public agencies in Maryland to federal immigration authorities. We discovered, among other things, that ICE was remotely accessing state motor vehicle records and running facial recognition searches on driver images. We then collaborated with CASA to develop legislation to prevent this kind of warrantless rummaging through public datasets in Maryland. The Maryland Driver Privacy Act went into effect in 2022 after the legislature overrode the governor's veto.

These are just a few examples of the impact our work has had, and they are a good illustration of our mission, vision and change-making strategy.

We believe that our organization is particularly well suited to represent the interests of the class in this litigation. Almost all of our programmatic work (see question 4 below) directly addresses the struggle to protect privacy in the context of life lived on and through the internet. Our research on surveillance in the law enforcement and immigration contexts has specifically addressed location data, and the privacy and civil rights harms that arise from the location tracking that is made possible through commercial apps and digital services that incorporate geolocation, as well as through technologies (such as automated license plate readers) whose primary purpose is location tracking. In our policy advocacy, we have challenged the consent-based frameworks that often form the basis of corporate policy frameworks, not only because of the impossibility for most users to consent meaningfully, but because companies often build such redundancy into their data collection systems that effective opt-out is not possible. All four of the projects we are proposing for cy pres funding will include an aspect relating to location data.

3. Describe the organization's current goals.

Our long term goal is to see the right to privacy recognized, protected and — most importantly — *realizable* for all people. We believe that strong comprehensive federal privacy legislation will not be possible without a much broader base of educated, engaged and organized citizens. Therefore, our medium-term goals focus on building the capacity of individuals (especially new lawyers), communities, and other civil society organizations to understand the privacy and civil rights implications of digital technologies, and to participate politically in the important decisions now being made about what limits -- if any

-- will be imposed on the development and use of such technology. We collaborate with other advocates and academics, as well as with community based organizations across the United States, to identify new areas for research, and to develop advocacy strategies that use local, state and federal legal and policy frameworks to make progress towards a world where privacy protects everyone.

4. Current programs.

We currently have four program areas which house our active research and advocacy. The Privacy Center staff also offer courses almost every semester for law students, including our Surveillance & Civil Rights practicum course, which is a mini clinic that places law students at non profit organizations where they undertake 20 hours per week of fieldwork on projects related to privacy in the digital era. Finally, we host the Color of Surveillance conference, the 6th iteration of which will take place in the fall of 2024.

Surveillance in the Criminal Justice System

This program area focuses on the digital technologies that are increasingly built into the daily operations and decision-making of police, prosecutors, judges and corrections officials. We have released five reports on facial recognition technology, and published an interactive website and digital public education tool illustrating the way that algorithmic models are changing law enforcement systems and impacting the experiences of people within those systems. We are currently investigating the new DNA analysis technologies that are being developed by private corporations and sold to local law enforcement agencies.

Worker Privacy & Commercial Data Practices

Our work in this program area focuses on the failure of commercial privacy laws to protect the rights of both consumers and workers in the digital era. Currently our two most active projects are (1) the Stop Discrimination by Algorithms Act (SDAA), a bill introduced in the DC legislature to hold corporations accountable for discrimination in their algorithmic decision making systems, and (2) a long-term investigation of surveillance of grocery store workers and the impact of that surveillance on their ability to organize. We also participate regularly in advocacy with the various federal agencies charged with protecting consumers and workers. For example, last year we submitted a letter to the Federal Trade Commission's Advanced Notice of Proposed Rulemaking focusing on the FTC's authority to regulate corporate production and sale of technologies that impact workers.

Surveillance of Immigrant Communities

Our work in this program area focuses on the surveillance of immigrant communities by government agencies and corporations, and the impact of that surveillance on all Americans. Our first major report on this issue, *American Dragnet: Data-Driven Deportation in the 21st Century*, was released in 2022. The report received widespread attention in the media, provoked an oversight letter from Senators Markey (D-MA) and Wyden (D-OR) ICE Acting

Director Johnson, and has subsequently been cited extensively by other academics and researchers, reporters, policy-makers and community based organizations running campaigns to limit ICE surveillance in their communities. In early 2024, we will release our next report, which examines the Department of Homeland Security's DNA collection practices.

Surveillance of Families

This is a new program area for which we are still in the process of fundraising, and which a cy pres grant would substantially support (see below). We define "family surveillance" broadly to include everything from the surveillance of access to reproductive healthcare to the surveillance of families involved with the child welfare system. In June 2022, in response to the leaked opinion in *Dobbs v. Jackson Women's Health Organization*, the Center hosted a virtual edition of our Color of Surveillance conference called, The Color of Surveillance: Policing of Abortion and Reproduction. More than 250 participated in the live event. In November 2023 we submitted comments on the Department of Health and Human Services' Section 504 rulemaking on disability discrimination. Our comments called on HHS to look at the frontend of the family policing system — specifically, how disability discrimination shows up in reporting, screening, and investigations, including through surveillance and the use of data-driven tools.

5. Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.

In January 2023 we received a cy pres award of $1,006,583, as a beneficiary of the settlement in *In re Google LLC Street View Electronic Communications Litigation*. We are using the funds to support salary and non-salary costs associated with various projects across all of our program areas described above. To date we have spent approximately half of the funds awarded, and submitted two reports to Court detailing the activities we have undertaken, which are publicly available on the Google Street View settlement website.

6. Has your organization been reviewed or rated by Charity Navigator or similar entity?

The Privacy Center itself is not rated, but Georgetown University is rated by Charity Navigator as a four star institution with an overall score of 96%.

Proposal

7. Principal Investigator.

Emily Tucker, Executive Director

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

We are requesting $1.9 million in cy pres funds to support four initiatives. Two are existing initiatives of the Privacy Center which we would like to expand, and two are new projects in the early stages of development. To fully realize any of these projects will require funding beyond what is possible within our current annual operating budget. A cy pres grant of $1.9 million would allow us to execute all four of these projects at scale, with broad distribution and impact.

- **Digital privacy curriculum for middle and high school students.** Following the release of Cop-Out: Automation in the Criminal Legal System, our interactive website illustrating the use of algorithmic tools in policing and punishment in the U.S., we were invited to present the website at a D.C. area high school. This inspired us to begin developing a digital privacy curriculum specifically for middle and high school students in a style similar to the Cop-Out tool but encompassing a wider range of topics. We are designing the curriculum to be delivered as a set of teach-in style workshops during which students will become experts on the privacy implications of the technologies that they are voluntarily and involuntarily interacting with every day. The curriculum will involve the students in teaching the substantive material to each other, and will provide group exercises around which students can build their own conversations about the larger political and philosophical questions of life lived online. Finally, the curriculum will include a robust digital self defense training to teach students best practices for protecting their individual privacy. We are working closely with Georgetown's Street Law Program to develop the curriculum and hope to pilot the workshops in the D.C. area, also through a partnership with Street Law, in the fall of 2025. A cy pres grant would allow us to run the program in multiple schools on a yearly basis, to develop a set of highly designed interactive digital tools (similar to Cop-Out) to support the in-person workshops, and eventually to release the full curriculum as an open-source resource for educators, students, and community groups. Relevant to the interests of the class in this litigation, the curriculum will include a unit on location tracking -- what it is, how it works, what kinds of technologies it is built into, and methods for opting out.

- **Fellowship program expansion.**
  Since the founding of the Privacy Center, our fellowship program has been a key aspect both of our internal staffing structure and of our mission to provide advanced training to new lawyers, advocates and researchers in our field. After their time at the Privacy Center, our fellows have continued their careers in privacy law and policy through roles in government, non-profit organizations, universities and even tech companies. Having seen the impact that Privacy Center alumni are already having, we have decided to invest more deeply in our fellowship program to help build an even stronger pipeline of public interest technology professionals. We are working to convert our existing program, which is a one year program through which we host 1-2 fellows at a time, into a robust 2-year training program that will eventually include 4-6 fellows at a time.

Our fellows have always been integrated as junior staff members into all of our programmatic work, and this will remain the keystone of our new training program. But in addition to serving as team members on our research and advocacy projects, fellows in the new program will benefit from a series of special trainings and workshops, a mentorship program pairing fellows with senior leaders in our field, and career planning support for their post-fellowship professional life. The training program will include substantive continuing education style modules on topics relevant to our work from law, policy and technology. For example, we are planning a mini course on antitrust, one a workshop on machine learning, and (relevant to the interests of the class in this litigation) the application of the 4th Amendment to location tracking after *Carpenter*. Fellows will also receive skills and methods trainings on, for example, participatory action research, media communication skills, advanced writing for public policy, best practices for writing public records requests, and corporate accountability research, among others. A cy pres grant would allow us to launch the expanded fellowship program more quickly, to increase the number of participants in each cohort, to fully fund the mentorship program, and to engage external partners to provide some of the curriculum trainings.

- **New Research Project: Surveillance Tax on Essential Services**
  Within our program area on family surveillance, we are in the early stages of a new research project to investigate the ways that bureaucracies which administer essential benefits and services (especially to low income families) increasingly require people to submit to various forms of digital surveillance as a condition of receiving services. For example, twenty-four states require people who have qualified for unemployment insurance to submit to face scans in order to access their benefits. Child welfare agencies are increasingly relying on algorithms (which are often inaccurate or biased) to make decisions about when to remove children from their homes. The federal Department of Housing and Urban Development is subsidizing the installation of powerful video surveillance systems, enabled with facial recognition software, throughout public housing developments all over the country. Poor individuals and communities often depend on the services and benefits that these government agencies provide for their survival, and avoiding the surveillance upon which the bureaucracy increasingly depends is simply not an option.

  The purpose of this project is to: (1) create the first systematic catalog of the surveillance technologies being deployed in the administration of essential services and benefits for economically disadvantaged groups; (2) describe the disparate impact of essential services surveillance on communities subject to high levels of policing; (3) characterize the privacy and civil rights impacts of conditioning access to essential services on enhanced surveillance.

Our investigation will survey the federal and state systems involved in administering public programs in four key areas: child welfare, housing and homeless services, food assistance programs, and unemployment benefits. We will collect comprehensive data about the number and types of surveillance technologies being used in each area. We are primarily interested in three different types of surveillance: (1) biometric surveillance as an aspect of the application for, or the process for receiving, public services and benefits; (2) the use of data-intensive algorithms to administer benefits and services or to make decisions about when and how a government agency will intervene in a person's life; (3) the use of video and photographic data collection and surveillance in the physical environments built or shaped by programs for economically disadvantaged communities.

Our goal is to catalog each surveillance technology being used in each aspect of the digital bureaucracy, categorize each technology by type, and provide the demographic breakdown of the impacted population in each instance. We will also research and evaluate the privacy policies and practices relevant to all data-intensive surveillance technologies, with a particular focus on the availability to police of data gathered by government agencies that do not have a law enforcement mandate. We will partner with community based organization to understand the impact of what we are calling the "surveillance tax" on individual and public health. We will craft a set of policy recommendations to address the harms of non-optional and administratively unnecessary surveillance in the government systems involved in the administration of benefits and services for economically disadvantaged groups. We will publish our findings and recommendations in a report and make all raw data available publicly on our website. A cy pres grant would allow us to hire a new full time staff member to lead the project, which is what is necessary in order to execute the project at scale.

- **Guidance on Algorithmic Technologies for Municipal Policymakers.**

  One of the many problems with the lack of comprehensive federal privacy laws is that new digital infrastructure is often put in place through procurement processes outside of any public or legislative deliberation. The federal contracts for new digital systems and networks sometimes receive some scrutiny, but at the state and local levels the oversight is usually minimal to nonexistent. After the release of ChatGPT last year, the Privacy Center began receiving a steady stream of requests from policymakers, and in particular from municipal policymakers, wanting advice about how to understand the risks and potential benefits for their constituents of algorithmic technologies trained on massive data sets. City council members, mayors, and staff within local government agencies are being bombarded with marketing materials from corporations selling various digital products under the "AI" label, promising to increase bureaucratic efficiency, accuracy and fairness. Rather than continuing to provide case by case technical support, the Privacy Center is working on a set of guidelines to help local policymakers (1) understand how the different technologies marketed as "AI" actually work; (2) identify

potential privacy and civil rights harms that may flow from the adoption of a particular technology in a particular context; (3) evaluate whether procurement is an appropriate process for the acquisition of a new technology or whether more robust democratic process is necessary; (4) develop local laws to put guardrails around the acquisition and use of algorithmic technologies by government agencies. Our guidance will explicitly address the specific harms of location tracking, and give policymakers the tools they need to identify which technologies include a location tracking component, to assess the appropriate of location tracking based on the context, and to ensure that location tracking is never covert. Support from a cy pres grant would allow us to produce the guidelines in the form of a comprehensive municipal toolkit, to present the toolkit in a variety of fora for audiences of both policymakers and advocates, to make the toolkit available for free on our website, and to continue to provide some individualized technical support to policymakers who are interested in implementing some of the ideas in the toolkit.

9. Explain why the organization is approaching the issue and/or opportunity in this way.
The four projects for which we are requesting support together represent different aspects of our theory of change. We know that in order for privacy rights to be realized it is not enough to have them enshrined in law. If the public does not know how and to what degree their privacy is being violated, and if they do not understand what is at stake in the violation of individual and collective privacy, they will not be willing or able to make demands about privacy from their government.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

The following are estimates of the approximate costs and timeline for each proposed project:

Digital privacy curriculum -- ($300k over 2 years). Funds will support the salary of one senior staff member and one to two fellows over the course of two years, costs associated with graphic design and web design, costs of external consultants on secondary education curriculum design, costs for travel and project materials.

Fellowship -- ($750k over 3 years). Funds will go primarily to fellow salaries, and will also help to pay for training modules, fully fund the mentorship program, and support individual personal development funds for each fellow.

Surveillance tax research project -- ($600k over 3 years). Funds will support salary costs for a new full time associate and partial salary of the Privacy Center's Director of Research & Advocacy, fees associated with public records requests, costs of Freedom of Information Act litigation if necessary to obtain key records, costs of producing and publishing the final report.

Guidance on algorithmic tech for municipal policymakers -- ($250k over 2 years). Funds will be used to support partial salary for one associate and the Center's Executive Director, who will lead the project. Funds will also support the presentation of the guidance in various fora including conferences and webinars, focusing on audiences of policymakers and advocates.

11. Will the money be used to continue an existing project or create a new project?
The digital privacy curriculum and fellowship program are existing initiatives which we hope to expand. The new "surveillance tax" research project and the guidance on algorithmic tech for municipal policymakers are new projects which we have begun to develop but which we cannot complete without new funding.

12. What target population will your organization's project benefit?
We believe that while each project takes a distinct strategic approach, all four projects will have a positive impact on the future of internet privacy in the U.S., and thus will benefit everyone in the country. Obviously, the digital privacy curriculum is designed to have immediate positive impacts for youth, and the fellowship program will increase opportunities for young people interested in public interest technology careers.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months, informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?
Yes

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

Each of the projects for which we are requesting support has the clear potential to promote internet privacy by adding to existing knowledge about the privacy harms of digital technologies, by conveying that knowledge to a wide range of people and system actors, and by training the next generation of lawyers and advocates to use the knowledge they have to carry the fight for privacy forward. For each project, the level of success will depend on the quality of execution, and we have systems in place for ensuring that all of our work meets a high standard of rigor and impact. We typically evaluate all of our research, advocacy, and education projects at the outset and on an ongoing basis to determine (1) does the project align with the Privacy Center's mission and vision; (2) is the project progressing according to the original timeline, and if not what adaptations need to be made; (3) are we reaching the intended audience and, if not, what adaptations need to be made.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Yes, as described above, the research on surveillance in essential services will be published in the form of a Privacy Center report and made publicly available on our website, along with the raw data we collect through our research. Our digital privacy curriculum for highschool and middle school students will also ultimately be published online as an open source resource for educators and community groups.

Exhibit F

ConnectSafely

VIA EMAIL

Larry Magid
larry@connectsafely.org
ConnectSafely
3481 Greer Rd.
Palo Alto, CA 94303
650-523-4950

Tina Wolfson
Ahdoot & Wolfson
1016 Palm Ave
West Hollywood, CA 90069

Michael Sobol
Lieff, Cabraser, Heimann & Bernstein
275 Battery Street, Suite 2900
San Francisco, CA 94111

Re: *In re Google Location History Litigation* Proposed Cy Pres Award

Dear Ms. Wolfson and Mr. Sobol:

Thank you for the opportunity to propose a project funded by *In re Google Location History Litigation*. The information you requested is as follows.

Organization Information

1. Name of organization
2. Discuss the founding and history of the organization

ConnectSafely, Inc. was founded in 2005, initially for the purpose of educating parents and youth about the safe use of social media. It was at first a subsidiary of another non-profit, but in 2015, it was incorporated as ConnectSafely, Inc. and given 501C-3 status by the IRS. Its co-founder, Dr. Larry Magid (Ed.D), serves as President and CEO. Maureen Kochan is Vice President and COO. Other staff and board members are listed in the About Us section of ConnectSafely.org.

The organization has always and continues to provide educational materials and programs to parents and children through guides, blog posts, videos, animations, podcasts and other media, including TV and radio appearances, newspaper and magazine stories, speeches and presentations. It operates a website, ConnectSafely.org, that reached more than 1.6 million unique visitors in 2022.

In 2014, ConnectSafely was appointed the official U.S. host of Safer Internet Day, an international event that takes place in more than 100 countries. This appointment had to be endorsed by a US government official (a member of Congress) and approved by a committee of the European Commission as well as an international NGO that coordinates Safer Internet Day. ConnectSafely conducts annual in-person and online Safer Internet Day events in partnership with the National PTA and other non-profits as well as corporate sponsors.

3. Describe the organization's current goals.

ConnectSafely's goal is to continue to provide parents, youth and educators with practical information on how to protect young people in their use of connected technology regarding safety, security and privacy, including location sharing, digital civility, protection from scams as well as misinformation and disinformation.

We also now have programs and resources for senior citizens, the LGBTQ community and parents of very young children.

4. Provide a brief description of the organization's current programs.

ConnectSafely creates and publishes parent and educator guides and shorter Quick Guides on a wide range of topics, including specific issues and risk factors and popular online services and apps. A complete list, with links, can be found at connectsafely.org/allguides.

The organization creates videos on important topics regarding safety and produces a twice-monthly podcast ("Are We Doing Tech Right?") and a twice-weekly radio segment ("ConnectSafely Report") that's heard on more than 50 CBS News Radio affiliates in the U.S. and Canada.

We are also the official U.S. coordinator of Safer Internet Day, which takes place in February. In addition to in-person and virtual events, we sponsor local events in communities across the country, providing educational resources and financial support to local educators and community organizations.

We publish a newsletter and maintain a website that received 1.6 million unique visitors in 2022. Our 2022 impact report is here.

5. Has your organization ever received a prior cy pres award? If yes, please cite the applicable

case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) Funded.

In 2015 ConnetSafely received a $500,000 *cy pres* award in the case of Angel Fraley, et al., Plaintiffs, v. Facebook, Inc., Defendant. It was an unrestricted grant that did not require a proposal. The funds were used for a variety of projects, including creating parent and educator guides on social media safety, presenting at conferences on subjects related to online safety and privacy and support for Safer Internet Day, where ConnectSafely serves as the official U.S. host.

6. Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?

Yes. Charity Navigator gave us a rating of 73%. Impacting our score were zeros in three categories: Whistleblower Policy, Document Retention & Destruction and Tax Form Posted. We have addressed these issues and look forward to a new and much higher rating once Charity Navigator evaluates our upcoming 2023 990 tax return.

Grant Proposal

7. Identify the organization's principal investigator or project director.

The principal investigator will be Larry Magid, Ed.D, who will supervise the project alongside ConnectSafey COO Maureen Kochan.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

Location-Sharing Risks and Benefits

We have reserved the domain LocationSafety.org, which, alongside ConnectSafely.org, will host resources to help all internet users, but especially parents and families, better understand the pros and cons of sharing their location with family members or close friends or associates as well as with apps and companies. Resources will include an in-depth guide, a concise (two-page) Quick Guide, videos for parents and teens, lesson plans for classrooms, and animations for younger children. We will also provide short-form advice on social media and through our twice-weekly ConnectSafely Report radio segment for CBS News, as well as in-depth discussions of the issue on our podcast, "Are We Doing Tech Right?" As with all of our areas of expertise, we will use other media such as TV and radio appearances, newspaper columns and op-eds, presentations at conferences and distribution of resources to our local school and community organization partners.

The materials will explain the risks associated with location sharing, including the possibility of relationships deteriorating, as well as risks associated with abusive relationships, including with a family member or romantic partner. There will be information on how companies, including operating system providers, websites, app developers and other entities, use location information and how to prevent, control or remove their access to that data. There will also be resources on device security as it relates to location information.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

Nearly every mobile device is capable of accessing the user's information, which can be a good thing in an emergency situation or if the user wishes to take advantage of location-specific services such as maps or information on nearby resources. But that information can also be misused and abused for a variety of purposes ranging from unwanted marketing to physical abuse, intimidation and stalking. All users are at risk, including children. The goal of this project is to provide widespread awareness of both the risks and potential benefits of location sharing (it can be very reassuring for families and close friends and can save lives in emergencies) so that users, including parents, can decide if and when it is appropriate to use, while greatly reducing potential harm.

We are creating a hub of resources easily understood by the general public, with additional resources for children and teens, to help people fully understand the potential harms (and benefits) of location information. Our resources will be accessible on the web and on mobile devices.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

We request a total of $1.5 million to be used over at least four years. The initial year will be used for staffing and costs to develop the website and materials, including professionally produced videos and animations, written materials, and presentations. Subsequent years will be used to operate the program, update materials, maintain the website and engage in ongoing education, including providing funds to educators and community organizations for local education programs. We envision this as a long-term ongoing project that will continue even after the initial funding has been spent.

11. Will the money be used to continue an existing project or create a new project?

This will be a new project but based on our 18 years of experience that includes developing similar-type resources on other online safety, privacy and security subjects.

12. What target population will your organization's project benefit?

Our project will mainly target families and educators with information that applies to children, teens and parents.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes. We will comply with any Court requests for information, including reports, every six months.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

We will track the number of people reached, including visits to LocationSafety.org and participants at events and in classrooms. We will also collect after-event reports from key program participants.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

As the proposal indicates, we will produce numerous publications along with video and audio resources. In addition, we participate in several conferences each year, including the U.N. Internet Governance Forum, the International Society of Technology in Education, the Family Online Safety Institute conference and our own events around Safer Internet Day.

Sincerely,

CONNECTSAFELY

/s/ Larry Magid
By: Larry Magid

Exhibit G

DATA& SOCIETY

Organization Information

1. *Name of organization*

Data & Society Research Institute (DBA Data & Society)

2. *Discuss the founding and history of the organization.*

Data & Society was founded in 2014 by researcher danah boyd to advance strategies for change in how data-centric technologies are understood and governed in society. Since its founding, Data & Society has grown from seven researchers based in New York City to over 45 staff members across the United States and abroad. During that time, we have grown as an organization, built a strong board and governance structure, and brought on an experienced and values-driven senior leadership team. As an institution, **we are equally committed to research and engagement**, ensuring the impact of our findings in policy and media spheres. Our theory of change rests on the belief that quantitative evidence, though valuable and necessary, is not sufficient for understanding the social implications of data-centric technologies.

From the beginning, our work has been animated by a set of core concerns:

1. Data-centric technologies have social, cultural, and political implications that are far-reaching, unevenly distributed, and poorly understood.
2. These technologies' negative impacts disproportionately harm marginalized populations.
3. The concentration of power in the tech industry has significant implications for both democratic practice and the governance of data-centric technologies.

Over the past three years, these concerns have become central to the work of many advocacy and research organizations in our field; to policymakers at various levels of government; and to the broader public. This shift is both a result of our work (and that of many partner organizations in our network) and an opportunity to push further.

Since we were founded, understanding and securing internet privacy has been central to Data & Society's mission. Some examples of our work in this area include:

Empirical Research

- *Privacy, Security, and Digital Inequality*, which provided the first in-depth analysis of the digital privacy and security experiences of low socioeconomic status populations in the United States.
- *The Wisdom of the Captured*, which analyzed how users may be negatively impacted by the internet-mediated data collection tools which enable automated technologies to make intelligent decisions.
- *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest*, which discussed privacy impact assessments and their value in assessing accountability of algorithmic systems.
- *Fairness in Precision Medicine*, which was the first report to deeply examine the potential for biased and discriminatory outcomes in the emerging field of "precision medicine."
- *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech*, which explored how consumer monitoring, audience-targeting, and automated technologies have been weaponized by political and anti-democratic actors to increase their influence.
- *Digital Identity in the Migration & Refugee Context*, which focused on how the migrant crisis was used as an excuse for pervasive biometric data tracking and collection—with no ability for these vulnerable populations to opt out.
- *The Constant Boss: Labor Under Digital Surveillance*, which looked at the changing social conditions of workplaces that pushed for worker data protection and privacy to enable workers to advocate for their rights.
- *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, which discussed how workers and patient employers submit to privacy-disrespecting geolocation and biometrics as part of the changing nature of care work.
- *At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers*, which connects the rise of home doorbell cameras to a broader erosion of privacy, which in turn has undermined the working conditions and labor rights of precarious, low-wage workers.
- *Essentially Unprotected: Health Data and Surveillance of Essential Workers During the COVID-19 Pandemic*, which followed how misunderstandings of privacy regulations (and their ability to keep up with new and changing technologies) produce harm for workers.

Policy Publications

- *Response to the FTC's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, which advocates for rulemaking to combat extractive surveillance practices that harm consumers and impede a just American technology ecosystem.
- *Democratizing AI: Principles for Meaningful Public Participation*, which offers evidence-based recommendations for integrating public participation into the AI development and implementation life cycle.
- *Algorithmic Accountability: A Primer*, which looks at the growth of harmful trends surrounding data privacy and collection, among other accountability issues.
- *Response to the White House OSTP's Request for Information on Automated Worker Surveillance and Management*, which highlighted the grave risks that automated surveillance and management tools present to workers.
- *Policy Brief* for the *Electronic Visit Verification* report listed above.
- *Policy Brief* for the *Assembling Accountability* report listed above.

3. *Describe the organization's current goals.*

We envision a future in which the values that inform the design and governance of data-centric technologies are visible and intentionally chosen with respect for human dignity and just outcomes. Governance of new technologies is often rooted in **assumptions** about how that technology *might* impact society. These assumptions often stem from extreme utopian or dystopian narratives, rather than an exploration of nuanced trade-offs. Instead, we believe it is critical to build governance around the documented **experiences** of people who live with the technology in question.

The overall goals of our work include:

- **Changing the terms of debate** by working with media and policymakers to advance human-centered and empirically grounded public discourse on technology and society issues;
- **Shifting power** by foregrounding the communities most impacted by data-centric technologies, we argue for approaches to technology design and governance that are grounded in equity and just outcomes; and
- **Shaping policy and practice** by translating research findings for policymakers with the goal of advancing rights-respecting, human-centered, and empirically grounded governance of data-centric technologies, including artificial intelligence and algorithmic systems.

Each of our projects also pursues individual goals that relate to its respective topic and intended audiences. For instance, past projects have sought to protect workers from commercial surveillance; create safe and secure online spaces for marginalized communities; and develop methodologies for assessing AI's impact on protected groups and communities to inform governance.

4. *Provide a brief description of the organization's current programs.*

Our core research programs work alongside our policy and engagement teams to ensure this research can be used to affect real-world change. Below we have provided a brief overview of each program:

Current Research Programs

- **AI on the Ground**. This program develops robust analyses of AI systems; effectively assesses their impact; and informs their future design, use, and governance. Our team recently launched the Algorithmic Impact Methods Lab (AIMLab), which brings together various partners to engage in an interdisciplinary approach to designing and piloting public interest methods for algorithmic impact assessments.
- **Labor Futures**. This program uses ethnographic research to better understand emergent disruptions in the labor force as a result of data-centric technological development, with a special focus on privacy and structural inequalities. Our team strives to center workers' concerns in research and action in order to envision just futures for labor in data-centric work environments.
- **Trustworthy Infrastructures**. This program works alongside marginalized groups to understand emerging approaches to building trust online, as well as the possibilities these practices set in motion. Rather than simply diagnosing threats and naming harms, our research aims to inform and advance effective sociotechnical solutions that reflect the knowledge and expectations of the communities that have been disproportionately harmed by the status quo.

Current Engagement Programs

- **Policy Engagement**. Our policy team works alongside our research teams to translate rigorous, empirical social science for multiple audiences and create actionable learning and policy recommendations for key targets and partners. They work closely with academic and policy research bodies; government institutions; civil and human rights advocacy groups; and community-based

organizations. Our policy work currently focuses on opportunities at the federal level, particularly with executive agencies that are directly engaged in developing and implementing new approaches to governing artificial intelligence and data security.

- **Public Technology Leadership Collaborative (PTLC).** This peer learning collective, led by Data & Society in partnership with ten academic research centers, creates knowledge communities between government decision-makers and scholars grappling with the use, study, and regulation of data-centric technologies and artificial intelligence. The PTLC offers a dynamic slate of programming—including workshops, seminars, and salons—that are intentionally informal, private, and focused on cultivating trust and sharing context. Past programming has focused on building responsible AI, fostering trust in technical systems, and incorporating public participation into the development of new technologies.
- **Media Engagement.** Our communications team builds and maintains relationships with national and global media outlets to ensure the circulation and visibility of our work. Their proactive media engagement strategy incorporates educational and convening opportunities for journalists, editors, and publishers to develop specialized knowledge in areas related to D&S research. The team also provides bespoke media training to our researchers and senior leadership to ensure they are prepared to engage with various audiences and media spaces.

5. *Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.*

We have never received a prior cy pres award.

6. *Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?*

We have a 100% 4-star rating on Charity Navigator. This is the highest rating possible, indicating that our organization "exceeds or meets best practices and industry standards across almost all areas."

DATA& SOCIETY

Grant Proposal

7. *Identify the organization's principal investigator or project director.*

The project director will be Executive Director Janet Haven. She will be supported by:
- Policy Director Brian Chen;
- PTLC Program Director Charley Johnson;
- AI on the Ground Program Director Jacob Metcalf; and
- Labor Futures Program Director Aiha Nguyen.

8. *Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.*

Concern for privacy has been a critical throughline of Data & Society's work from the beginning. The current lack of federal data privacy protections, such as those proposed in the American Data Privacy and Protection Act, leaves every American vulnerable to well-documented harms caused by widespread data collection, retention, and use practices. These practices often violate norms and assumptions that individuals hold about privacy, as well as their fundamental rights and core values. We have repeatedly seen the tech industry ignore the laws that are put into place to protect consumers from invasive data collection measures, simply because they believe the value of a big data set will outweigh legal ramifications[1]. When we do see companies take steps to put privacy controls in place, these measures are often coercive (i.e., terms of service agreements) and based on the idea that each and every person will take individual responsibility for the protection of their privacy (i.e., Facebook's privacy settings dashboard). Finally, our research has shown that online privacy violations harm vulnerable and low-income populations in a distinct and often overlooked manner. While these communities clearly understand the risks and harms associated with data collection, they often lack the legal protections, tools, and strategies needed to take action to sufficiently protect themselves[2].

The issues of online privacy and data protection have become even more pressing and complex with the launch of retail generative AI systems like ChatGPT. These systems are trained on data scraped from across the internet without permission, opening a broader debate about data privacy protections and the role of individual agency within them.

[1] Lane et al. (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014).
[2] Mary Madden, *Privacy, Security, and Digital Inequality* (Data & Society, 2017).

Indeed, the Biden Administration's Blueprint for an AI Bill of Rights includes data privacy as one of five core principles for building safe and rights-respecting AI systems, arguing that Americans "should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."[3]

And yet, current legal doctrines on privacy have ossified in the face of modern data extraction and online privacy abuse.[4] Many privacy harms are small but numerous, and they can also scale up rapidly. A breach of privacy may be an inconvenience to an individual; but when it happens to millions of people, the aggregate harm is meaningful to society. Because the law fails to recognize many privacy harms—other than those that are highly individualized and financial or physical in nature—the networked and highly distributed impacts of data technologies are often not remediable by courts.[5]

To address this, we would like to leverage Data & Society's research and engagement expertise to focus on the concept of "collective" or "networked" privacy. This will entail a framework shift—including research, narrative, and policy work—to account for communal privacy harms in data-centric and algorithmic environments. By looking at the forest, and not just the trees, we aim to demonstrate how the privacy harms wrought by AI and other algorithmic systems are experienced most acutely at the collective level—and therefore must be contested there.

We plan to address this topic by building on our already-robust work on privacy to bring a focus on collective privacy to all three of our research programs. Past research has shown that harmful data collection practices and subpar privacy regulations inflict greater harm on marginalized and disadvantaged communities[6]. By taking up collective privacy as a framework for both research and policy, the next phase of our work will focus on how unprotected internet and digital spaces abuse our privacy, how those impacts are measured, and how new approaches to governance can mitigate these harms altogether.

---

[3] "Blueprint for an AI Bill of Rights," The White House, 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/#:~:text=Data%20Privacy,-You%20should%20be&text=Systems%20should%20not%20employ%20user,be%20appropriately%20and%20meaningfully%20given.

[4] Citron and Solove, "Privacy Harms," *Boston University Law Review 102,* no. 793 (2022).

[5] Indeed, recent research from our AIGI team has demonstrated that algorithmic harms share this challenge with privacy harms, indicating the need for new regulatory interventions that can provide recourse to people and communities injured by algorithmic systems. See Metcalf et al., "Taking Algorithms to Courts: A Relational Approach to Algorithmic Accountability," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1450–1462 (Association for Computing Machinery, 2023), doi:10.1145/3593013.3594092.

[6] Alice E. Marwick, *The Private Is Political: Networked Privacy and Social Media,* (Yale University Press, 2023).

DATA& SOCIETY

Goals and Objectives

The long-term goal of this focus is to explore **collective privacy as both a social concept and a usable governance framework.** Our work will help determine the gaps in our shared understanding of **internet privacy for both individuals and groups, as well as potential remedies to address harms when they occur.** In doing so, we also plan to:

- Deepen relationships with the communities most impacted by internet privacy violations to ensure we take an inclusive and participatory approach our research and engagement;
- Pursue new research topics in our core areas of concern (i.e., health, labor, platform governance, trustworthy infrastructures, vulnerable communities, and AI governance) that bring together insights on collective privacy from multiple sectors; and
- Inform government leaders and policymakers about the risks, conditions, and pitfalls of regulations surrounding privacy online, with a particular emphasis on the importance of collective privacy.

Activities

This award would allow us to greatly increase our capacity for dedicated research and engagement on internet privacy, including new research into the undertheorized area of collective privacy as well as direct collaborations with policymakers and government leaders.

Engagement Activities

Our policy engagement team, led by Brian Chen, and our Public Technology Leadership Collaborative, led by Charley Johnson, already do extensive work with government leaders and policymakers, and these connections will be very beneficial to us as we seek to move our research on collective privacy into policy impact.

These teams already have experience working with government personnel on issues relating to internet privacy, including:

- Legislative work with federal and state lawmakers to promote statutory privacy protections, including sufficient notice, guaranteed transparency, and proper accountability when people's data is collected through technology;

- Leading responses to regulatory requests from the FTC in the context of consumer protection, in which we advocate for rulemaking that would protect people's privacy from extractive data practices and commercial surveillance;
- Working with the United States Agency for International Development (USAID) to explore the harms and impacts of surveillance technologies; and
- Leading responses to regulatory requests from the White House for worker rights amid the growing implementation of algorithmic management practices, including guidance to clarify how worker surveillance and location tracking violates their privacy and jeopardizes their physical and mental health.

These teams will lead activities that translate our findings on collective privacy for policy audiences. These will include creating policy briefs and producing events and salons for government personnel to engage directly with our research and related topics.

Research Activities

Our **Labor Futures** team plans to carry out a suite of research projects related to internet and data privacy and the impact this has on workers and their workplaces. In particular, their work will address how workplaces are skirting digital privacy laws with new worker surveillance tools. This will include providing recommendations to address these loopholes in both workplace practices and in federal policy. This project will build on their past work on worker surveillance, where they documented how the changing nature of technology in the workplace (particularly biometric surveillance) is being used and abused by employers, particularly in the wake of COVID-19. Other ongoing projects will also be expanded to consider workers' collective privacy concerns, including a forthcoming event series on generative AI in the workplace and new projects focused on the intersections of labor, race, and technology.

Our **Algorithmic Impact Methods Lab (AIMLab)**, a component of our AI on the Ground program, already views privacy as a central area of investigation when looking at algorithmic impact assessments (AIAs). There are many ways algorithms create digital privacy concerns, and we believe that AIAs can simultaneously provide governance of algorithmic decision-making and safeguard our rights to privacy[7]. At present, federal assessments hold no obligation to actually engage with vulnerable communities when measuring and ameliorating "impact." We founded AIMLab to address this issue by empowering those communities to set the terms of these

[7] Kaminski and Malgieri, "Algorithmic impact assessments under the GDPR: producing multi-layered explanations," *International Data Privacy Law* 11, no. 2 (2021),125–144.

assessments. Impacted communities are often put in a dilemma that more privileged individuals do not face: trading their privacy and autonomy to algorithmic systems in order to access the most basic needs. To build AIAs that effectively serve these populations where current frameworks fail, we will use multiple case studies and different types of systems and applications to develop analytics that will help inform new methodologies for impact assessments. Aligning with the work of privacy scholar Deirdre K. Mulligan, we believe that to "make productive use of privacy's essential contestability, we [must] argue for a new approach to privacy research and practical design, focused on the development of conceptual analytics that facilitate dissecting privacy's multiple uses across multiple contexts"[8]. AIMLab's goal is to create AIA methodologies that *measure* what matters most to impacted communities, in order to facilitate their capability to *contest* how those systems deploy and operate.

Our newest research program, **Trustworthy Infrastructures**, works alongside communities most impacted by trust, safety, and privacy harms online. The fundamental goal of this research is to move towards day-to-day interactions with technology that create and sustain trust. To do so, we not only need to limit a flood of harmful attacks on privacy online, but must also look to bolster and expand existing practices and social infrastructures by putting forth new sociotechnical solutions that increase trust and protect our internet privacy. We have two upcoming projects that relate to communities who are deeply impacted by lack of privacy protections online: indigenous and black communities. The first of these projects, led by Indigenous Mestiza scholar Tiara Roxanne, looks at developing protocols of trust and safety online with Indigenous communities based in Central and South America. The second, led by Joan Mukogosi, focuses on how privacy and trust online have impacted how Black communities find and receive health care advice, particularly in the wake of COVID-19. Both these projects work directly with the communities impacted by privacy harms, and the empirical research we produce will shape the development of trustworthy digital infrastructures as well as the policies and regulations that govern them.

Publications and Events

During this period, we will produce:

- **Standalone research publications** of our findings related to the protection of internet privacy;

[8] Mulligan et al., "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy," *Philosophical Transactions of the Royal Society A* 374, (2016).

- **Policy briefs** based on our research that are designed to intervene on a specific privacy technology or regulation;
- **Public events** that bring Data & Society staff members together with invited speakers to talk about digital and collective privacy concerns;
- **Salons for government leaders** that give them a space to learn about and better understand the issues surrounding collective internet privacy; and **Relationships with media outlets and journalists** to ensure the broader public understand the implications of our research and policy work.

Timeline

We see this work taking shape over five years, a timeframe which includes significant research and engagement periods:

Year	Project Quarter	Phase/Project
1	Q1	Hiring and Capacity Building
1	Q2	Research and Community Engagement
1	Q3	Research and Policy Engagement
1	Q4	Evaluation, Impact Stories, and Reports Research and Policy Engagement
2	Q5	Publication Release and Public Event
2	Q6	Policy Brief Release
2	Q7	Research and Community Engagement
2	Q8	Evaluation, Impact Stories, and Reports Research and Policy Engagement
3	Q9	Research and Policy Engagement
3	Q10	Publication Release and Public Event
3	Q11	Policy Brief Release

3	Q12	Evaluation, Impact Stories, and Reports Research and Policy Engagement
4	Q13	Research and Policy Engagement
4	Q14	Publication Release and Public Event
4	Q15	Policy Brief Release
4	Q16	Evaluation, Impact Stories, and Reports Research and Policy Engagement
5	Q17	Research and Policy Engagement
5	Q18	Publication Release and Public Event
5	Q19	Policy Brief Release
5	Q20	Evaluation, Impact Stories, and Reports

Ongoing activities throughout this timeline include: quarterly reporting; salons with government leaders; media placements; op-eds; travel for conferences and meetings; and responses to government requests for information as needed.

9. *Explain why the organization is approaching the issue and/or opportunity in this way.*

We consider the protection of privacy to be a social and technical concern: it's not just about sharing data, it's also about people's experiences of being watched and trusting the digital technologies they use[9]. As a result, our goals and objectives relate not only to how these companies are regulated, but also to how trust is built and sustained by the communities that use these technologies. Focusing our approach on collective trust is therefore key to building a body of research and policy action that could lead to profound change.

We have a history of using a sociotechnical perspective to inform policy debates, change, and action. Accordingly, we believe this approach is what the current privacy debate

[9] Metcalf et al., "Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery, 2021), 735–746.

needs. Rather than simply producing research and releasing it into the world, we build dedicated engagement into every research project. We engage policy, practitioners, and media communities with the goal of translation and influence, as well as engaging our peers in academia, rights-based organizations, and aligned communities to learn, collaborate, and strengthen our field to increase shared power.

Some examples of this successful engagement include:

- Our *Electronic Visit Verification* report about the abuses of privacy in care work was pivotal in our submission to the Office of Science and Technology Policy's Public and Private Sector Uses of Biometric Technologies RFI; was cited in Supreme Court of the State of New York about their digital ID practices; and was listed as a primary source by the European Parliament Research Service in their publication "AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework".
- We saw our explainer on algorithmic management in the workplace used as a foundational citation by Jennifer Abruzzo, the general counsel of the National Labor Relations Board, in her memo Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights. In this memo, Abruzzo announced that she will urge the NLRB to adopt a new framework for protecting workers from intrusive and abusive electronic monitoring and automated management practices.
- We have helped change the terms of debate around workers and automated systems. This includes the latest debates surrounding the Writer's Guild of America and the use of AI systems.
- Our AI on the Ground team has had numerous engagements with local, state and federal policy makers to inform their decisions about algorithmic impact assessments.
- Our *Digital Doorstep* report helped build new partnerships with on-the-ground advocacy groups to see real change, cited by multiple other research institutes including the Washington Center for Economic Growth, and was featured on multiple podcast interviews including *BBC Digital Planet* and *Marketplace Tech*.

DATA& SOCIETY

10. *Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.*

Year 1

Total Personnel costs for the first year are $889,055, which will either fully or partially cover the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), and Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000, which will cover Project Supplies & Materials (i.e. include licenses, software, publication costs), Events (i.e., venue rental and honoraria) and Travel (related to conferences, events and fieldwork).

Total costs for the first year: $1,004,055

Year 2

Total Personnel costs for the second year are $955,085, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), and Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the second year: $1,070,085

Year 3

Total Personnel costs for the third year are $983,738 which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program

Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab) Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the third year $1,098,738

Year 4

Total Personnel costs for the fourth year are $1,013,250, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the fourth year $1,128,250

Year 5

Total Personnel costs for the fifth year are $586,674, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $112,198 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the fifth and final year $698,872

Total Personnel costs are $4,427,802. Total Direct Project costs are $572,198 for a total of $5,000,000 across 5 years.

11. *Will the money be used to continue an existing project or create a new project?*

This money will be used to sustain and increase the capacity of our current programs, as well as to fund new research projects within those programs. It will not be used to start a new, dedicated program.

12. *What target population will your organization's project benefit?*

These activities will respond to broad and pressing internet privacy concerns that impact the general public, while also maintaining a particular focus on collective privacy as it relates to low-income and precarious workers and other vulnerable communities. These projects will benefit these groups by directly including them in the research process, designing governance approaches grounded in participatory methods[10], and engaging government leaders on our research findings in ways that foreground these groups.

Evaluation

13. *Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?*

We agree to provide a report to the Court and the parties every six months; this report will detail how the funds have been (and will be used to support this work). We routinely provide narrative and financial reports of our programs to other funders, so our team certainly has the experience needed to ensure this is carried out every six months.

14. *Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.*

[10] Michele Gilman, *Democratizing AI: Principles for Meaningful Participation* (Data & Society, 2023).

DATA& SOCIETY

We build a series of impact measures and evaluation periods into the timeline of every project we take on. This work is led by Ania Calderon, our managing director, alongside our strategy and engagement team, who bring significant experience in setting impact measures, tracking our impact, and evaluating the results of our work.

Our impact and evaluation model for projects has six core components. They are:

1. **Learning questions**. Each year, our projects and programs develop two timely learning questions that help us assess the kind of impact we are making. For this project, we will develop these learning questions related to internet privacy in consultation with the associated research programs. They will focus on asking questions of impact that bring us closer to our long-term goal of the protection of internet privacy.
2. **Project retrospectives**. We regularly hold project retrospectives as part of our research pipeline, often in conjunction with the launch of a report or major publication. These retrospectives are used to reflect on each project's intended purpose: how it promotes the protection of internet privacy; what successes we saw in the process; and the biggest factors that contributed to change and impact.
3. **Quarterly program progress**. Each quarter, we take stock of—and report on—program progress and share this information with the organization as a whole. These updates reflect on the outputs we've been successful in producing, review our key learning questions and assumptions, and explain how we will move this work forward in the future.
4. **Learning Labs**. Our strategy and engagement team hosts biannual org-wide learning labs. These sessions bring us together as a group to share insights, connect learnings across programs and project retrospectives, review the impact we are having, and discuss how we might use these insights to inform future decisions. For this project, Learning Labs will give us an opportunity to review our long- and medium-term goals related to internet privacy alongside the work of the entire organization.
5. **Impact stories and annual reports**. Where appropriate, we publish our outcomes and progress as impact stories. These stories are narrative tools for communicating the processes and outcomes of our work to various stakeholders. They connect the dots across our various projects and organizational initiatives, showcasing common themes and learnings that elucidate how our work is reflecting the values and strategy of the organization as a whole. Since our work on internet privacy will be done across all of our research programs, impact stories will be an essential tool for bringing each component together to create a comprehensive portrait of our work and its impact.**Board Oversight.** Data &

DATA& SOCIETY

Society's board of directors maintains oversight over all of our work through regular reporting on organizational goals and strategy, as well as scrutinous financial oversight. They also provide important support and guidance that shapes how we evaluate and track the overall impact and success of our projects.

15. *Does your organization intend to use the results of the project in any publications, conference papers, and presentations?*

We intend to produce outward-facing reports, articles, papers, and presentations as part of this project. We have a long history of producing and publishing reports in-house through our website, as well as having papers and articles accepted into journals and media outlets. Our researchers are also regularly invited to present at conferences, events, and institutions around the world. These include the Mozilla Festival; AI and Tech Summit; ACM Conference on Fairness, Accountability, and Transparency (FAccT); Association of Internet Researchers Conference; and Trust and Safety Research Conference.

Exhibit H

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

Exhibit I

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.

Exhibit J

CLIP Center on Law and Information Policy
AT FORDHAM LAW SCHOOL

October 5, 2023

Re: *In re Google Location History Litigation* Proposed Cy Pres Award

Dear Ms. Wolfson and Mr. Sobol,

I write in response to your letter of September 15, 2023, inviting the Center on Law and Information Policy (CLIP) at Fordham University School of Law to submit a proposal to receive a *cy pres* award from the settlement of *In re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal.). On behalf of CLIP, I submit a proposal under this cover.

Our proposal contemplates four discrete projects, summarized here and described in detail in the accompanying proposal packet:

1. ***Privacy Educators Program:*** A revision and expansion of an existing CLIP-developed curriculum designed to educate elementary and middle school students about online privacy. *Funding Range: $228,200.00 - $911,913.58*.

2. ***Educating Educators About Privacy-by-Design:*** A new program aimed at training K-12 educators and administrators about privacy concepts as they design or purchase education and monitoring tools that may access or collect data about students. *Funding Range: $112,000.00 - $680,513.58*.

3. ***Making Data Breach Notifications Work: A Large Language Model Approach to Safeguarding Consumer Privacy:*** A new project that will leverage advancements in machine learning and natural language processing to translate complex data breach notifications into simple language, and evaluate how effective simplified notifications are in encouraging people to take remedial action in the event of a breach. *Funding Range: $20,500.00 - $150,500.00*.

4. ***Global South Privacy Researcher Fellowship:*** A new program that will allow CLIP to host internet privacy scholars from regions in the Global South for academic-year-long research fellowships. *Funding Range: $56,000.00 - $280,000.00*.

We would welcome and appreciate support for any or all of these proposed projects.

The funding ranges provided reflect our best estimates of the costs associated with achieving the goals, objectives, and activities of each project, as described in detail in the accompanying proposal packet. If the Court and the parties should wish to offer funding beyond the indicated ranges, we would welcome the additional support and would apply it in furtherance of stated project goals and objectives.

Additionally, CLIP, like the other research centers at Fordham University School of Law, relies on outside funding in the form of grants and individual donations to support its general administration and operation. Should the parties and the Court wish to provide additional funding to support CLIP's administration and operation in any amount deemed appropriate, we would welcome that as well.

We would be happy to discuss our proposals in more detail, or to answer any questions that you may have. Please do not hesitate to contact us.

We appreciate your recognizing CLIP's work toward promoting internet privacy, and we thank you for inviting us to submit a proposal.

Sincerely,

Tom Norton
Executive Director, Fordham Center on Law and Information Policy (CLIP)
Fordham University School of Law
(212) 930-8878
tnorton1@fordham.edu
clip@fordham.edu

Organization Information

1. Name of organization.

Fordham University School of Law Center on Law and Information Policy (CLIP).

2. Discuss the founding and history of the organization.

The Center on Law and Information Policy (CLIP) is an academic research center at Fordham University School of Law. CLIP was founded in 2005 to make significant contributions to the development of law and policy for the information economy, as well as to teach the next generation of information law leaders.[1] Toward these ends, CLIP brings together scholars, the bar, the business community, technology experts, the policy community, students, and the public to address and assess policies and solutions for cutting-edge issues that affect the evolution of the information economy.

CLIP supports and conducts research, organizes public events, and facilitates high-level discourse on topics such as data privacy and security, internet governance, intermediary liability, online speech, and others. CLIP's work is disseminated widely, helping to influence the guiding principles of our information-driven society and find solutions to legal issues posed by information technologies.

Over the past ten years, CLIP has focused substantially on internet privacy. CLIP's work on student data privacy has produced groundbreaking research, including studies about public schools' use of cloud computing services, as well as the marketplace for student data among data brokers. CLIP has also received two grants from the National Science Foundation (NSF) to study online privacy notices in interdisciplinary collaboration with computer science colleagues. And last year, CLIP was awarded a third grant from the NSF to investigate methods to design software systems that are accountable to privacy and data protection law and regulation.

CLIP's work has had significant and meaningful impact on law and policy. Its work on student data privacy sparked a Congressional hearing about "How Data Mining Threatens Student Privacy"—a first-of-its-kind meeting between members of the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and the U.S. House of Representatives Committee on Education and the Workforce, Subcommittee on the Early Childhood, Elementary, and Secondary Education.[2] The research also influenced the passage of Vermont's data broker registration law.[3] Additionally, multiple examples of CLIP's work on online

---

[1] CLIP was founded by the late Joel Reidenberg, the Stanley D. and Nikki Waxberg Chair and Professor of Law, who was a pioneer in the field of information law. Professor Reidenberg's groundbreaking 1998 article, *Lex Informatica: The Formulation of Information Policy Rules Through Technology* (76 TEX. L. REV. 553 (1998)), laid the foundation for conceptualizing information systems as governance schemes and showed that the design of networked systems creates rules that compete with—and sometimes supplant—traditional forms of regulation.

[2] *See How Data Mining Threatens Student Privacy: Joint Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives and the Subcommittee on Early Childhood, Elementary, and Secondary Education of the Committee on Education and the Workforce,* 113th Cong. (2013).

[3] *See* Data Brokers, OFF. OF THE VT. ATT'Y GEN. (Dec. 5, 2017), https://ago.vermont.gov/blog/2017/12/05/data-brokers/ (listing N. Cameron Russell, Joel R. Reidenberg, Elizabeth Martin & Thomas B. Norton, Transparency and the Marketplace for Student Data, VA. J.L. & TECH. 107 (2019) among the materials that were publicly submitted to

privacy notices were cited by the California Office of the Attorney General as Documents and Other Information Relied Upon in drafting regulations to the state's landmark California Consumer Privacy Act.[4] Beyond this, CLIP regularly publishes in law and technology forums, and presents at leading conferences and events. CLIP is guided by a Board of Advisors that has counted among its members lawyers practicing information law, industry professionals, and members of the federal judiciary.

3. Describe the organization's current goals.

CLIP's current goals include:

- ***Conducting cutting-edge research in information law topics.*** CLIP aims to continue its track record of producing high-quality, influential scholarly work on information law topics including data privacy and security, internet governance, intermediary liability, online speech, and more. Through rigorous analysis and interdisciplinary collaboration, CLIP endeavors to produce research that not only contributes to academic discourse, but also informs policy decisions and shapes the future of information law.

- ***Facilitating public discourse on information law topics.*** CLIP is committed to fostering a vibrant public discourse on critical issues that impact the information society as a whole. CLIP aims to continue to educate the public on issues in information law by organizing and hosting public events, including lectures, conferences, symposia, and roundtable discussions. These events serve as platforms for experts, policymakers, and the public to exchange ideas, share insights, and explore the implications of information law in our increasingly digital world. By promoting open dialogue and knowledge sharing, CLIP aims to empower individuals to make informed decisions and advocate for policies that uphold the values of privacy, security, and free expression in the digital age.

- ***Training law students to form the next generation of information law leaders.*** CLIP is deeply committed to nurturing the next generation of legal professionals who will shape the future of information law. CLIP believes that hands-on experience and mentorship are essential for students aspiring to become leaders in this field. To this end, CLIP aims to provide law students with valuable opportunities for engagement through fellowships, research projects, and collaborative initiatives that equip them with the practical skills and real-world experiences necessary to excel as information law leaders.

---

the Vermont General Assembly in connection with Vermont's data broker regulation legislation, Act of May 22, 2018, 2018 Vt. Acts and Resolves 584).

[4] *See* CCPA Regulation – Documents and Other Information Relied upon, STATE OF CALIF. OFF. OF THE ATTY. GEN., https://oag.ca.gov/privacy/ccpa/docs-info (listing Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Norton, Thomas B., The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model, 27 Fordham Intell. Prop. Media & Ent. L.J. 181 (2016); and Reidenberg et al., Ambiguity in Privacy Policies and the Impact of Regulation (March 22, 2016) Journal of Legal Studies, Forthcoming; Fordham Law Legal Studies Research Paper No. 2715164, among the materials that the state's Department of Justice relied upon during its rulemaking process).

4. Provide a brief description of the organization's current programs.

CLIP's current programs include research initiatives, public events, and student engagement opportunities:

Research

CLIP has two ongoing, multi-year interdisciplinary privacy research projects funded by the National Science Foundation:

- *Legal Accountability as Software Quality:* A collaboration with computer science colleagues at Carnegie Mellon University to examine how people trained in law and software engineering can work together in design teams to collect and represent legal and technical information for the purpose of building accountability into software from the outset of the design process.

- *Answering People's Privacy Questions:* A collaboration with computer science colleagues at Carnegie Mellon University and Penn State University to develop query answering tools for privacy, to relieve consumers' burden to read and understand privacy disclosures by offering them technological tools to answer their privacy questions based on automated processing of privacy policy text.

Public Events

- *Law and Information Policy Roundtable Series:* Each month, CLIP hosts a roundtable discussion about an emerging information law topic. The series convenes academics, lawyers, industry experts, technologists, and students to discuss current developments in the information law field in an off-the-record, casual setting.

- *Annual Reidenberg Lecture Series:* CLIP hosts an annual lecture program to honor the life and contributions of the late Professor Joel Reidenberg, CLIP's founder.

- *Conferences and Symposia:* CLIP hosts and co-sponsors conferences and symposia on information law topics. CLIP faculty and staff also appear as speakers, panelists, and moderators for outside programs.

- *Lectures, Presentations, Book Talks, and Workshops:* CLIP hosts experts in the field of information law, including academics, technologists, industry professionals, and others, to present their recent work.

Student Engagement Opportunities

- *Decennial Fellows Program:* A program for a select group of first-year law students with a demonstrated interest in information law for community-building, networking, and extracurricular learning about topics in information law.

- *Student and Tech-Law Faculty Conversation Series:* A bi-weekly conversation series to bring together Fordham law students and technology-focused faculty for informal discussions about emerging developments in information law.

- *Privacy Educators Program:* A first-of-its-kind privacy education program in which Fordham law students visit New York City public schools to teach a CLIP-developed curriculum focused on online privacy and safety to elementary and middle school students.

- *CLIP-ings Weekly E-Newsletter:* A weekly roundup of information law news produced by student editorial fellows.

- *Tech Law Career Series:* A career mentoring series for which CLIP invites information law practitioners from diverse sectors (*e.g.*, big law, non-governmental organizations, small and boutique firms, public interest organizations, etc.) to meet informally with students to discuss their work and dispense career advice.

- *International Association of Privacy Professionals (IAPP) Westin Scholar Award:* Each year, CLIP nominates a student committed to working in privacy to receive the award, which comes with a cash prize, IAPP membership, and free access to trainings and programs.

5. **Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.**

Yes. In 2012, CLIP received $75,000 in *cy pres* funds from settlement of the NebuAd class action lawsuit (*Valentine v. NebuAd, Inc.*, No. 3:08-cv-05113 (TEH) (N.D.Cal.)). The award funded CLIP to develop a first-of-its-kind privacy education program geared toward elementary and middle school students, the Privacy Educators Program. The award supported the development of a set of turnkey curriculum materials and the piloting of the program in a New York City middle school.

In 2015, CLIP received $120,000 from the Digital Trust Foundation, the non-profit privacy foundation charged with controlling the disposition of *cy pres* settlement funds in the Facebook Beacon Privacy Class Action Lawsuit (*Lane v. Facebook*, Case No. 5:08-cv-03845-RS (N.D.Cal.)). The grant funded a full-time privacy fellow at CLIP and supported the continuation of the Privacy Educators Program.

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?**

As CLIP is part of Fordham University School of Law, it has not been separately reviewed. However, Fordham University has been reviewed by Charity Navigator and received a 100% Four-Star rating.

Proposal #1: Privacy Educators Program

7. Identify the organization's principal investigator or project director.

Tom Norton is the Executive Director of the Center on Law and Information Policy. His research focuses on privacy and data protection law and policy as well legal accountability in software systems. His work appears in both law and technology publications, and he has received support from the National Science Foundation. At Fordham, Tom teaches courses in Information Privacy Law. Tom earned a JD from Fordham University School of Law and served as CLIP's Privacy Fellow from 2014 to 2016. Prior to returning to CLIP as Executive Director, Tom was a litigation attorney at the law firm Arent Fox LLP in New York City. He is admitted to practice in the State of New York and the Commonwealth of Massachusetts.

Ron Lazebnik is the Academic Director of the Center on Law and Information Policy, the Director of Fordham's J.D. Externship Program, and the Director of the school's Samuelson-Glushko Intellectual Property and Information Law Clinic. His academic and scholarly interests include IP law, information law, and intersection of law and technology. Before joining Fordham, he was in private practice, where he helped represent clients in various matters involving patents, copyrights, trademarks, trade secrets, and general commercial litigation. He has also assisted in the defense of corporations and government agencies being investigated by the SEC, the Public Company Accounting Oversight Board, and the U.S. Department of Justice. Professor Lazebnik is a graduate of Harvard Law School, and holds a Master's degree in electrical engineering from Case Western Reserve University.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

CLIP will update and expand its Privacy Educators Program ("PEP"), a first-of-its-kind curriculum designed to teach elementary and middle school students about online privacy and safety.

PEP aims to enhance elementary and middle school students' digital privacy literacy by teaching them about the technology they use, how it works, and how it relates to their own privacy and identity. Through the program, students learn what privacy is, why it is of value to them, and how they can safeguard it while engaging in digital, social culture. The program also teaches students practical tips for steps they can take to protect their privacy online, such as managing their social network accounts, passwords, and mobile privacy settings. The program is designed to educate children about how to use internet-connected technologies in privacy-mindful ways.

CLIP first developed the Privacy Educators Program curriculum in 2013. CLIP makes the curriculum available as a set of free, open-source documents to any educators who want to use the instructional materials to address the many privacy issues children and teens face as their use of technology skyrockets.

In its current form, the curriculum features a set of five one-hour-long sessions covering the following topics:

1. *Introduction to Privacy:* This session introduces the concept of privacy and discusses its importance. Students investigate what privacy means to them and how it is relevant in their daily lives. It creates a baseline for subsequent sessions on more specific privacy and technology issues.

2. *Passwords and Behavioral Ads:* This session explains how passwords can be used to protect privacy. It provides students with practical tips for creating secure passwords and assesses the risks involved in sharing passwords. The lesson also addresses behavioral, targeted advertising.

3. *Dealing with Social Media:* This session gives students practical tips for navigating tricky social situations that can arise because of social media use. Discussions in this section focus on privacy tradeoffs, managing privacy settings, maintaining a healthy balance between online and offline relationships, maintaining a healthy relationship with social media, and ways to disengage from social media.

4. *Understanding Mobile, Wi-Fi, and Facial Recognition:* This session focuses on how the technologies we use every day may be compromising our privacy in unexpected ways. Students learn the basics of how certain information technologies work and discuss the costs and benefits of data collection and use.

5. *Managing a Digital Reputation:* This session challenges students to think about how to actively manage a digital reputation. It introduces the concept of audiences and highlights the multiple audiences involved in digital communications. This session emphasizes the permanent, searchable nature of online communications and how this impacts reputation management.

Each spring, CLIP assembles a team of law student volunteers to teach the PEP curriculum at two diverse public schools in Manhattan. As described in more detail below, CLIP proposes to update the program so that it better reflects current and emerging privacy issues that students in the target demographic face, as well to expand the program's adoption in New York City, the New York metropolitan area, and beyond.

Issue Addressed

Young people using connected devices often misunderstand how their virtual actions affect their privacy, safety, and long-term reputation. Young people are uniquely vulnerable to hackers, cyberbullies, fraud, and even their own conduct online. Indeed, recent studies have shown that increased online activity can negatively affect children's health and wellbeing.[5] In response, PEP teaches elementary and middle school students how to protect their privacy online, navigate the complex world of social media, manage cyberbullying incidents, and safeguard their online reputations. Through a five-week series of lessons, discussions, and exercises, PEP teaches young people both why privacy and good digital citizenship are important and how to weigh the consequences of their virtual actions before they interact online. PEP primarily serves low-income and minority students in public school systems, as these populations are often among the most vulnerable.

[5] *See, e.g.*, Matt Burgess, *A Huge Scam Targeting Kids with* Roblox *and* Fortnite *'Offers' Has Been Hiding in Plain Sight*, Wired, Aug. 14, 2023, 9:19 a.m., https://www.wired.com/story/poison-pdf-scam-fortnite-roblox/?redirectURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fpoison-pdf-scam-fortnite-roblox%2F.

Goals and Objectives

Goals	Objectives
Update the PEP curriculum materials to better reflect current and future privacy issues children and teens face online, including by aligning the program curriculum with New York State STEM standards.	Engage an education consultant to conduct a review of and undertake large-scale revision of existing curriculum materials.
Develop benchmarking and assessment tools to measure and quantify the program's effectiveness towards developing students' privacy knowledge and affecting their privacy practices.	Engage an education consultant with expertise in developing benchmarking and assessment tools.
Create and host interactive digital content based on the program curriculum.	Engage an expert in developing interactive, digital education content. Identify a hosting service to maintain that content.
Expand the program's adoption by schools in New York City, the New York metropolitan area, and beyond.	Host, produce, and present program demonstrations for school personnel, including teachers, administrators, and members of boards of education. Host a yearly educators' forum at Fordham University School of Law.
Create a full-time position within CLIP for an individual to administer the program over a multi-year span toward the achievement of these goals and objectives.	Hire a full-time Privacy Fellow to serve as the program's administrator and figurehead.

Timeline of Activities

Year 1:

- Months 1-3: Hire and train a full-time Privacy Fellow to oversee and administer the program.
- Months 3-9: Hire an education consultant to review and update existing curriculum materials and begin development of benchmarking and assessment tools.
- Months 9-12: Conduct pilot tests of revised curriculum and benchmarking and assessment tools.
- Year 1 Spring: Run the program at CLIP's existing partner schools in New York City.

Year 2:

- Months 1-3: Revise updated curriculum and benchmarking and assessment tools.
- Months 3-6: Conduct second round of pilot testing on updated curriculum and benchmarking and assessment tools.
- Months 6-9: Hire digital content creator to create interactive digital materials based on the program curriculum.
- Months 9-12: Begin promotional and rollout activity for the newly updated curriculum, including initial presentations to education professionals including teachers, administrators, and boards of education.
- Year 2 Spring: Run the program at CLIP's existing partner schools in New York City, as well as in new partner schools.

Year 3:

- Continue promotional and rollout activity, including presentations to education professionals including teachers, administrators, and boards of education.
- Update the curriculum and digital content as necessary.
- Host an educators' forum.

- Run the program at CLIP's existing partner schools in New York City, as well as in new partner schools.

Year 4:

- Continue promotional and rollout activity, including presentations to education professionals including teachers, administrators, and boards of education.
- Update the curriculum and digital content as necessary.
- Host an educators' forum.
- Run the program at CLIP's existing partner schools in New York City, as well as in new partner schools.

Year 5:

- Continue promotional and rollout activity, including presentations to education professionals including teachers, administrators, and boards of education.
- Update the curriculum and digital content as necessary.
- Host an educators' forum.
- Run the program at CLIP's existing partner schools in New York City, as well as in new partner schools.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

PEP, through adult-guided peer discussions among elementary and middle school students, teaches young people about the technology they use, how it works, and how it relates to their own privacy and identity. The project encourages young people to explore their sense of privacy, why it might be of value them, and how they can safeguard it while engaging online. The program provides students with practical skills and tips on things they can do to safeguard their privacy, including managing their social network accounts, passwords, and mobile privacy settings.

We believe this is the best approach for four reasons:

- Young people in the target age group are just beginning to interact on social media and are at a formative stage in their social development. This is a critical window for learning awareness of digital privacy as online engagement increases.
- The program employs an interactive, discussion-based method to stimulate peer interaction rather than lecture. This is a more effective way to reach students in the target age group and convey an appreciation of privacy.
- The program offers practical skills training so that youth will be equipped to deal with changing technologies.
- The goal of creating partnerships in the local community and beyond will lead to the program having lasting impact.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

The major components of this project include developing new curriculum materials for the PEP with the assistance of consulting experts, promoting the program toward expanded adoption via workshops, presentations, and forums, and hiring a full-time Privacy Fellow to manage the program.

Funding Range

Scope	Cost
5-Year Full-Scope	$911,913.58
4-Year Partial-Scope	$761,162.70
3-Year Partial-Scope	$613,690.00
2-Year Partial-Scope	$459,400.00
1-Year Partial-Scope	$228,200.00

Budget Detail

	Year 1	Year 2	Year 3	Year 4	Year 5	*Totals*
Privacy Fellow[6]	$100,000.00	$103,000.00	$106,090.00	$109,272.70	$112,550.88	*$530,913.58*
Education Consultant	$50,000.00	$50,000.00	$10,000.00	$5,000.00	$5,000.00	*$120,000.00*
Digital Content Creator	$50,000.00	$50,000.00	$10,000.00	$5,000.00	$5,000.00	*$120,000.00*
Research Assistants[7]	$12,000.00	$12,000.00	$12,000.00	$12,000.00	$12,000.00	*$60,000.00*
Web Hosting Services	$1,200.00	$1,200.00	$1,200.00	$1,200.00	$1,200.00	*$6,000.00*
Outreach/Expansion Activities	$5,000.00	$5,000.00	$5,000.00	$5,000.00	$5,000.00	*$25,000.00*
Educators Forum at Fordham	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	*$50,000.00*
Yearly Totals:	*$228,200.00*	*$231,200.00*	*$154,290.00*	*$147,472.70*	*$150,750.88*	***$911,913.58***

11. Will the money be used to continue an existing project or create a new project?

The money will be used to continue the existing Privacy Educators Program. Specifically, the funds will be directed toward achieving the goals, objectives, and activities outlined in response to Question 8, above.

[6] Reflects yearly salary plus mandatory benefits, accounting for an estimated 3% yearly cost-of-living increase.

[7] Reflects costs for two Research Assistants per semester, each working 10 hours per week for 10 weeks at a rate of $20/hr., for each of the fall, spring, and summer semesters.

12. What target population will your organization's project benefit?

The project will benefit elementary and middle school students in New York City, the New York metropolitan area, and beyond, many of whom come from underrepresented or vulnerable backgrounds. Additionally, the project will benefit law students who participate in the program by giving them the opportunity to develop key lawyering skills, including skills in public speaking and presentation, as well as in tailoring content to a target audience.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes. CLIP agrees to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

CLIP will evaluate the program's success based upon several factors:

- **Students better understand privacy and the impact of their online behavior.** Students receiving privacy education through PEP develop and practice more informed, privacy-conscious habits when using online services. Newly created assessment tools meaningfully measure these objectives.

- **CLIP develops and makes available to the public updated curriculum materials.** Updated curriculum materials, including new interactive digital content, better reflect current and future privacy issues children and teens face online. To encourage adoption of the program, these materials align with New York State STEM standards.

- **CLIP develops meaningful tools to track and evaluate student learning.** The newly created tools assess PEP's effect on student knowledge and conduct as related to the PEP's topics.

- **New partner institutions teach the PEP curriculum.** Partner institutions represent New York City, the New York metropolitan area, and beyond. CLIP collaborates with these partner institutions to identify schools willing to adopt the PEP curriculum. CLIP creates protocols for tracking institutional participation and student impact and to provide support as needed.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

CLIP may use select results from the project in publications, conference papers, and presentations.

Proposal #2: Educating Educators About Privacy-by-Design

7. Identify the organization's principal investigator or project director.

Tom Norton is the Executive Director of the Center on Law and Information Policy. His research focuses on privacy and data protection law and policy as well legal accountability in software systems. His work appears in both law and technology publications, and he has received support from the National Science Foundation. At Fordham, Tom teaches courses in Information Privacy Law. Tom earned a JD from Fordham University School of Law and served as CLIP's Privacy Fellow from 2014 to 2016. Prior to returning to CLIP as Executive Director, Tom was a litigation attorney at the law firm Arent Fox LLP in New York City. He is admitted to practice in the State of New York and the Commonwealth of Massachusetts.

Ron Lazebnik is the Academic Director of the Center on Law and Information Policy, the Director of Fordham's J.D. Externship Program, and the Director of the school's Samuelson-Glushko Intellectual Property and Information Law Clinic. His academic and scholarly interests include IP law, information law, and intersection of law and technology. Before joining Fordham, he was in private practice, where he helped represent clients in various matters involving patents, copyrights, trademarks, trade secrets, and general commercial litigation. He has also assisted in the defense of corporations and government agencies being investigated by the SEC, the Public Company Accounting Oversight Board, and the U.S. Department of Justice. Professor Lazebnik is a graduate of Harvard Law School, and holds a Master's degree in electrical engineering from Case Western Reserve University.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

CLIP will start a new program aimed at making sure that the educators and administrators responsible for the education of students in grades K-12 are more aware of privacy-by-design concepts as they design or purchase education and monitoring tools that may access or collect data about their students.

Issue Addressed

While there are several laws that protect student data, such as the Family Educational Right and Privacy Act and the Children's Online Privacy Protection Act, the existence of these laws makes educators and their administrators believe that as long as they are complying with the laws, they are fulfilling their students' privacy requirements. The problem with this frame of mind is that it allows for the compilation of large data sets regarding students. Should cybersecurity measures fail to protect this data, or should third party vendors facilitating the collection or use of the data not be as complaint as school systems are led to believe,[8] the information regarding these children becomes at risk. Educators and their administrators must therefore be educated about the principles of privacy by design to better understand when it is appropriate to collect student information and to limit what is collected to only what is necessary to achieve a legitimate goal for the school system.

[8] See, for example The Federal Trade Commission's action against education technology provider Chegg Inc. https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf

Goals and Objectives

Goals	Objectives
Determine the level of attention educators and their administrators have for minimizing the amount of data they gather regarding students and the policies school systems follow in selecting third party data to handle student data.	Engage a Privacy Fellow to assist in the collection, categorization, and statistical coding of online privacy policies and guidelines in U.S. school systems.
Develop curriculum to address limitations in the ways school systems train teachers and administrators regarding the use of student data and develop an interactive online course and certification tool to help train educators and their administrators.	Engage an expert in developing interactive, digital education content. Identify a hosting service to maintain that content.
Deploy the interactive course and reach out to school systems to encourage adoption of the training.	Host, produce, and present program demonstrations for school personnel, including teachers, administrators, and members of boards of education. Host a yearly educators' forum at Fordham University School of Law.

Timeline of Activities

Year 1:

- Months 1-3: Hire and train a full-time Privacy Fellow to oversee and administer the program.
- Months 3-4: Develop research protocol for the collection of information from all U.S. school systems in consultation with Fordham University faculty engaged in empirical research.
- Months 4-5: Hire and train research assistants to help in the collection and statistical coding of the data.
- Months 6-12: Engage in the collection and statistical coding of the data.

Year 2:

- Months 1-12: Continue in the collection and statistical coding of the data, draft and publish report on findings.

Year 3:

- Months 1-3: Develop curriculum and script for training materials.
- Months 4-6: Hire digital content creator to create interactive digital materials based on the program curriculum Update the curriculum and digital content as necessary.
- Months 7-9: Conduct pilot tests of digital materials.
- Months 9-12: Begin promotional and rollout activity, including initial presentations to education professionals including teachers, administrators, and boards of education.

Year 4:

- Continue promotional and rollout activity, including presentations to education professionals including teachers, administrators, and boards of education.
- Update the curriculum and digital content as necessary.
- Host an educators' forum.

Year 5:

- Continue promotional and rollout activity, including presentations to education professionals including teachers, administrators, and boards of education.
- Update the curriculum and digital content as necessary.
- Host an educators' forum.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

Most teachers in U.S. school systems face a limited budget and a significant number of demands on their attention to provide meaningful education to students that complies with state and federal guidelines. By developing an open-source interactive online video tutorial and certification system, educators will have easy access to the concepts of privacy by design. This will make review of these important concepts relatively easy given the limited amount of time teachers are able to focus on these issues instead of their primary focus of education.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

Funding Range

Scope	Cost with Funding for Proposal #1	Cost Without Funding for Proposal #1
5-Year Full-Scope	$119,600.00	$680,513.58
4-Year Partial-Scope	$108,400.00	$546,762.70
3-Year Partial-Scope	$92,200.00	$411,290.00
2-Year Partial-Scope	$36,000.00	$239,000.00
1-Year Partial-Scope	$12,000.00	$112,000.00

Budget Detail

With Funding for Proposal #1

	Year 1	Year 2	Year 3	Year 4	Year 5	*Totals*
Digital Content Creator	-	-	$50,000.00	$10,000.00	$5,000.00	*$65,000.00*
Research Assistants [9]	$12,000.00	$24,000.00	-	-	-	*$36,000.00*
Web Hosting Services	-	-	$1,200.00	$1,200.00	$1,200.00	*$3,600.00*
Outreach/Expansion Activities	-	-	$5,000.00	$5,000.00	$5,000.00	*$15,000.00*
Yearly Totals:	*$12,000.00*	*$24,000.00*	*$56,200.00*	*$16,200.00*	*$11,200.00*	***$119,600.00***

[9] Reflects four Research Assistants per semester, working 10 hours per week for 10 weeks at a rate of $20/hr., for half the first year and all the fall, spring, and summer semesters the second year.

Without Funding for Proposal #1

	Year 1	Year 2	Year 3	Year 4	Year 5	*Totals*
Privacy Fellow[10]	$100,000.00	$103,000.00	$106,090.00	$109,272.70	$112,550.88	*$530,913.58*
Digital Content Creator			$50,000.00	$10,000.00	$5,000.00	*$65,000.00*
Research Assistants[11]	$12,000.00	$24,000.00				*$36,000.00*
Web Hosting Services			$1,200.00	$1,200.00	$1,200.00	*$3,600.00*
Outreach/Expansion Activities			$5,000.00	$5,000.00	$5,000.00	*$15,000.00*
Educators Forum at Fordham			$10,000.00	$10,000.00	$10,000.00	*$30,000.00*
Yearly Totals:	*$112,000.00*	*$127,000.00*	*$172,290.00*	*$135,472.70*	*$133,750.88*	***$680,513.58***

11. Will the money be used to continue an existing project or create a new project?

The money will be used to start a new project. Specifically, the funds will be directed toward achieving the activities outlined in response to Question 8, above.

12. What target population will your organization's project benefit?

The ultimate target population for the project is children in grades K through 12 but the immediate beneficiaries will be educators for grades K through 12 who have more access to training in the use of student data online.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes. CLIP agrees to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

The initial success of the program will be measured by CLIP's ability to publish an empirical report on the policies and guidelines used throughout the U.S. to guide educators and their administrators in their

[10] Reflects salary plus mandatory benefits, accounted for an estimated 3% yearly cost-of-living increase.

[11] Reflects four Research Assistants per semester, working 10 hours per week for 10 weeks at a rate of $20/hr., for half the first year and all the fall, spring, and summer semesters the second year.

design of projects that use student data, as well as the ability to present the findings at educator forums. Following completion of the first phase of the project, indicators of success will be based on the number of certifications issued by the programs and the number school systems that issue guidance to educators in line with the principals of privacy-by-design.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

CLIP may use select results from the project in publications, conference papers, and presentations.

Proposal #3: Making Data Breach Notifications Work: A Large Language Model Approach to Safeguarding Consumer Privacy

7. Identify the organization's principal investigator or project director.

Aniket Kesari is an Associate Professor at Fordham Law School. His research focuses on law and technology, data science, and public policy. He uses techniques drawn from causal inference, machine learning, and natural language processing to investigate questions in law & tech, and he is also interested in integrating data science into empirical legal studies more broadly. Some of his recent scholarship looks at data breach notification laws, mandatory cybersecurity risk disclosures, privacy and algorithmic fairness, trademark search engines, and online hate speech. His work has appeared in law reviews (*George Washington Law Review*, *Berkeley Technology Law Journal*, *Illinois Journal of Law, Technology, and Policy*, *NYU Journal of Legislation and Public Policy*), peer-reviewed social science outlets (*Journal of Empirical Legal Studies*, J*ournal of Online Trust and Safety*), and peer-reviewed computer science proceedings (*Neural Information Processing Systems AI for Social Good Workshop*, A*CM Symposium on Computer Science and Law*). Prior to joining Fordham, Aniket was a researcher at NYU's Information Law Institute, UC Berkeley's Social Science Data Lab, and ETH Zurich's Center for Law and Economics. At Berkeley, he conducted research and developed training materials for an NSF grant funding hate speech research, and a NIH grant funding doctoral computational social science training. He holds a PhD from UC Berkeley, a JD from Yale, and BA from Rutgers – New Brunswick.

Tom Norton is the Executive Director of the Center on Law and Information Policy. His research focuses on privacy and data protection law and policy as well legal accountability in software systems. His work appears in both law and technology publications, and he has received support from the National Science Foundation. At Fordham, Tom teaches courses in Information Privacy Law. Tom earned a JD from Fordham University School of Law and served as CLIP's Privacy Fellow from 2014 to 2016. Prior to returning to CLIP as Executive Director, Tom was a litigation attorney at the law firm Arent Fox LLP in New York City. He is admitted to practice in the State of New York and the Commonwealth of Massachusetts.

Ron Lazebnik is the Academic Director of the Center on Law and Information Policy, the Director of Fordham's J.D. Externship Program, and the Director of the school's Samuelson-Glushko Intellectual Property and Information Law Clinic. His academic and scholarly interests include IP law, information law, and intersection of law and technology. Before joining Fordham, he was in private practice, where he helped represent clients in various matters involving patents, copyrights, trademarks, trade secrets, and general commercial litigation. He has also assisted in the defense of corporations and government agencies being investigated by the SEC, the Public Company Accounting Oversight Board, and the U.S. Department of Justice. Professor Lazebnik is a graduate of Harvard Law School, and holds a Master's degree in electrical engineering from Case Western Reserve University.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

Can law inform consumers about and safeguard them against identity theft? Every U.S. state now has a "data breach notification law" that requires breached firms to disclose these incidents to consumers. In theory, these laws should empower consumers to take control of their identity theft mitigation efforts and encourage organizations to adopt stronger cybersecurity standards.

However, these breach notices are often ineffective, in part because they are not legible to average consumers. Then-Attorney General Kamala Harris noted that breach notifications are often written at a college reading level, well above the 7th-8th grade average for American consumers.[12] These notices oftentimes contain legalese and are not clear about what steps consumers should take to opt into services such as identity theft protection. Some states have adopted requirements that breach notices be written in more accessible formats with clear headings, but most states have not.

This project aims to fill this gap by leveraging recent advances in machine learning and natural language processing (NLP) to translate data breach notifications for the public. Leveraging new NLP models such as GPT-4, CLIP will develop a pipeline for summarizing data breach notifications, simplifying them to the 7th-grade reading level, and assessing their efficacy at getting consumers to opt in to certain interventions such as subscribing to identity theft protection services, freezing their credit following a breach, and availing themselves of privacy-enhancing technologies such as two-factor authentication. CLIP will use survey experiments to assess whether consumers find our summaries more readable and actionable, and field experiments to assess whether simplified breach notifications spur consumer safeguarding of personal data.

This project builds on work previously done by PI Kesari on both data breach notification laws and legal summarizers. Previously, Kesari has empirically examined whether data breach notification laws reduce identity theft reports, and which statutory mechanisms might be most effective at reducing identity theft.[13] He is also currently working on a series of projects that use GPT-4 to summarize United States Supreme Court opinions and make them accessible at a 7th-grade reading level. Initially results from a survey in the field suggest that the methodology works well for improving reading comprehension of complex legal opinions.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

Much of the empirical work on data breach notifications has focused on retrospective assessments of whether these laws work and under what conditions. The methodology proposed here provides an interesting opportunity to turn to *prospective* work that can inform future changes to breach notification laws and directly help consumers. Data breach notification laws are the most popular and ubiquitous U.S. privacy laws and are updated routinely in all 50 states. The outputs from this project can therefore influence the development of the legal discourse around privacy and security in an impactful way and explore how to make sure these laws achieve their purpose.

Conducting field experiments on different delivery mechanisms for simplified breach notifications is also promising because of its potential to directly benefit research subjects. Regardless of the outcome of the

---

[12] Kamala D. Harris, Data Breach Report 2012, California Department of Justice, https://oag.ca.gov/system/files/attachments/press_releases/BREACH%20REPORT%202012.pdf.

[13] Kesari, A. (2022). Do data breach notification laws reduce medical identity theft? Evidence from consumer complaints data. Journal of Empirical Legal Studies, 19(4), 1222–1252. https://doi.org/10.1111/jels.12331; Kesari, Aniket, Do Data Breach Notification Laws Work? (August 30, 2022). Forthcoming, NYU Journal of Legislation and Public Policy. Available at SSRN: https://ssrn.com/abstract=4164674 or http://dx.doi.org/10.2139/ssrn.4164674.

research, this methodology will ensure that consumers who have been the victim of data breaches will receive some direct benefits.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

The major components of this project will include compute resources for generating simplified summaries, funds to run high-quality surveys to assess the usefulness of the summaries, and funds for a field experiment to measure consumer propensity to opt into privacy enhancing interventions. Beyond these funds, CLIP also anticipates that funding would be used host events to train law students in data breach notification drafting and response, and as well as to host an annual conference for training industry professionals on identity theft, data security, and privacy.

Funding Range

Scope	Cost
5-Year Full-Scope	$150,500.00
4-Year Partial-Scope	$123,000.00
3-Year Partial-Scope	$90,500.00
2-Year Partial-Scope	$58,000.00
1-Year Partial-Scope	$20,500.00

Budget Detail

	Year 1	Year 2	Year 3	Year 4	Year 5	*Totals*
Language Model Resources	$1,000.00	$1,000.00	$1,000.00	$1,000.00	$1,000.00	*$5,000.00*
Compute Resources	$500.00	$500.00	$500.00	$500.00	$500.00	*$2,500.00*
Surveys and Field Experiments	$5,000.00	$10,000.00	$5,000.00	$5,000.00	$0.00	*$25,000.00*
Research Assistants[14]	$12,000.00	$12,000.00	$12,000.00	$12,000.00	$12,000.00	*$60,000.00*
Travel for Conferences, Presentations, etc.	$2,000.00	$4,000.00	$4,000.00	$4,000.00	$4,000.00	*$18,000.00*
Conference Hosting	$0.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	*$40,000.00*
Yearly Totals:	*$20,500.00*	*$37,500.00*	*$32,500.00*	*$32,500.00*	*$27,500.00*	***$150,500.00***

[14] Reflects two Research Assistants per semester, working 10 hours per week for 10 weeks at a rate of $20/hr., for each of the fall, spring, and summer semesters.

11. Will the money be used to continue an existing project or create a new project?

The money will be used to begin a new project, as described in response to Question 8 above.

12. What target population will your organization's project benefit?

The project will benefit consumers who have been the victims of data breaches and identity theft more broadly. Nearly every American consumer has had data compromised in a breach. Nearly 3 million Americans suffer from identity theft annually. The average identity theft incident case costs $1,300 to resolve, making an incident massively costly to the average American consumer. The elderly, low-income, and Black Americans are victimized at particularly high rates. If the project is successful, it can inform future legal interventions to bolster data breach notification laws. Even without legal change, this research will help empower these populations to reduce their risk of identity theft.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes. CLIP agrees to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

CLIP will evaluate our real-world impact in several ways. First, CLIP will measure whether our interventions encourage better consumer uptake of privacy enhancing measures and technologies, and consequently reduce identity theft. Second, CLIP will track state and federal legislative changes to data breach laws and measure whether our interventions aimed toward improving their readability become the legal standard across various jurisdictions. Third, CLIP will monitor existing publicly posted data breach notices to see if our work encourages firms to write them more clearly and at an accessible reading level.

Beyond these outcomes, CLIP will also evaluate the training programs and measure whether the students and practitioners we train are better prepared to help their organizations prevent data breaches in the first place and manage the consequences of data breaches when they do occur. CLIP will emphasize the importance of understanding how breaches occur, plugging security holes once they are discovered, and communicating with consumers and other stakeholders clearly effectively so that they might safeguard their privacy.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

CLIP may use select results from the project in publications, conference papers, and presentations.

Proposal #4: Global South Privacy Researcher Fellowship

7. **Identify the organization's principal investigator or project director.**

Tom Norton is the Executive Director of the Center on Law and Information Policy. His research focuses on privacy and data protection law and policy as well legal accountability in software systems. His work appears in both law and technology publications, and he has received support from the National Science Foundation. At Fordham, Tom teaches courses in Information Privacy Law. Tom earned a JD from Fordham University School of Law and served as CLIP's Privacy Fellow from 2014 to 2016. Prior to returning to CLIP as Executive Director, Tom was a litigation attorney at the law firm Arent Fox LLP in New York City. He is admitted to practice in the State of New York and the Commonwealth of Massachusetts.

Ron Lazebnik is the Academic Director of the Center on Law and Information Policy, the Director of Fordham's J.D. Externship Program, and the Director of the school's Samuelson-Glushko Intellectual Property and Information Law Clinic. His academic and scholarly interests include IP law, information law, and intersection of law and technology. Before joining Fordham, he was in private practice, where he helped represent clients in various matters involving patents, copyrights, trademarks, trade secrets, and general commercial litigation. He has also assisted in the defense of corporations and government agencies being investigated by the SEC, the Public Company Accounting Oversight Board, and the U.S. Department of Justice. Professor Lazebnik is a graduate of Harvard Law School, and holds a Master's degree in electrical engineering from Case Western Reserve University.

8. **Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.**

The Global South Privacy Researcher Fellowship is a proposed collaborative initiative aimed at fostering international cooperation between CLIP and scholars from the Global South to address privacy issues affecting the Global South. As digital technologies continue to advance, privacy concerns have become increasingly complex and varied. This fellowship program seeks to facilitate knowledge exchange, capacity-building, and collaborative research by providing law researchers from the Global South with the opportunity to address pressing privacy concerns emerging facing Global South regions. Under the proposed program, each academic year (approximately August through May), CLIP will host a visiting researcher from a region in the Global South who will conduct substantive privacy research as well as participate in the public dissemination of their work.

Goals and Objectives

- **Facilitate scholarly and public discourse on privacy issues affecting the Global South.** The program will encourage the development of knowledge, expertise, and dialogue among academia and the public about privacy issues faced in the Global South.

- **Contribute to Policy and Practice.** Work produced by program participants will generate valuable insights and recommendations that can inform policy development and best practices in the field of privacy protection in the Global South and around the world.

- **Foster Collaboration.** The program will encourage and facilitate collaboration and knowledge exchange among law researchers from Global South regions and other areas of the globe.

Timeline of Activities

Year 1: Program Launch and Application Solicitation

- Establish a program committee comprising CLIP personnel and key stakeholders.
- Define program objectives, selection criteria, and eligibility requirements for visiting researchers.
- Promote the program and solicit applications for participation.
- Select an incoming visiting researcher for the following year's first implementation of the program.

Years 2, 3, and Beyond: Program Implementation

- Welcome visiting researcher to CLIP and Fordham.
- Researcher conducts substantive research on privacy issues.
- Researcher participates in seminars, workshops, and knowledge-sharing sessions.
- Researcher presents their findings in public lectures or seminars and publish research papers and reports based on their work.
- CLIP solicits and reviews applications for, and recruits, future visiting researchers.
- Foster further collaboration among program alumni and new researchers.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

CLIP proposes the Global South Privacy Researcher Fellowship for several reasons:

- **Complexity of Privacy Challenges:** Privacy issues are complex and multifaceted, often influenced by local culture, legal frameworks, and technological contexts. International collaboration allows for a more comprehensive understanding of these complexities by convening diverse perspectives from different regions.

- **Global Nature of Privacy Concerns:** Privacy concerns transcend national borders. Data flows, digital platforms, and technology companies operate internationally. Collaborating with researchers and experts on a global scale ensures a holistic approach to understanding privacy challenges.

- **Shared Learning and Best Practices:** Different regions of the world apply unique approaches and best practices in addressing privacy concerns. International collaboration provides an opportunity to share knowledge and learn from successful strategies implemented in diverse global contexts.

- **Increased Impact and Policy Influence:** By uniting researchers, institutions, and stakeholders from different parts of the world, the program can amplify the impact of its efforts. Research findings and policy recommendations generated through the program are more likely to be influential and relevant on a global scale. Because policymaking and regulatory decisions in the digital age have significant international ramifications, the program's collaborative efforts can influence global policies and standards, contributing to a more consistent and robust privacy framework.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

Funding Range

CLIP aims to award each visitor receiving the fellowship a $56,000 stipend. This figure accounts for an estimated $3,000 per month for rent and $1,500 per month for food and transportation for the approximately ten months (August through May) of each fellowship term, as well as $10,000 for travel to and from the U.S. Support for this program over multiple years would require funding as follows:

Total No. Years	Total Cost
1	$56,000.00
2	$112,000.00
3	$168,000.00
4	$224,000.00
5	$280,000.00

11. Will the money be used to continue an existing project or create a new project?

The money will be used to begin a new project, as described in response to Question 8 above.

12. What target population will your organization's project benefit?

The primary beneficiaries of this project include:

- **Visiting Researchers:** Scholars who participate in the program will gain access to resources, mentorship, and opportunities to conduct in-depth research on emerging privacy issues in their regions. The program will empower them to develop expertise, publish research, and contribute to policy discussions, ultimately enhancing their professional growth and impact.

- **Local Communities and Populations in the Global South:** As researchers investigate and address privacy issues specific to their regions, the knowledge generated through this project will benefit local communities and populations in the Global South. By promoting privacy protection and raising awareness of digital rights, the project contributes to safeguarding the interests and privacy of individuals and organizations in these regions.

- **Law and Policy Makers:** The research findings and recommendations produced by the program will be shared with policymakers, government agencies, and regulatory bodies in the Global South. These stakeholders will benefit from evidence-based insights to inform the development of privacy policies, legislation, and guidelines that better serve their constituents and uphold privacy rights.

- **The International Privacy Research Community:** The project's collaborative approach fosters knowledge exchange and collaboration among researchers, institutions, and experts from around the world. The international privacy research community will benefit from the enriched discourse and cross-cultural perspectives on privacy issues.

- **Civil Society and Advocacy Groups:** Non-governmental organizations and civil society groups dedicated to privacy and human rights in the Global South will benefit from the program's research. They can use this information to advocate for stronger privacy protections, raise awareness, and hold relevant stakeholders accountable.

- **The Technology and Business Sectors:** Businesses and technology companies operating in the Global South and across the globe will benefit from a better understanding of regional privacy expectations and regulations. This knowledge can guide them in developing privacy-compliant products and services, fostering trust among their users.

Evaluation

13. **Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?**

Yes. CLIP agrees to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. **Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.**

We will evaluate the success of the program in several ways. First, we will closely monitor the program's impact on scholarly and public discourse including research output, publications, and public engagements such as seminars and lectures. Second, we will assess the program's contribution to policy and practice by evaluating the extent to which the research conducted by visiting researchers informs policy decisions, both locally and globally. We will also analyze how their insights contribute to the development of best practices in the realm of privacy protection. Third, we will track the growth of professional networks and collaborations among visiting researchers, both within their home countries and across various Global South regions. Furthermore, we will seek feedback and testimonials to gain insights into how effectively the program promotes collaboration and cross-cultural understanding.

15. **Does your organization intend to use the results of the project in any publications, conference papers, and presentations?**

CLIP may use select results from the project in publications, conference papers, and presentations.

Exhibit K

December 21, 2023

Deborah De Villa, Esq.
Ahdoot & Wolfson, PC
2600 W. Olive Avenue | Suite 500
Burbank, CA 91505

Michael Sobol, Esq.
Lieff Cabraser Heimann & Bernstein, LLP
275 Battery Street, Floor 29
San Francisco, CA 94111

Re: Google Location History Litigation, No. 5:18-cv-05062-EJD (N.D. Cal.)

Dear Ms. De Villa and Mr. Sobol:

Free Press appreciates the invitation to submit a proposal to receive a *cy pres* award in the above case. Free Press would make full use of an award in any amount to promote the protection of internet privacy. All activities underwritten by the settlement fund would be educational and charitable in nature, in accordance with IRS statutes regulating 501(c)(3) organizations.

What follows is the information requested by the Court.

I am grateful for your consideration. Should you have any questions or need for additional information, please do not hesitate to contact me at (310) 809-2577 or jgonzalez@freepress.net.

Sincerely,

Jessica J. González
Co-CEO
Free Press

ORGANIZATION INFORMATION

1. Name of Organization

Free Press

2. Founding and History of Organization

At Free Press, we believe that an equitable media and technology system is essential to achieving a peaceful, multiracial democracy and realizing a just society.

Free Press advocacy helps to mold public policy decisions that change the media and tech landscape, and we sound the alarm when people's rights are in danger. We focus on protecting civil and human rights online (including online privacy), ensuring internet access is universal and affordable, uplifting the voices of people of color in the media, challenging old and new media gatekeepers to serve the public interest, defending press freedom, and reimagining local journalism.

Free Press was founded in 2003 to ensure that the people have a say in these crucial policy debates that shape media and technology. By 2005 we had launched Save the Internet, the first-ever U.S. campaign for Net Neutrality — a historic effort that united a broad and diverse coalition that grew to include millions of activists and thousands of groups. This set the stage for many successful coalitions, campaigns, protests and victories to follow, including winning strong Net Neutrality rules at the Federal Communications Commission in 2015, and strong privacy rules for ISPs at the FCC the following year. We also organized a blockbuster public awareness campaign in 2020 to hold online platforms accountable - called Stop Hate for Profit - which resulted in over 1,000 companies pausing advertising on Facebook in response to its irresponsible business practices.

Free Press has a strong track record of fighting for internet privacy, including authoring a model federal privacy policy that has been the foundation of many legislative and regulatory policy proposals. In 2013, Free Press began tackling government surveillance as well as commercial privacy concerns online. We organized Stop Watching Us, a coalition that formed in the wake of revelations about the NSA's widespread surveillance of U.S. phone calls and messages, and organized the biggest-ever protest against the government spying on its own citizens.

Headquartered in Washington, D.C., under the leadership of co-CEOs Craig Aaron and Jessica J. González, alongside a staff of 37 and a base of 1.4 million activists in all fifty states, Free Press combines organizing and advocacy power; legal, research, and policy expertise; narrative and cultural strategies; digital communications and media outreach capacity; and network-building

and field coordination. All of this is bolstered by the lobbying capacity of our related 501(c)(4) organization, Free Press Action Fund.

3. Current Goals for Online Privacy Work

Free Press plays a central role in building power behind media and technology policy ideas that advance racial justice and civil and human rights. As a watchdog and advocate, we educate policymakers, the press and the public; pressure corporations to serve the public interest; organize campaigns with grasstops and grassroots constituencies to hold decision-makers accountable; and lead winning coalitions. We believe in building coalitions and uplifting the voices of those not heard often enough in the halls of power, and a theme that goes across our work is our generosity to partners and our commitment to organizing diverse groups with shared goals.

The following is a brief description of our core goals in our Democracy and Digital Civil Rights program, which manages all of our online privacy advocacy.

A. Research and Organizing to Pass Federal Privacy Regulations

Free Press will organize and build off research products like *Insatiable: The Tech Industry's Quest for All Our Data*, to push the Federal Trade Commission to move forward with its ongoing proceeding on online privacy. That agency rulemaking proposes to limit the amount of data online platforms can collect and retain, and prohibit use of private data to discriminate against protected classes. As the agency progresses through its formal timeline for adopting such rules, Free Press will conduct legal and policy analysis, file its own comments, and assist allies and coalitions in filing theirs.[1]

[1] This submission last Fall built on the Disinfo Defense League Policy Platform, a collective effort on which Free Press led in crafting the legal, policy and factual research underpinning that document. The DDL Policy Platform outlines the steps Congress, the administration and the United Nations must take to protect digital civil rights. In December 2021, Free Press co-CEO Jessica J. González testified before Congress on many of these recommendations, in a hearing on disrupting dangerous algorithms and addressing the harms of persuasive technology. That hearing culminated a year of public education and collaborative work with then-Acting FTC Chair Rebecca Kelly Slaughter, along with other lawmakers and grassroots activists, to expose the pervasive problem of the use of private data for targeting disinformation towards communities who speak languages other than English.

Through Free Press Action Fund, a related, independent and autonomous 501(c)(4) organization, we will directly advocate in Congress and to the White House for data privacy laws and policies to stem unwarranted surveillance online.[2]

B. Public Pressure Campaigns to Protect User Privacy and Civil Rights

As co-chair of Change the Terms, a coalition of more than five dozen civil and digital rights groups that pressures online platforms to act responsibly, we will work to raise public awareness about how targeted disinformation and harassment campaigns are fueled by the collection and exploitation of people's personal data. With research, direct advocacy to companies and high-profile campaigns we will pressure companies to stop using private data to exploit and target their users with scams, disinformation, harassment and other abuse.

C. Protecting Online Privacy of Those Seeking Reproductive Healthcare

Post *Roe v. Wade*, law enforcement, government officials, and others began using online location data to investigate and harass people seeking reproductive healthcare. We sent Google a letter from 50+ civil rights organizations urging it to stop saving location data that contains sensitive health information. Google agreed to delete the location histories for users visiting abortion clinics. Shortly thereafter, Google broke that promise. Earlier this month Google announced that it will be updating its default policies to auto-delete every three months (instead of every eighteen). Free Press will continue to monitor the situation and apply pressure as needed.

4. Other Current Programs

In addition to our Democracy and Digital Civil Rights work, Free Press organizes three other program areas:

A. Equitable Internet: Access for All to the Open Internet

We fight for Net Neutrality, and advocate for public investment and policies to close the digital divide, all to ensure communications networks do not discriminate and are affordable, reliable and resilient. We are on track to restore the FCC's authority over broadband that was abdicated by the last administration, and to pass a federal Net Neutrality regulation through the Federal

[2] Most recently in Congress, we shaped a landmark bipartisan privacy and civil rights bill in 2022, the American Data Privacy and Protection Act (ADPPA), which would ban online platforms and other entities from collecting, processing and sharing people's data in ways that discriminate "on the basis of race, color, religion, national origin, sex, or disability." The ADPPA builds on core civil-rights principles of the kind laid out in model legislation that Free Press Action developed with the Lawyers Committee for Civil Rights Under Law in 2019. While the bill was not enacted, it was voted out of committee in the House by a nearly unanimous bipartisan vote, setting the stage for future advocacy and eventual passage.

Communications Commission in 2024 and defend that regulation in court in the year that follows.

B. Future of Journalism: Increasing Sustainable News and Civic Information

Free Press is committed to transforming the policies and practices that shape local journalism to create civic media that helps communities thrive. Through its journalism initiatives, Free Press designs and advances state and federal policies that sustain an accessible, diverse and equitable civic-information system. Alongside this work, we organize with communities and engage newsrooms to build power behind promising policies and reshape newsgathering practices to meet local needs.

C. Media Reparations: Reckoning With History and Envisioning a Liberatory Future

Through our Media 2070 project, we call on newsrooms, media and tech companies, the government and the broader public to reckon with and repair the historical and ongoing harm our nation's media system has caused Black communities.

5. Past Cy Pres Awards

We are honored to have been entrusted as the recipient of the following *cy pres* award:

2012	$75,000	*Valentine v. NebuAd, Inc.*, No. C08-cv-05113 (N.D. Cal.)

The award was unrestricted rather than allocated to a specific project. Free Press used this funding to advance our public interest work on internet access and data privacy and security.

6. Charity Navigator Ratings

On Charity Navigator, Free Press has the highest-possible 4-star rating, with an additional rating of 99 percent.

On Guidestar (Candid), Free Press has achieved a Platinum Transparency rating (the highest possible).

On Great Nonprofits, Free Press has maintained a Top Nonprofit rating for more than ten years running.

GRANT PROPOSAL

7. Project Director

Jessica J. González, co-CEO. An attorney and racial-justice advocate, Jessica is a leader in the fight to push media and tech companies to crack down on hate, disinformation and privacy violations online. She has testified before Congress on multiple occasions on issues including discriminatory algorithms, privacy and civil rights, tech accountability, Net Neutrality, media-ownership diversity and affordable internet access. Jessica co-founded Change the Terms, a coalition of more than 60 groups that works to disrupt online hate, helped lead the Stop Hate for Profit campaign's Facebook advertising boycott and sits on the Real Facebook Oversight Board. She has been featured in the *New York Times, Washington Post*, *Los Angeles Times*, on CBS, CNN, NPR and more. She sits on the boards of America's VOICE and the Latino Media Collaborative. Previously, Jessica was the executive vice president and general counsel at the National Hispanic Media Coalition, where she led the policy shop and coordinated campaigns against racist and xenophobic media programming. Prior to that she was a staff attorney and teaching fellow at Georgetown Law's Institute for Public Representation.

For a complete Free Press staff list and full bios see www.freepress.net/about/staff.

8. Summary of Proposed Program

Over the next three years, Free Press plans to set and advance priorities, in collaboration with allied organizations across the media, tech and democracy field. We will fight to protect privacy and other civil rights online, ensure public safety, uphold information integrity, and support democratic processes and values. In summary, Free Press plans to:

A. Release research that informs educational and policy interventions.

Free Press is currently implementing a research agenda that will help raise public awareness on the extent and effects of online privacy violations, and that will support both government and corporate policy interventions to protect online privacy. In December 2023, Free Press launched a national polling project that aims to better understand what Americans understand and want when it comes to online privacy (and on other media and tech issues too). This research will inform our testing of educational messages in 2024 that will be designed to build support for public policies to regulate tech companies and increase privacy protections, as well as messages that help folks better understand how media, tech and AI are impacting our privacy and influencing our election information environments. In Q1 2024, we'll release the poll's findings, using the data to build persuasive public education campaigns for corporate accountability and government interventions to enhance user privacy online.

B. Launch public education campaigns that support policy interventions and pressure tech companies to stop using private data to target their users.

With the aim of reaching the press, policymakers, tech companies and the public, our campaign will educate these target audiences about how nefarious actors are using people's digital data, discriminatory algorithms and AI to undermine democracy. We intend to use these calls to action to build public support for public policy interventions that:

- Minimize the collection, retention and use of people's personal data to discriminate based on race, ethnicity, nationality, gender, LGBTQ+ status, or other protected categories.
- Curb unnecessary tracking of people's geolocation, healthcare, or other personal data.
- Reduce the virality and visibility of hate and disinformation flowing from machine learning tools that target users along an array of private identity markers.

In partnership with our Change the Terms coalition partners, in 2024 we'll launch an additional campaign that will pressure social media companies to improve election integrity policies, refrain from using people's data to manipulate them and enforce content moderation policies throughout the 2024 election cycle and 2025 inauguration.

Over the next three years, we will also shine a light on platforms' failures by releasing research and analysis on companies' policies, and their enforcement and governance structures. We'll also dialogue directly with platforms to improve those policies. Free Press will continue to watchdog corporations for privacy violations and be prepared to launch corporate pressure campaigns as needed to protect online privacy.

C. Anchor policy analysis and advocacy on treating data abuse as a civil rights and justice issue.

Over the next two years, Free Press will continue to build momentum and political and legal cover for the Federal Trade Commission to move forward with its rulemaking on commercial surveillance and online discrimination. In 2024, we'll ramp up pressure for the FTC to move forward in that proceeding. Once the agency successfully adopts rules, we expect to have to defend those rules against legal challenges in the following year.

In Congress, we are seeing bipartisan disdain for tech excesses, and bipartisan support for bills like the Fourth Amendment Is Not For Sale Act, the Government Surveillance Reform Act, and the American Data Privacy and Protection Act. We will continue to provide research, analysis and education on ways to strengthen these bills and build broad support for their passage.

To empower grassroots groups led by people of color to set the agenda in these policy debates, Free Press will continue advising more than 200 Disinfo Defense League groups on policy and advocacy strategies. We will coordinate tactics with them to bring attention to the experiences of communities of color when it comes to harm from privacy invasions, discrimination, and targeted hate and disinformation online. This past year, we began collecting stories that illustrate the harms caused by such privacy invasions and discrimination, all to help supply federal agencies with the evidence they need to ground their own legal strategies and actions. In the coming year, Free Press will continue to document these stories and amplify them, by supporting grassroots engagement among impacted communities with the FTC's commercial surveillance proceeding, urging leaders to prioritize solutions that address discrimination, online privacy and civil rights.

9. Approach and Rationale

Social media and other tech companies profit from collecting vast quantities of people's personal data, which they've used along with ad-targeting tools and AI to discriminate against people based on their race, gender and other identities. For too long, women, LGBTQ people and people of color have been disproportionately harmed by this system of increasingly automated exploitation and discrimination. Companies and governments collect information from people that is then used to exclude them from economic and educational opportunities, deprive them of civil liberties, discourage their civic participation, and target them with disinformation. Free Press is committed to bringing front and center an analysis that shows the impacts on these communities; and to elevating their voices, stories and leadership when it comes to advancing and implementing solutions that advance civil and human rights.

The *Google Location History Litigation* reveals what is a chronic and foundational problem of tech platforms' exploitative business models. There is an urgent need for privacy regulation to hold tech giants, data brokers and all who facilitate the data marketplace accountable; and to protect users' privacy and civil rights. These regulations must prioritize:

- Data minimization: narrowing the permissible scope for the collection, retention, use and sale of personal data, allowing only what is necessary and proportionate to provide or maintain the specific product or service that a user requests;
- Transparency: enabling us to see whether companies are complying with their own policies (and, in the future, regulatory requirements);
- Digital civil rights: protecting people's rights so personal data isn't used to discriminate against or disadvantage us on the basis of protected characteristics;
- Data control: giving people easy and clear choices on how their data may be collected and used, as well as the ability to delete previously collected data; and

- Private right of action: letting people go to court when their civil rights and privacy rights are violated.

Free Press employs a team of lawyers, economists and policy researchers to analyze and develop public policies and educate policymakers and the public.

10. Funding Requirements

Free Press requests an award of $5 million over a three-year period, structured as $1.4 million in year one; $1.7 million in year two and $1.9 million in year three.

This level of support represents approximately 20% of our projected annual budget, which is $7.5 million in 2024, $8.25 million in 2025, and $9 million in 2026.

Funds would be targeted to cover staffing, direct and indirect costs of the Democracy and Digital Civil Rights program area that manages all of our online privacy advocacy and campaigning. The core team includes 7 full-time staff:

Co-CEO, Jessica J. González
VP of Policy and General Counsel, Matt Wood
Senior Counsel and Director Digital Justice and Civil Rights, Nora Benavidez
Senior Advisor, Economic and Policy Analysis, S. Derek Turner
Policy Counsel, Jenna Ruddock
Managing Director, Candace Clement
Campaign Manager, Rose Lang-Maso

This team is supported by time from 30 other staff in executive, marketing/communications, operations/finance/security, and development roles. Salaries, payroll taxes and benefits amount to 75% of all costs in any year. Therefore if awarded $5 million, $3.75 million would ensure retention of current staff and modest expansion of up to two full-time positions early in the three year timeframe.

Added capacity will help Free Press in expanding coalition coordination, education and policy advocacy efforts at the FTC, as well as mobilizing grassroots support to ensure the adoption of strong privacy regulations by the same agency. In year three, we will shape the implementation of the FTC rules, including by ensuring that any regulations survive judicial scrutiny, and by tracking and flagging corporate practices that would seem to violate those new rules.

Direct program costs include consultant and advisor fees to conduct research and polling; publications and communications; evaluation; meetings/events and travel. Indirect costs include allocation of Free Press overhead such as rent, utilities, insurance, legal, audit, website, and

licensed software. Non staffing direct and indirect costs would be $1.25 million over the three year period.

If the *cy pres* funding granted is smaller or larger, we can accept a different amount and will seek to leverage this support with additional funding from private foundations, public charities and individual donors. Free Press has a longstanding gift acceptance policy designed to ensure our independence and sole focus on the public interest. We do not accept donations from for-profit corporations or government entities. This differentiates Free Press from many organizations in our sector.

Free Press has a demonstrated track record of effective stewardship of multi-year funding, and many current multi-year supporters have high trust in our organization's financial capacity such that they distribute the entire grant up front. In these instances Free Press internally restricts funding for the future years, retaining funds in FDIC insured accounts.

11. Use of Funds

Cy pres funding will be used to continue existing Democracy and Digital Civil Rights program work that has demonstrated success, shown strong momentum, and proven the ability to replicate or expand. Full funding at the amount requested will enable strategic expansion of capacity to carry out the goals outlined above.

12. Target Population

Free Press' online privacy advocacy will protect the privacy and civil rights of all Americans, but especially classes of people protected under federal civil rights law.

Free Press prioritizes serving communities that don't often have a voice in policy making, particularly communities of color. Our work in this area is led by our co-CEO, a Mexican American woman, and the Free Press team, which is half people of color.

A key focus of Free Press activities is to educate policymakers at independent federal agencies such as the Federal Communications Commission and Federal Trade Commission, as well as decision-makers in Congress, at the White House, Commerce Department and Justice Department.

EVALUATION

13. Reporting

Free Press has strong capacity to monitor program outcomes and deliverables and to provide interim and final evaluation and impact reports. Free Press agrees to provide a report to the Court and the parties every six months, informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. Evaluation and Success

Free Press utilizes the "OKRs" (Objectives and Key Results) framework to set and evaluate goals. At the beginning of the year, and again at the outset of each quarter, the executive team sets organizational-wide OKRs, and each team, including the Democracy and Digital Civil Rights team, sets supporting OKRs, which will enhance or promote the protection of internet privacy. Evaluation metrics will include campaign progress, legal and regulatory successes, field reach and growth, research impact, event success, equity, press and media reach, and fiscal and operational health. Evaluation is rigorous and includes monthly, quarterly, and annual reflections at the staff and board levels, so as to learn from challenges and build from success.

15. Publications

Results of the project will be published in legal filings and testimony, research reports, policy agendas, fact sheets and memos, blog posts and op-eds. These products are disseminated widely via press releases, earned press, and conference presentations, and are freely accessible for download at our website at www.freepress.net.

Each year, Free Press earns thousands of media hits, where our policy positions and analysis are shared with the public. For example, in 2022 we had 3,500 press hits in outlets including ABC, the Associated Press, the BBC, CBS, CNN, *The New York Times*, NBC, *On the Media*, Reuters, *The Wall Street Journal*, *The Washington Post* and *USA Today*. Our op-eds appeared in places like *The Boston Globe*, CNN, *The Columbia Journalism Review* and *USA Today*.

Exhibit L

In re Google Location History Litigation, No. 5:18-cv-05062-EJD (N.D. Cal.)

CY PRES *RECIPIENT APPLICATION FROM THE FPF EDUCATION AND INNOVATION FOUNDATION (FPF)*

Organization Information

1. Name of organization.

FPF Education and Innovation Foundation (Future of Privacy Forum, FPF)

2. Discuss the founding and history of the organization.

FPF is a 501(c)(3) non-profit organization that serves as a catalyst for privacy leadership and scholarship. Founded in 2008, the organization has become a trusted partner, working with academics, consumer advocates, policymakers, regulators, industry, and other thought leaders to explore the challenges posed by evolving technologies and business practices. With offices in Washington, DC, Brussels, Singapore, and Tel Aviv, FPF works to advance responsible data practices in the United States and brings to bear its privacy thought leadership, technological expertise, and legal background to its work around the world.

FPF has a demonstrated track record of addressing internet privacy concerns and promoting the protection of internet privacy.

3. Describe the organization's current goals.

FPF is an organization that believes: 1) that privacy is a fundamental human right; 2) that data protection is one effective means to balance rights and freedoms in society; 3) that law, policy, and technology can mitigate harms of data use and misuse; 4) in the fair and ethical use of technology to improve people's lives; 5) in the power of inclusive collaboration; and 6) in equitable access to the benefits of the digital world.

FPF has bridged the policymaker-industry-academic gap to explore the challenges posed by evolving technologies and develop privacy protections, ethical norms, and workable business practices. Our work involves translating ideas or concerns raised by academics, advocates, companies, and policymakers into policy solutions and convening key stakeholders to discuss and determine best practices across a range of industries and sectors. FPF is led by Jules Polonetsky, an international authority on responsible data practices, and has more than 50 staff and policy fellows and an Advisory Board of thought leaders from industry, academia, and civil society. FPF is supported by over 200 leading companies, the National Science Foundation, and prominent private foundations such as the Bill and Melinda Gates Foundation, the Alfred P. Sloan Foundation, and the Chan Zuckerberg Initiative.

4. Provide a brief description of the organization's current programs.

FPF brings together experts and thought leaders from industry, academia, and government to explore the challenges posed by emerging technologies and develop privacy protections, ethical norms, and workable best practices. We publish original research and analysis, educate stakeholders, and convene thought leaders to identify pragmatic steps that improve internet privacy. Our programming includes work in the following areas, among others:

- ***Mobility and Location***: FPF advances privacy practices and understanding related to new in-vehicle technologies, advanced mapping techniques, and the transportation sharing economy. We help ensure responsible practices are in place so that the benefits of these technologies will be well received by consumers. FPF has been at the vanguard of policy and discussion related to data use in connected cars, autonomous vehicles, smart transportation, rideshare platforms, modern mapping technologies, and location-based services that rely on mobile phones and other connected devices.
- ***Ethics and Data Sharing***: FPF engages stakeholders across academia and industry to produce best practices and ethical review structures that promote responsible research. Our work is centered around the goal of streamlining, encouraging, and promoting responsible scientific research that respects essential privacy and ethical considerations throughout the process. FPF also works with policymakers to develop legislative protections that support effective, responsible research with strong privacy safeguards, including hosting events that allow policymakers and regulators to engage directly with practitioners from academia, advocacy, and industry.
- ***Immersive Technologies***: FPF works with experts from industry, academia, and civil society to identify the privacy and data protection risks in this nascent field, which includes all extended reality technologies (XR) such virtual reality (VR) and augmented reality (AR). FPF analyzes how these technologies are implicated by existing and emerging regulations and develops best practices and policy recommendations.
- ***Artificial Intelligence (AI)***: FPF aims to address the unique privacy impacts resulting from the expanded use of machine learning, AI systems, and XR technologies. We bring together corporate and academic stakeholders to discuss privacy issues and work with industry, academic, and civil society partners to develop best practices for managing risk in AI and assess whether historical data protection concerns around fairness, accountability, and transparency are sufficient to answer the ethical questions raised by these emerging technologies and their evolving uses.
- ***Advertising Technology (AdTech)***: FPF explores new and evolving advertising technologies and provides guidance on potential privacy issues. We help bring stakeholders together to discuss commercial benefits of advertising technologies as well as the need to address related privacy issues to build and maintain consumer trust.
- ***De-Identification***: FPF develops models that improve transparency and terminology around and advance practical measures of data de-identification, research ethics, and algorithmic decision-making. We focus on applying a combination of practical strategies and high-level thought leadership to address new opportunities and privacy risks presented by novel uses of personal information.
- ***Health and Wellness***: FPF explores issues at the intersection of health, data, and privacy, with a primary focus on the privacy challenges related to the collection, use, and sharing of data outside of Health Insurance Portability and Accountability Act (HIPAA)

regulations. The program brings together stakeholders to analyze how new technologies and data practices in the health and wellness ecosystem can impact individual privacy and promote the more effective and ethical use of data.

- ***Open Banking***: FPF works with a community of experts to identify the privacy and data protection risks in this space, educate policymakers about the challenges facing the open banking ecosystem, and develop best practices and policy recommendations.
- ***Biometrics***: Biometric technology continues to be adopted in many sectors, including financial services, transportation, health care, computer systems and facility access, and voting. In many cases, this technology is more efficient, less expensive, and easier to use than traditional alternatives, while also eliminating the need for passwords, which are broadly recognized as an insufficiently secure safeguard for user data. FPF aims to address privacy concerns around the collection, use, storage, sharing, and analysis of the data that are generated by these systems.
- ***Global Privacy***: FPF engages stakeholders in industry, academia, civil society, and regulatory bodies to facilitate the exchange of ideas and to foster understanding between the American privacy culture and data protection regimes around the world. We focus on tracking and analyzing policy and legal developments in Europe, Asia-Pacific, the Middle East, and Latin America. FPF has built strong partnerships across these regions through its convenings for policymakers and regulators (for example, through the inaugural convening of the Global PETs (Privacy Enhancing Technologies) Network in 2023). This engagement helps global regulators, policymakers, and data protection authorities better understand the technologies at the forefront of data protection law.
- ***Youth and Education Privacy***: FPF aims to ensure that child and youth privacy is protected as new education technology and uses of student data are employed to help students succeed. FPF believes that there are critical improvements to learning that are enabled by data and technology, and that the use of data and technology is not antithetical to protecting student privacy. To facilitate this balance, FPF equips and connects advocates, industry, policymakers, and practitioners with substantive practices, policies, and other solutions to address education privacy challenges at both the K-12 and higher education levels.
- ***Cybersecurity***: FPF examines the overlap between data privacy and cybersecurity and how different laws and policy regimes tackle that overlap. The Privacy and Cybersecurity Expert Group and the Inaugural Advisory Committee also provide space for collaboration and facilitate the opportunity to elevate practices and approaches.

5. Has your organization ever received a prior *cy pres* award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.

FPF has been the recipient of the following *cy pres* awards:

- FPF was previously awarded funds under the settlement in Lane v. Facebook. The settlement of that case created a pool of *cy pres* funds to be administered by the Digital Trust Foundation. FPF received $150,000 ($125,000 original, plus $25,000 supplemental) over 24 months for the activities detailed below and here:
    - This grant supported the creation of resources, convenings, and activities designed to educate stakeholders on legal uses of student data, opportunities to correct

inaccurate data, and ways to increase privacy controls and protections. FPF relaunched its website FERPA|Sherpa (now called Student Privacy Compass), named after the federal law governing student data privacy, in June 2017 with a slew of updated and new resources for parents, schools and districts, ed tech companies, and policymakers. New resources included: The "Parent's Guide to Student Data Privacy," developed with the National PTA and Connect Safely in English and Spanish, to provide families with information about their rights under FERPA and COPPA; and The Educators Guide to Student Data Privacy, developed with Connect Safely to enable teachers to educate themselves about how to evaluate an app or program and protect a student's personally identifiable information. Convenings included: The National Student Privacy Symposium, which gathered more than 220 industry advocates, privacy experts, and educators in Washington, DC to discuss the value of student data and the requirements for student data privacy; and a Student Privacy Boot Camp at UC Hastings Law School in San Francisco, where approximately 40 education technology startups learned about pertinent student privacy laws and their own responsibilities to protect student data in partnership with schools. In addition to new resource development and convenings, FPF also partnered with the Houston Independent School District (ISD) to engage students in all grades in creating videos that address data privacy issues affecting their peer groups. Winning videos were posted on FERPA|Sherpa and Houston ISD websites.

- FPF was previously awarded funds under the settlement in Guarisma v. Microsoft Corp., No. 1:15-cv-24326-CMA.: Per Section VI. THE SELECTION OF A CY PRES RECIPIENT funds that could not be distributed due to uncashed settlement checks were "… distributed (with the Court's approval) to Future of Privacy Forum (https://fpf.org) as a *cy pres* recipient on behalf of the Class." FPF received $22,800. These unrestricted funds were used to support FPF's general work to advance privacy.

6. Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?

FPF currently holds a 4-star (100%) rating for Accountability and Finance from Charity Navigator.

Grant Proposal

7. Identify the organization's principal investigator or project director.

John Verdi, JD, FPF's Senior Vice President of Policy, will serve as Principal Investigator (PI) and provide overall direction and oversight.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

Background and Issue Addressed: Rapidly evolving technologies and business practices increasingly rely on location data and other sensitive personal information in order to properly function. Sensitive data use is a key issue across FPF's portfolio: location data impacts

connected cars and mobile apps, sensitive health information is increasingly used for critical research, sensitive biometric data is used by immersive technologies and identity verification services, data about children and youth are categorically sensitive, and large data sets are utilized for training and maintaining AI tools. At the same time, sensitive personal data poses substantial privacy risks for individuals about whom it pertains or relates. Navigation apps can leak individuals' location history to stalkers, publicly operated AR devices can collect detailed images and profiles of unsuspecting bystanders, and health data can be breached, revealing medical conditions and treatment causing ostracization, social stigma, or other harms. Sensitive data can also be inferred from the collection and analysis of other data, with additional risks, including risks as to accuracy, bias, and discrimination.

Policymakers recognize the risks posed by sensitive data use, but recent attempts to set strong internet privacy rules have struggled to find the right approach to regulation. This is unsurprising, since data protection experts routinely grapple with the best way to mitigate the risks that arise from sensitive data use while preserving data-driven services and research that benefit individuals, communities, and society at large. At the same time, new approaches to transparency mechanisms, PETs, accountability frameworks, and data protection impact assessments (DPIAs) promise to give stakeholders new tools to address the challenges.

Goals and Objectives: FPF seeks an award of *cy pres* funds to support an ambitious three-year project that will: 1) identify and analyze the privacy risks associated with the collection and use of sensitive personal data - with a particular focus on location data - by organizations; 2) identify pragmatic strategies that can mitigate those risks; and 3) promote technical, legal, and policy tools that can implement the mitigation strategies.

FPF's overall organizational goals include: 1) increasing stakeholder understanding of the privacy risks associated with connected products and services that process location data and other sensitive personal information; 2) identifying practical strategies to mitigate the privacy risks; and 3) promoting technical, legal, and policy tools that can implement the mitigation strategies.

Approach and Activities: FPF proposes a cross-disciplinary project with a community of lawmakers and policymakers, private sector leaders, civil society advocates, legal and technical experts, and other key stakeholders to advance a general understanding of: 1) the drivers of the collection, transfer, and use of personal data, and key risks arising from sensitive data processing by companies, other organizations, and researchers; 2) how risks are distributed between different communities, including historically marginalized communities; 3) the most promising mitigation strategies; and 4) practical paths toward implementing those strategies (e.g., best practices, self-regulatory codes, regulation, legislation, or other means). FPF will convene meetings with key stakeholders and analyze leading work regarding PETs, accountability frameworks, and DPIAs. FPF will publish recommendations for practical ways to meaningfully define, control, regulate, and guard against the misuse of sensitive personal data.

This work will be performed by FPF experts in their respective sectors: Mobility & Location, Immersive Technologies, Ethics & Data Sharing, Health & Wellness, AdTech, and others, as appropriate.

For each area of work under the project, FPF will partake in a planning process, including the identification of specific SMARTIE (Specific, Measurable, Ambitious, Realistic, Timebound, Inclusive, Equitable) goal(s);[1] creation of a work plan, including tasks, timelines, milestones, and MOCHA (Manager, Owner, Consulted, Helper, Approver) role development[2] toward meeting each goal; and tracking activities and outputs to determine progress, measure success, and evaluate impact.

Timeline: The project plan will be flexible as needed to account for evolving technologies and business practices. FPF anticipates that the first year will focus on stakeholder briefings and meetings (e.g., privacy convenings and discussions) as well as large, publicly accessible events. The second year will involve research and analysis, and the third year will focus on publications and the promotion of resources and recommendations among key stakeholders.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

FPF has had substantial past success approaching internet privacy risks in this manner. Our work has led to self-regulatory codes of conduct recognized by President Obama and other leaders; stakeholder convenings that directly influenced strong legal protections for sensitive data; and best practices guidelines that promoted enhanced privacy safeguards for technology users on major online and offline services.

FPF's proposed approach builds on these past successes to address key issues confronting policymakers, industry, academics, civil society, and the public. We have identified the questions linked to sensitive data processing as some of the most pressing issues for all individuals and communities in light of the rapid evolution of the underlying technologies and business practices.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

FPF's requested budget for delivery of this work is $2,999,214 over a three-year period ($999,738 per year). This includes:

1. **Staff Salaries**: This funding helps support dedicated time for expert staff in the development and execution of all activities and deliverables outlined above. FPF's Events and Communications teams will provide support to events, publications, and media relations surrounding project deliverables.
2. **Fringe Benefits**: Fringe benefits are based on an overall 28.9% rate. This rate is made up of 3% for the 401(k)-employer contribution; 8.62% for medical, dental, and vision insurance contributions; 8.03% for life, disability, and other insurances; 1.6% for workers' compensation coverage; and 7.65% for employer payroll taxes.
3. **Events**: FPF elevates privacy issues and advances solutions among key stakeholders through high-profile symposia on privacy, data, and technology. FPF has allocated funds in this budget towards the planning and execution of the inaugural DC Privacy Symposium, an event that will bring together partners from across academia,

[1] https://www.managementcenter.org/resources/smartie-goals-worksheet/

[2] https://www.managementcenter.org/resources/assigning-responsibilities/

industry, government, and civil society. The symposium will serve as a forward-looking convening for practical, applicable, substantive privacy research and scholarship.

4. **Indirect Costs:** FPF does not have a negotiated indirect cost rate agreement (NICRA) with the U.S. government and therefore has calculated indirect costs at the 10% de minimis rate based on the direct cost base for each year. Indirect costs are calculated at 10% of all direct costs and applied across the budget.

11. Will the money be used to continue an existing project or create a new project?

The funds will be used to support a combination of new outgrowths or new phases of existing, successful projects (e.g., FPF's Data & Mobility Working Group) and new projects (e.g., new, original analysis of the privacy risks posed by contemporary practices involving collection, use, and sharing or sensitive data, including location data.)

12. What target population will your organization's project benefit?

FPF's project will benefit a range of stakeholders, including consumers, policymakers, industry data protection compliance experts, academics, members of civil society, and the public.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes, FPF will provide a report to the Court and the parties every six months informing them how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

FPF is dedicated to the enhancement and promotion of privacy protections, including individual privacy, with regard to the use of technology products and services. To evaluate the success of its *cy pres* grant, FPF will engage in goal-based evaluation, which includes the following:

- Identify, chart, and regularly review progress toward goals (described in the Grant Proposal, #8 above) and internally track activities and milestones.
- Hold internal planning and implementation calls to discuss progress and make adjustments (as required) to the planned implementation of this grant.
- FPF will create and share semiannual updates about its work on this grant through the reports to the Court (described above in #13).

FPF also creates an Annual Report each year to capture the organization's achievements and share progress towards its mission. The 2022 report can be found here.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

FPF regularly publishes our work and promotes our research in line with major conferences and events. FPF has presented at the following events in the past three years:

- International Association of Privacy Professionals (IAPP): Privacy. Security. Risk. Conference
- IAPP: Global Privacy Summit
- National Conference of State Legislatures (NCSL): Legislative Summit
- Access 4 Learning Community: Privacy & Interoperability Symposium
- Augmented World Expo
- Connected Health Initiative: AI and the Future of Digital Healthcare

FPF also hosts its own annual events where we feature not only our work, but the relevant work of others who study and analyze privacy risks, including:

- Privacy Papers for Policymakers, held annually since 2009
- Brussels Privacy Symposium, held annually since 2017

FPF's inaugural DC Privacy Symposium (to be held in June 2024) will bring together approximately 200 leaders from industry, academia, civil society, and government for a day-long forward-looking exploration of emerging topics in privacy and data protection. A report summarizing key takeaways will be prepared following the event.

The work of FPF and its expert staff have recently been featured or referenced in the following publications:

- *Bloomberg*
- *The Wall Street Journal*
- *POLITICO*
- *Washington Post*
- *Wired*

In the next three years, FPF will continue to look for ways to promote our work to the community and the key stakeholders who will benefit most from our work.

Exhibit M

GRANT PROPOSAL

Date: October 5, 2023
Organization:: Internet Archive
Address: 300 Funston Avenue, San Francisco, CA 94118
Email: **donations@archive.org,** (415) 561.6767
Proposal Submission: Joy Chesbrough, Director of Philanthropy
Principal Investigator: Thomas Padilla, Deputy Director Archiving & Data Services

Internet Archive Center for Next Generation Data Literacy

The nonprofit library Internet Archive seeks **$2,997,415** to launch the *Center for Next Generation Data Literacy (Center).* The Internet Archive works with libraries and allied organizations (e.g., local governments, universities, nonprofits) to support everyday people throughout the United States as they navigate internet privacy challenges.[1] Libraries have long helped a broad range of communities critically interact with data and protect their privacy. Examples of work performed by libraries in this vein can be seen in efforts to develop open educational materials, offer free training, and conduct privacy advocacy at the national level.[2] [3] As a responsible steward of the most complete archive of the internet (> 800 billion web pages, ~100 PB of data), with a track record of success working in partnership with hundreds of libraries and allied organizations to scale solutions that address diverse community needs, Internet Archive is uniquely positioned to deliver a next generation data literacy effort. With 1.5 million users and hundreds of partners accessing our resources, we have an opportunity to empower individual ability to safeguard privacy.[4]

Need & Opportunity

Privacy is a human right.[5] However, that right is less and less commonly realized in a rapidly evolving digital environment. As the internet and artificial intelligence driven tools become more pervasively integrated in our lives it becomes increasingly difficult to maintain the right to

[1] We define data literacy as the set of skills needed to critically produce, evaluate, share, and use data - a core component of data literacy entails the ability to critically manage the privacy of individual data amid a data ecosystem where a range of entities seek access to private data without permission, on a quid pro quo basis that can be difficult to assess, or through third parties.
[2] Civic Switchboard, https://civic-switchboard.github.io/about/.
[3] Privacy: An Interpretation of the Library Bill of Rights, American Library Association, adopted June 19, 2002, by the ALA Council; amended July 1, 2014; and June 24, 2019. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.
[4] Internet Archive, Community Webs, https://communitywebs.archive-it.org/.
[5] International Covenant on Civil and Political Rights https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

privacy. With respect to AI tools specifically, Meredith Whittaker, the President of the secure messaging platform Signal recently said:

> "[AI] requires the surveillance business model; it's an exacerbation of what we've seen since the late '90s and the development of surveillance advertising. AI is a way, I think, to entrench and expand the surveillance business model ... the Venn diagram is a circle."[6]

Recent literature on, "The Surveillance AI Pipeline" aligns with Whittaker's claim.[7] More broadly, individual privacy is subject to continuous assaults online from malicious ad-tracking on Google Chrome, to continued user monitoring by social media companies like Facebook post platform log-out, to data brokers that compile information about individuals and sell it without their consent.[8] [9] [10] A next generation data literacy training and advocacy solution is clearly needed to contend with evolving privacy challenges. Existing efforts that cultivate awareness of data privacy issues are fundamentally limited. The Berkman Klein Center for Internet and Society has a track record of impactful work but it is situated within an academic institution guided by ever-shifting, faculty-driven research prerogatives.[11] Library Freedom Project does wonderful work advancing privacy competencies but is organizationally precarious, with near total reliance on external funding.[12] Finally, no existing nonprofit effort to address privacy concerns has direct connection to the platforms and technologies that impact individual privacy. This gap is especially glaring in light of large language model (LLM) development and AI-driven service implementations that rely upon access to individual data. Addressing the challenge of individual privacy requires that an organization be mission-aligned with the scope of the challenge, has a track record of delivering solutions at the national level in partnership with a diverse range of organizations, is organizationally stable, has a strong public-facing user base that is aligned with internet privacy values, and is grounded in the technical challenges that protecting privacy presents in the contemporary digital environment.

Internet Archive is well-positioned to develop, implement, and advance a solution that protects individual internet privacy; a target population made up of a diverse population that uses the Internet for research and knowledge-seeking. Internet Archive's mission is global in scope and

---

[6] Coldewey, Devin. "Signal's Meredith Whittaker: AI Is Fundamentally 'a Surveillance Technology.'" *TechCrunch*, September 25, 2023. https://techcrunch.com/2023/09/25/signals-meredith-whittaker-ai-is-fundamentally-a-surveillance-technology/.

[7] Kalluri, Pratyusha Ria, William Agnew, Myra Cheng, Kentrell Owens, Luca Soldaini, and Abeba Birhane. "The Surveillance AI Pipeline." arXiv, September 26, 2023. https://doi.org/10.48550/arXiv.2309.15084.

[8] Amadeo, Ron. "Google Gets Its Way, Bakes a User-Tracking Ad Platform Directly into Chrome." Ars Technica. https://arstechnica.com/gadgets/2023/09/googles-widely-opposed-ad-platform-the-privacy-sandbox-launches-in-chrome/.

[9] EPIC - Electronic Privacy Information Center. "In Re: Facebook, Inc. Internet Tracking Litigation." https://epic.org/documents/in-re-facebook-inc-internet-tracking-litigation/.

[10] Cameron, Dell. "How the US Can Stop Data Brokers' Worst Practices—Right Now." *Wired*. https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/.

[11] Berkman Klein Center, https://cyber.harvard.edu/research/privacy.

[12] Library Freedom Project, https://libraryfreedom.org/.

reaches all ethnicities, ages and gender worldwide. Our activities are designed to encourage "universal access to all knowledge" for all people, with no cost to the public. Internet Archive has a deep track record of partnering with other libraries and allied organizations to maximize collective organizational ability to address core community needs. Examples of this work include but are not limited to the **(1)** Internet Archive's Community Webs program, a multi-year partnership with more than 150 public libraries focused on preserving underrepresented histories across rural and metropolitan areas through the cultivation of community data literacies[13]; **(2)** Co-founding Library Futures, a nonprofit national advocacy effort that works to advance equitable public access to information[14]; **(3)** the submission of many amicus briefs with allied organizations that seek to protect public access to information[15] [16] **(4)** as well as a multinational effort to "Build a Better Internet" with Creative Commons, Public Knowledge, Library Futures, and the Wikimedia Foundation.[17]

Internet Archive lends organizational stability to community focused efforts through adoption of a diversified organizational sustainability model that combines nonprofit services, external funding, and philanthropic support (high volume small contributions combined with major gifts). With respect to organizational grounding in the technical challenges that protecting privacy presents, Internet Archive has direct experience preserving the internet via the Wayback Machine and the underlying technologies that have impacted individual privacy across the 20th and 21st centuries, developing web-based digital services used by more than 1.5 million daily users, and responsibly experimenting with and implementing AI. Taken as a whole, these organizational characteristics and experiences uniquely position Internet Archive to develop a next generation data literacy effort that effectively empowers individuals on a national level as they contend with complex privacy challenges in digital environments. In order to meet this need, Internet Archive seeks support to create the *Center for Next Generation Data Literacy*.

The *Center for Next Generation Data Literacy* will:

- **convene** multi-sector privacy experts (e.g., academic, government, NGO, private) and community representatives to determine primary privacy challenges and opportunities. Convenings will support ongoing refinement of *Center* strategy, partnerships, and deliverables.
- **produce** openly accessible, expert-informed privacy education materials and policy work that supports delivery of free training and events for a diverse set of affected

[13] Internet Archive, Community Webs, https://communitywebs.archive-it.org/.
[14] Library Futures, https://www.libraryfutures.net/our-principles.
[15] Internet Archive amicus brief in Fox News vs. TVEyes, https://archive.org/details/InternetArchiveAmicusBriefInFoxNewsVTVEyes.
[16] Internet Archive amicus brief in Hiq Labs vs. Linkedin Corporation, https://epic.org/wp-content/uploads/amicus/cfaa/linkedin/42-EFF-DuckDuckGo-Internet-Archive-Amicus.pdf.
[17] Internet Archive Releases Report on Securing Digital Rights for Libraries, https://blog.archive.org/2022/12/01/internet-archive-releases-report-on-securing-digital-rights-for-libraries/.

communities throughout the United States. Special emphasis will be placed on ensuring that these materials benefit socioeconomically marginalized communities.

- **deliver 250-300** free privacy workshops and events in partnership with Regional Data Privacy Coalitions (West, Midwest, South, East). At least **5000-6000** individuals will have participated in in-person or virtual workshops. Workshop participants will come from all **50** States.

Internet Archive will advance this privacy training effort nationally through the formation and resourcing of Regional Data Privacy Coalitions managed by libraries and allied organizations committed to cultivating data literacy. Coalitions will be distributed across the Western, Midwestern, Southern, and Eastern regions of the United States. A focus on coalitions is intentional given recognition of the reality that progress in this space will depend on community specific combinations of organizational actors in order to effect optimal change. For example, a coalition focused on serving metropolitan areas could include a large library system, a single large municipal government, and a university while a coalition focused on serving rural areas could include multiple rural library systems, town governments, and tribal governments. The Regional Data Privacy Coalition model is inspired by prior library community experiences utilizing hub models to implement programs at the national level such as the Digital Public Library of America Hub Network, currently operating in 44/50 States.[18] Each Regional Data Privacy Coalition will drive outreach and education efforts in its region of the United States through **(1)** fund disbursement to libraries and allied organizations to hold free privacy workshops and privacy education events that make use of *Center* educational materials **(2)** privacy community building through formal (e.g., committee) and informal structures (e.g., interest groups) to support scaling of privacy awareness, **(3)** coordinated communications that highlight achievements making progress on privacy awareness (e.g., blogs, public events, news releases, interviews, open access articles), and **(4)** sharing workshop assessment data, lessons learned, and use cases from privacy awareness training and local community engagement that informs iterative refinement of *Center* educational materials and overall strategy. Through this coalition model, the *Center for Next Generation Literacy* will more effectively scale privacy awareness that is fit for purpose per community across the United States.

The *Center for Next Generation Data Literacy* will strengthen the ability of libraries and allied organizations throughout the country to cultivate privacy awareness. With *Center* support, hundreds of librarians and allied professionals will be given practical resources that advance data literacy in the communities they serve. In further support of this objective, the *Center for Next Generation Data Literacy* will establish partnerships with nonprofit organizations, academia, government, and mission-aligned private sector organizations that have a large public reach in order to increase *Center* impact. Representatives of each sector will serve on a multiyear advisory board to ensure that *Center for Next Generation Data Literacy* activities are as

[18] DPLA Hub Network, https://pro.dp.la/hubs.

responsive to community needs as possible and strategically aligned with complementary national efforts. The *Center for Next Generation Data Literacy* will scope all user engagement as inclusively as possible, so that all people regardless of vocation, education, cultural background, or geographic location can benefit from *Center* efforts.

Activities

Year 1 - Launch, Convene, and Produce

In the first year of activity Internet Archive will launch the *Center for Next Generation Data Literacy.* An advisory board will be formed and Internet Archive will use *Center* resources to hire an inaugural director of the *Center* and a coordinator. *Center* staff will convene stakeholder groups with representatives from organizations that Internet Archive has established relationships with like the Electronic Frontier Foundation, American Library Association, and Association of Research Libraries as well as representatives identified by the advisory board and Director. The Director will launch all four Regional Data Privacy Coalitions.

- Deliverables
    - Hold **advisory board and stakeholder privacy symposium** at Internet Archive that gathers and synthesizes primary challenges and opportunities in addressing individual data and internet privacy challenges.
    - Produce and publicly **release stakeholder-informed *Center* strategic roadmap and policy paper**. The roadmap and policy paper will be released openly on archive.org, promoted by strategic partners, and distilled into pieces with local news outlets and national news outlets such as Time, Wired, Ars Technica to encourage broader public engagement.
    - *Center* staff present on *Center* roadmap and policy paper virtually and in-person at relevant symposiums and conferences (e.g, Association for Rural and Small Libraries, Digital Library Federation, International Association of Privacy Professionals, PrivacyCon, American Library Association).
    - *Center* staff launch **4 Regional Data Privacy Coalitions** (West, Midwest, South, East).
    - *Center* staff **begin producing privacy training materials** in partnership with national privacy and education partners that support in-person and virtual training. Training modules will be recorded in order to support asynchronous training. Training materials will be vetted by community representatives prior to release.

Year 2 - Deliver, Support, Partner

During year 2 *Center* staff continue producing and refining privacy training materials, and support a coalition of hundreds of libraries and allied organizations in the delivery of these materials for benefit of diverse local communities in rural and metropolitan areas throughout the United States. *Center* staff form partnerships and begin implement a nonprofit funding sustainability model that sustains the *Center* post-launch.

- Deliverables
    - In partnership with Regional Data Privacy Coalitions, deliver **125-150** free privacy workshops and events focused on cultivating privacy skills. At least **2500-3000** individuals will have participated in in-person or virtual workshops or privacy events. Workshop participants will come from all **50** States. The public will have access to recorded training material modules to increase public reach.
    - *Center* staff **revise privacy training materials** based on community feedback provided by Regional Data Privacy Coalitions.
    - *Center* staff present on *Center* activities at relevant symposiums and conferences (e.g, Association for Rural and Small Libraries, Digital Library Federation, International Association of Privacy Professionals, PrivacyCon, American Library Association).
    - *Center* staff **hold the second national privacy symposium** at a partner organization venue - or where research identifies the greatest need for knowledge and regional diversification**.** The working symposium will inform *Center* strategy and produce a policy position paper that will address a core privacy challenge prioritized by *Center* stakeholders. The policy paper will be released openly on archive.org, promoted by strategic partners, and distilled into pieces with local news outlets and national news outlets such as Time, Wired, Ars Technica to encourage broader public engagement.
    - *Center* staff, in partnership with the advisory board and stakeholders **begins implementing a nonprofit sustainability model** that will sustain the *Center* post-launch funding.

Year 3 - Deliver, Support, Sustain

During year 3 *Center* staff will complete iterative development of privacy training materials per community feedback, and continue supporting coalitions representing hundreds of libraries and allied organizations in the delivery of these materials for benefit of diverse local communities in rural and metropolitan areas throughout the United States. Year 3 will have a particular focus on completing implementation of the nonprofit funding sustainability model that will support *Center* operations into the future.

- In partnership with Regional Data Privacy Coalitions, deliver **125-150** free privacy workshops and events. At least **2500-3000** individuals will have participated in in-person or virtual workshops or privacy events. Workshop participants will come from all **50** States. The public will have access to recorded training material modules to increase public reach.
- *Center* staff, **complete implementation of a nonprofit funding sustainability model.**
- *Center* staff **complete iterative development of privacy training materials** based on community feedback provided by Regional Data Privacy Coalitions and stakeholders.
- *Center* staff present on *Center* activities at relevant symposiums and conferences (e.g, Association for Rural and Small Libraries, Digital Library Federation, International Association of Privacy Professionals, PrivacyCon, American Library Association).
- *Center* staff **hold the final national privacy symposium** at the Internet Archive. The final symposium celebrates *Center* successes and produces a roadmap and policy paper for implementing privacy solutions and leveraging the resources of all stakeholders. The roadmap and policy paper will be released openly on archive.org, promoted by strategic partners, and distilled into pieces with local news outlets and national news outlets such as Time, Wired, Ars Technica to encourage broader public engagement.

Reporting & Evaluation

Center staff will report on project activities and objectives every 6 months to funders. Semiannual reports will cover: **(1)** Progress on activities and objectives **(2)** Lessons Learned **(3)** Challenges encountered, if any **(4)** Links to materials generated by *Center* (e.g., workshop materials, policy papers) **(5)** Links to outreach generated by *Center* (e.g., promotional blog posts, webinars, presentations), and **(6)** Financial Report detailing project spending. Key metrics include: formation of 4 Regional Data Privacy Coalitions, delivery of 250-300 privacy workshops and events, reaching 5000-6000 participants in all 50 States with privacy workshops and events, openly publishing 3 national policy papers, and conducting 6 conference presentations on *Center* activities. On a granular level, performance against metrics is tied to annual periods of performance - year 1, year 2, year 3. In support of *Center* reporting and evaluation, Regional Data Privacy Coalitions will issue quarterly reports to the *Center* on coalition activities, objectives, and spend.

A range of ongoing evaluation methods will be used to strengthen *Center* activities. All privacy education materials will include pre-workshop and post-workshop participant surveys to document participant demographics and assess participant success achieving privacy learning outcomes. Results from surveys in combination with feedback provided by Regional Data Literacy Coalitions will support assessment and ongoing refinement of educational materials. Securing additional feedback on educational materials from privacy and education partners throughout the project will support additional evaluation and ongoing refinement. Policy paper and conference presentation impact will be evaluated based on privacy and education partner feedback, downloads, citations, web traffic, and diversity of communities reached by these deliverables as evidenced by publication and conference venue.

Budget Rationale

Salaries and Wages

Director will serve as the executive leader tasked with administering all *Center* activities. The Director will be responsible for: *Center* strategy; liaising with *Center* advisory board; ensuring coalition activities meet strategic goals; partnership formation; sustainability planning and implementation; finances and reporting. The Director will be recruited immediately after notification of success seeking funding for the *Center*. The Director will dedicate 100% of their time to the *Center*.

Salary: 100% of FTE base salary ($110,000 with 6% annual COLA) x 3 years = $350,196
Benefits: Calculated at 20% of salary and wages for a total of $70,039
Thomas Padilla, Program Administrator, will recruit the Director and Coordinator of the *Center*. The Program Administrator will manage the Director. The Program Administrator

will provide strategic support to the Director, and provide additional administrative oversight to *Center* activities, objectives, and finances. The Program Administrator will dedicate 10% of their time to the *Center*.

Salary: 10% of FTE base salary ($143,850) x 3 years = $43,155
Benefits: Calculated at 20% of salary and wages for a total of $8631

Coordinator will be responsible for coordinating coalition reporting on a quarterly basis, *Center* communications, event planning, meeting coordination, and project managing *Center* privacy training material development. The Coordinator will be recruited immediately after notification of success seeking funding for the *Center*. The Coordinator will dedicate 100% of their time to the *Center*.

Salary: 100% of FTE base salary ($75,000 with 6% annual COLA) x3 years = $238,770
Benefits: Calculated at 20% of salary and wages for a total of $47,754

Regional Data Privacy Coalitions

Regional Data Privacy Coalitions (West, Midwest, South, East) will be established with libraries and allied organizations to support everyday people throughout the United States as they navigate data privacy challenges. Under administration by the *Center*, each Regional Data Privacy Coalition will drive privacy outreach and education efforts in its region through **(1)** stipend disbursement to libraries and allied organizations to hold free public privacy workshops and events that make use of *Center* educational materials **(2)** privacy community building through formal (e.g., committee) and informal structures (e.g., interest groups) to support scaling of privacy awareness, **(3)** coordinated communications that highlight achievements making progress on privacy awareness (e.g., blogs, public events, news releases, interviews, open access articles), and **(4)** sharing of workshop assessment data, lessons learned, and use cases from privacy awareness training and local community engagement that inform iterative refinement of *Center* educational materials and overall strategy.

Regional Data Privacy Coalitions will use *Center* subawards to support staff costs to advance project objectives and outreach costs with remaining funds allocated to stipends awarded to libraries and allied organizations to hold free privacy workshops and events.

Data Privacy Coalition West Funding:

- Workshop and event stipends for libraries and allied organizations: $360,000
- Program staffing costs: $84,000
- Program outreach costs: $6,000

- **3 year total $450,000**

Data Privacy Coalition Midwest Funding

- Workshop and event stipends for libraries and allied organizations: $360,000
- Program staffing costs: $84,000
- Program outreach costs: $6,000
- **3 year total $450,000**

Data Privacy Coalition South Funding

- Workshop and events stipend for libraries and allied organizations: $360,000
- Program staffing costs: $84,000
- Program outreach costs: $6,000
- **3 year total $450,000**

Data Privacy Coalition East Funding

- Workshop and event stipends for libraries and allied organizations: $360,000
- Program staffing costs: $84,000
- Program outreach costs: $6,000
- **3 year total $450,000**

Total cost: $1,800,000

National Privacy Symposiums

The *Center* will hold 3 national privacy symposiums that inform *Center* strategy, support formation of partnerships that help increase impact, and advance efforts that address privacy at the policy level. Funds will be used to cover event space, travel, and participant & staff support.

Total cost: $100,000

Coalition Activities

Throughout this project, *Center* staff will promote *Center* activities, liaise with Regional Data Privacy Coalitions, and secure strategic partnerships. Funds will cover flights as well as per diem and lodging aligned with standard Federal General Service Administration rates.

Total cost: $30,000

Professional Services

Center staff will secure professional services to support production of high-quality educational materials that advance data privacy - e.g., graphic design, brand identity, translation, accessibility, DEI, multi-media recordings.

Total cost: $27,000

Privacy & Education Partners

Center staff will compensate nationally renowned privacy and education partners for assisting with the creation of the privacy workshop content - authoring open access modules, instructional materials, and assessment strategies for reuse throughout the United States. Partners will be drawn from a range of sectors with demonstrated track record of excellence in this space.

Total cost: $60,000

Indirect

The total indirect costs for this project are $221,870. This number is calculated as 11% of an indirect cost base of $2,017,000 which is the total direct costs minus salaries and wages.

Total Project Costs

We are requesting a total of **$2,997,415** for the *Center for Next Generation Data Literacy.*

Outcomes

At the conclusion of its first three years of activity the *Center for Next Generation Data Literacy* will have achieved the following outcomes:

1. Delivery of no less than **250-300** privacy workshops and events. At least **5000-6000** individuals will have participated in in-person or virtual workshops. Workshop participants will come from all **50** States. Additional participants will be reached through availability of recorded training material modules.
2. Production of freely accessible privacy training resources that support libraries and allied organizations in their efforts to increase data and internet privacy awareness in the communities they serve.

3. Three annual privacy focused symposiums that inform *Center* as well as national strategy and collective action with respect to data and internet privacy challenges.
4. Three openly accessible privacy policy papers building on each national symposium that guide national responses to privacy challenges. These deliverables will be released openly on archive.org, promoted by strategic partners, and distilled into pieces with local news outlets and national news outlets such as Time, Wired, Ars Technica to encourage broader public engagement.
5. Six conference presentations that promote *Center* activities at relevant symposiums and conferences (e.g, Association for Rural and Small Libraries, Digital Library Federation, International Association of Privacy Professionals, PrivacyCon, American Library Association).
6. Strategic partnerships and implementation of a nonprofit sustainability funding plan that supports ongoing sustainability of *Center* operations post 3-year startup period.

Internet Archive is a convener and internet leader poised to strengthen data and internet privacy awareness for everyday people in communities large and small throughout the United States. As a nonprofit operating and promoting values of sound security controls and public privacy policies for decades, Internet Archive is excited to work with partners all over the United States whose reach is well known in the digital and web community. Launching the *Center for Next Generation Data Literacy* will bring together the strengths of the library community and allied organizations in order to educate and empower individuals to protect their privacy online. Privacy is a human right and Internet Archive is invested in making sure that right is maintained in an ever more complex digital environment.

ORGANIZATIONAL INFORMATION

Date: October 5, 2023
Organization:: Internet Archive
Address: 300 Funston Avenue, San Francisco, CA 94118
Email: donations@archive.org, (415) 561.6767
Proposal Submission: Joy Chesbrough, Director of Philanthropy
Principal Investigator: Thomas Padilla, Deputy Director Archiving & Data Services

Internet Archive History

A passionate advocate for public Internet access and a successful *Internet Hall of Fame* entrepreneur, Brewster Kahle has spent his career intent on a singular focus: providing *Universal Access to All Knowledge*. In 1996, Kahle founded the nonprofit Internet Archive, one of the world's largest digital libraries, serving more than 1.5 million learners around the world each day. For 26 years, the Internet Archive's staff of 160 engineers, archivists, scanners and librarians have been connecting knowledge seekers with the published works of humankind. Today, our main site, *archive.org*, is one of the world's top 300 websites, offering journalists, researchers, students, teachers, gamers, and millions of people access to more than 100 petabytes of data, including 625 billion web pages, 38 million digital books and texts, and millions of audio, video and software items. In 2001, the Internet Archive launched the Wayback Machine, which has grown to be the world's largest, longitudinal public archive of the web.

At the Internet Archive, we believe passionately that access to knowledge is a fundamental human right. The Internet Archive is a special place: a library, not a profit-seeking corporation, so we make our resources available to anyone for free, without ads or tracking, respecting the privacy of every patron. Like the internet itself, the Internet Archive is a critical part of the digital infrastructure, the "pipes and hard drives" through which knowledge flows to partners and people around the world. The Internet Archive works with more than one thousand library and university partners to create a free digital library, accessible to all. If the Internet Archive were to disappear, the public would no longer be able to look back and reference the history of the web. We would all be caught in the perpetual present, "digital dystopia" of our own making.

Goals & Accomplishments

The Internet Archive's goal has been about changing the world by preserving cultural artifacts and digitizing materials from around the world. By documenting our cultural history, we are providing information that would otherwise be lost. This is all being accomplished while providing equal access to people from all economic, cultural, educational, and technical backgrounds. The Internet Archive's main goal is to be a repository of knowledge. Please find our annual report highlighting our goals and accomplishments more in detail.

https://online.flippingbook.com/view/1037520727/

Core Programs & Descriptions
The Internet Archive has five core programs.

Wayback Machine
The Wayback Machine is an invaluable resource for academics, researchers, reporters, students and the public. It serves more than 800 people a day and allows anyone who has access to the Internet the opportunity to view websites that have changed over time. Journalists and fact-checkers use it to research and verify news stories, as well as archived versions of websites when the current version is not available on the Web. Even courts in some countries accept Wayback Machine webpage captures as evidence. The Wayback Machine has been capturing websites and web pages since the beginning of the World-wide Web. Internet Archive teams and bots capture digital information and web pages daily, and the information is stored on private servers.

Democracy's Library
The Democracy Library program will allow scholars, journalists, educators, businesses, and the general public the ability to easily access information governments have produced. Free and open access to public information is critical for any functioning democracy. Every citizen should be able to seek knowledge in the public domain without the hassles of paywalls, lace of efficient curation or lost or hidden resources. Compounding the issue, and one this program will solve, is the fact that much of the information governments have produced has never been digitized. The Internet Archive plans to digitize and preserve this information over the next few years and the goal of Democracy's Library will be to catalog and make findable important government documents, starting with those in the U.S and Canada. This will include laws, scientific studies & reports, safety standards, copyright records and much more.

Open LIbrary
Not everyone has access to a public or academic library – especially ones with good collections. That's where Internet Archive's Open Library comes in. Open Library began digitizing books in 2005 – and today is home to 7 million books digitized by the Internet Archive, including millions of downloadable public domain works and millions of modern texts available through Controlled Digital Lending. Our growth is continuously accelerating. As is our extensive physical and digital infrastructure. But throughout our growth, privacy remains one of our highest priorities. Which is one reason we build and maintain all our own systems. It allows us to better prepare for the future, but even more importantly, allows us to set our own standards of user privacy—so that third-party services, like AWS, cannot access patron browsing data.

Community Webs
The Internet Archive's Community Webs program entrusts the archiving of important resources to our country's most experienced professionals: public community librarians.

Ideally positioned to record events impacting their communities, the public librarians with whom we partner are committed to preserving their local history. This includes the actual voices of those most socially, economically, and politically at risk—voices and information that will ultimately frame history. The Community Webs program is allowing the voices of marginalized groups to be read and heard on the Internet.

Canadian Data Center

The Canadian Data Center is a secure and sustainable back-up for the entire Archive. Our goal is to continue providing access to knowledge for decades to come, and this project ensures we can and will. This Data Center stores everything in our Archive – as a back-up. It's a full, second live copy preserved outside the US - which ensures our data cannot be compromised by threats to a single system or location. Creating decentralization is part of our mission to provide a free and open Internet – and we firmly believe that providing Universal Access to All Knowledge includes access outside the United States, not restricted to a single nation or country. The Canadian Data Center also contains a scanning center and an extensive digital storage system which allows us to both digitize materials and house existing data from Canadian research centers, grassroots organizations, and Canadian libraries.

Charity Navigator

The Internet Archive has a 2 to 3 Charity Rating and that is only because our conflict of interest policy, tax forms and other documents were not uploaded into the system on time. These documents exist and are slated to be uploaded this year, which will place our rating back to a 4 star rating. What is great is we have 25 out of 25 points for our program expenses,which are regularly evaluated and audited. In addition, we have an audit and oversight committee, and score 20 out of 20 for material diversion of assets and have an independent board of directors. Lastly, we have perfect scores for our fundraising efficiency and working capital.

The Internet Archive has not received a Cy Pres award, and that is why we are deeply grateful and excited at being chosen as a recipient. As a high-performing nonprofit that is indeed making a difference in internet privacy and accessibility, we are ready to improve and educate our stakeholders, partners and the millions of our public users that rely on the Internet Archive to promote internet privacy and safety education..

Exhibit N

The Markup

Organization Information

1. Name of organization: The Markup

2. Discuss the founding and history of the organization.

The Markup challenges technology to serve the public good. Internet privacy has been a significant focus because it is a public good that is not always well-represented by market forces. Our journalism combines data-driven investigations and our technological expertise to reveal the hidden impact of technology across our society and its systems.

The Markup began publishing in February 2020 with tremendous results. We've been cited 21 times by Congressional leaders, helping legislators and government agencies like the Federal Trade Commission and The Department of Health and Human Services push forward in their work to protect consumers and their data. Blacklight, our real-time privacy inspector, has been used 11.7 million times in our short tenure. Our work has resulted in 9.7 million data breach notifications and 35 class action lawsuits to hold leaky companies to account. Multiple industry leaders have told us that our work has inspired much more rigorous inspection of the internal use of tracking technologies.

We are honored to have been recognized for our commitment to user privacy by The Electronic Privacy Information Center (EPIC), which presented The Markup the Champion of Freedom Award in 2021. The annual award recognizes individuals and organizations that have helped safeguard the right of privacy, promote open government, and protect democratic values with courage and integrity. Our number one most-viewed story in 2022, Facebook is Receiving Sensitive Medical Information from Hospital Websites, was awarded Digiday's Best Story of the year.

Not only *should* those that design and deploy tech solutions do better from a privacy and security standpoint, our technical expertise guides our work because we know that they *can* do better. We know that because we operate our organization according to our Privacy Promise: "The Markup will collect as little personal information about you as possible when you visit our site, and we will never monetize this data." There are trade-offs to working this way, since audience-building often depends on tools like cookies that we don't employ and vendors that

align with our values of transparency and privacy can be difficult to find, but we find it as important to live by those values as it is to report based on them.

3. Describe the organization's current goals.

In 2023, The Markup's goals are:

- Create work that is actionable and drives real-world impact, launching major evidence- and people-driven investigations that hold technologies and their decision-makers to account
- Tell investigative, journalistic stories, in a distinct way that instills the feeling of agency in our readers, and not helplessness
- Create and improve our own tools and resources that give readers superpowers, such as adding more features to people's ability to scan any website for how it tracks them through our Blacklight tool, or creating tools like our twitter throttling detector, that lets readers check what websites twitter is throttling *right now*
- Grow the editorial team to 19, including 5 editors, 8 reporters, and 5 journalism engineers and data reporters
- Continue to build sustainable fundraising strategy, deepen relationships with existing and potential donors, and explore other potential revenue streams

4. Provide a brief description of the organization's current programs.

Our work is organized into investigations, tools, and blueprints. Examples of work that has previously fallen into these categories are listed below, and are illustrative of what may continue to be generated during the grant period.

- Investigations: Our investigations use data-driven journalism and our own engineering expertise to reveal the hidden impacts of how tech is used. Investigations have found that telehealth providers were leaking sensitive customer data to the world's largest advertising platforms, that tax filing companies were shuttling personal financial data to Facebook, and that political campaigns are using your movements to target you with ads (part of a massive market for customer location data that impacts nearly everyone).

The Markup

- Tools: Our tools hold institutions accountable for the way they use technology, pulling back the curtain so readers can see for themselves how technology affects them. This includes Blacklight, a real-time website privacy inspector (used over 11 million times, and recently updated with new features) and a research partnership that allowed us to hunt the Meta Pixel and what information it shared with Facebook across the internet. These tools and partnerships led to investigations on how nonprofit websites are riddled with ad trackers and how organizations from hospitals to the Department of Education have sent users' information to Facebook. Blacklight in particular has proven a powerful tool for reporters, researchers, and advocates.

- Blueprints: We show our work so communities, journalists, and researchers can build on our reporting—crucial for our commitment to capacity building. This includes:

    - Methodologies that set the standard on how to measure algorithmic harm
    - Citizen Science initiatives to explain how to measure harm from the front lines
    - Transparent datasets that encourage skeptics to test our work for themselves
    - Privacy-forward software to make it easy for others to do the right thing
    - Products that help researchers, policymakers, and technologists measure harms

5. Has your organization ever received a prior cy pres award?

No

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?**

Candid.org, Platinum Transparency

Nabiha Syed
CEO

P.O. Box 1103
New York, NY 10159

THEMARKUP.ORG

The Markup

Grant Proposal

7. Identify the organization's principal investigator or project director.

- **Nabiha Syed** is the CEO of The Markup. Under her leadership, The Markup's unique approach has been referenced by Congress 21 times, inspired dozens of class action lawsuits, won a national Murrow Award and a Loeb Award, and been recognized as "Most Innovative" by FastCompany in 2022.

  Before launching The Markup in 2020, Nabiha spent a decade as an acclaimed media lawyer focused on the intersection of frontier technology and newsgathering, including advising on publication issues with the Snowden revelations and the Steele Dossier, access litigation around police disciplinary records, as well as privacy and free speech issues globally. Described by Forbes as "one of the best emerging free speech lawyers", she has briefed two presidents on free speech in the digital age, delivered the Salant Lecture at Harvard, headlined SXSW to discuss data privacy after Roe v. Wade, and was awarded the NAACP/Archewell Digital Civil Rights award in 2023 for her work.

  A California native and daughter of Pakistani immigrants, Nabiha holds a J.D. from Yale Law School, where she co-founded one of the nation's first media law clinics, a B.A. from Johns Hopkins University, and a law degree from Oxford, which she attended as a Marshall Scholar. She serves on the boards of the New York Civil Liberties Union, The New Press, and the Scott Trust, among others.

- **Sisi Wei** is the editor-in-chief at The Markup. Before joining The Markup, she was co-executive director of OpenNews, where she envisioned and executed transformative initiatives for journalism. As part of her work, Sisi founded the DEI Coalition, a journalism community dedicated to sharing knowledge and taking concrete action in service of a more anti-racist, equitable, and just journalism industry.

  She was assistant managing editor at ProPublica from 2018 to 2020, where she oversaw three editorial teams focused on news apps, interactive storytelling, and visual investigations. She also managed large, interdisciplinary investigations across the newsroom, one of which won the Pulitzer Prize for National Reporting in 2020. Sisi

worked at ProPublica for seven years, investigating abuses of power and betrayals of the public trust across a range of topics, including health care, higher education, government, and immigration.

In 2021, IWFM awarded Sisi the Gwen Ifill Award, which recognizes an outstanding woman journalist of color whose work carries forward Gwen's legacy, especially by serving as a role model and mentor for young journalists. In 2019, Sisi and her fellow Journalists of Color Slack admin team won the ONA Community Award, which recognizes a person or small team in online journalism that has made outsized contributions to creating tools or work environments that allow digital journalists to do their best work. Sisi also serves on the board of News Revenue Hub.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

At The Markup, we use our expertise in tech to investigate tech and internet privacy—whether that's by digging into code to challenge a company's claims or by building new tools that restore people's agency over the technology in their lives—especially in a time of rapid, unchecked innovation, with money pouring into the development of high-stakes technologies to an unprecedented degree. As we craft a vision for justice and equity in an algorithmically-mediated world, one thing is certain: everyone deserves high-quality, independent information to guide their choices. And when it comes to privacy on the internet, the news can feel bleak.

To date, our work has revealed how your family safety app, your grocery store, and your car are all collecting massive amounts of personal data as a consequence of your use. Some of our most impactful work arises from our Pixel Hunt series, the first large-scale crowdsourced study of the Meta Pixel, a snippet of computer code embedded in a website and used for tracking you around the web. It's not just about serving you ads for shoes you might like; even websites processing highly sensitive information can have the Pixel installed.

But beyond reporting on disturbing breaches of privacy, we go one step further and equip our readers with the tools they need right now to address our findings. We published a resource specifically for employees who want to audit their own company's pixel usage, we help readers comb through the fine print of privacy policies and we give concrete steps to protect your

privacy. There have been tremendous legal consequences for the companies we've reported about. But we have merely scratched the surface.

Now, the frenzy to invest in and deploy both industry-guiding and consumer-facing technologies like ChatGPT leaves dangerously ample room for unforeseen privacy consequences, similar to those we've been uncovering, but potentially even more sinister. We need our work to not only continue, but to evolve and keep up alongside those developing new technologies with seemingly unlimited resources.

We will remember 2023 as the year where frontier technology burst into our collective consciousness, and The Markup is primed to help the public—laypeople, policymakers, and industry—make sense of the rapid change.

To do so, we will accomplish the following:

- Goals and objectives:
    - Continue to maintain and iterate upon successful tools like Blacklight and partnerships like Pixel Hunt for further return on investment
    - Empower data journalists and journalism engineers to create new methods, tools, or partnerships for investigating privacy breaches and empowering the public
    - Publish original investigations that reveal new information about privacy in the context of the development or deployment of technologies, especially emerging ones, with actionable insights
    - Track impact in three categories: legislative, industry, and community

- Activities:
    - Data-driven investigative journalism
    - Development and maintenance of tools for gathering investigative data in a non-exploitative way
    - Creation of resources: Publicly available datasets, methodologies, story recipes, and processes for the continuation and replication of our work

- Timeline: Ongoing

The Markup

9. Explain why the organization is approaching the issue and/or opportunity in this way.

Journalism is a node in a social change ecosystem—but not the one you might think it is.

You might think of journalism as a literal amplifier—a machine that you plug other peoples' work into that shouts it as loudly and as far as possible.

But at The Markup, we enter the ecosystem one important step before that, using our engineering and investigative skills to reveal and quantify harms, handing changemakers the knowledge they need to stop harmful systems in their tracks today.

There are things that we may intuitively know, feel, or assume to be true—"My phone is listening to me and serving me ads"—but nothing changes until local leaders that get quality, independent, bulletproofed information to back that claim from an organization that has a birds-eye view of the tech landscape and how it trickles down to the daily citizen experience.

There is simply no other institution that produces knowledge on a timeline that changes the harm that is happening *right now*. Supporting journalism is supporting local organizations with information that opens up how they understand their own work and that they use, literally, to implement more change.

Untangling society's complex, systemic problems is like putting together an enormous puzzle without having a full picture of what pieces are missing. The Markup has a track record of finding the right puzzle piece at the right time in a variety of industries. Our theory of change sits at the intersection of rigorous data analysis and powerful storytelling, in a way that both measures what needs to be fixed and connects with the subjects of those harms in a deeply personal way.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

In 2023, The Markup had a $6 million annual budget, with over 75% of our funding going toward staff compensation.

Nabiha Syed
CEO

P.O. Box 1103
New York, NY 10159

THEMARKUP.ORG

The Markup

Past annual budgets:

2022: $6 million
2021: $5.5 million
2020: $4.5 million

We respectfully request an award of $6 million in order to accomplish our goals and objectives around internet privacy, to be apportioned as follows:

- **2024: $3 million (50% overall projected operating budget)**
- **2025: $3 million (50% overall projected operating budget)**

The resources from this award will specifically be used to investigate, report on, and create tools to address issues of internet privacy and security, and what the public can do to protect itself.

11. Will the money be used to continue an existing project or create a new project?

The money will be used to continue our work (investigations, tools, and resources) on internet privacy, building on existing work and supporting newly pitched stories and projects as well.

12. What target population will your organization's project benefit?

Our work is for a national audience and intends to provide information and surface knowledge in three categories:

1. Laws and regulations: Technology is used to make crucial life decisions and is unavoidable for work, education, and most core needs. When our bulletproofed investigations reveal exploitative or dangerous tracking technology, lawmakers have the data they need to push for lasting, systemic change.

2. Organizational leadership: Innovations that help companies optimize their own work may be harmful or exploitative in unintended ways. But we've found that when leaders know better, they do better (like removing tracking pixels that leak customer data).

Nabiha Syed
CEO

P.O. Box 1103
New York, NY 10159

THEMARKUP.ORG

The Markup

3. People and communities: We know that communities know best how to advocate for themselves. Our work raises awareness and agency, arming people with the practical, actionable information they need to make change, such as teaching a parent how to protect their child's location data in an app.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

Each of our three impact areas sees distinctly important outcomes from The Markup's work. We measure success through the work's concrete impacts. Past examples in the privacy space include the following:

1. Impact in Government
    a. **We've been referenced by Congress 21 times across multiple investigations**, like this summer when our investigation into tax prep companies directly fueled a bombshell Congressional report by Elizabeth Warren. In the report citing The Markup, Warren said "Big Tax Prep companies have recklessly shared personal and financial data of millions of taxpayers with Big Tech for years. Regulators need to fully investigate and prosecute those who violated the law."
    b. Citing our Meta Pixel story on healthcare data breaches, the Department of Health and Human Services confirmed that "tracking technologies" on patient portals are covered by HIPAA privacy rules.

Nabiha Syed
CEO

P.O. Box 1103
New York, NY 10159

THEMARKUP.ORG

The Markup

2. Industry Action:
    a. 9.7M data breach notifications have been issued in response to issues uncovered by our work.
    b. 35 data breach class action lawsuits (and counting!) have been filed (including one from law firm Wisner Baum just last month, the first RICO class action case naming tax prep firm H&R Block, Meta, and Google in a conspiracy to defraud consumers).
    c. At least 19 companies made real changes—like removing the Meta Pixel from their website—soon after being contacted by The Markup. These companies include major hospital network patient portals.
    d. Multiple industry insiders have told The Markup that internal industry trainings inside the healthcare industry now include instructions on how to skip or limit the use of the Meta Pixel.

3. Community Impact:
    a. Our digital trainings, like “Who’s Got My Data? How students can protect their personal information at school” (feat. Todd Feathers), empowered people to take on big tech issues through both their personal choices and community advocacy.
    b. Jon Keegan and Jesse Woo’s reporting shares exactly how you can quickly get to the important truth inside any privacy policy.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Yes. We publish about four articles per week for our national audience, from investigations to explainers to newsletters, all of which will result from support provided by this award. Our editorial staff is often asked to present at professional conferences, run workshops, or teach classes for students ranging from high school to graduate school.

Nabiha Syed
CEO

P.O. Box 1103
New York, NY 10159

THEMARKUP.ORG

Exhibit O

Internet Policy Research Initiative
Massachusetts Institute of Technology

Proposal: MIT Privacy Engineering Action Lab

October 5, 2023

Organization Information

1. Name of Organization

MIT Internet Policy Research Initiative (IPRI)

2. Discuss the founding and history of the organization.

Founding

The MIT Internet Policy Research Initiative (IPRI) is an MIT-wide initiative pioneering a new style of cross-disciplinary research and policy dialogue that brings together scholars from across campus. IPRI was created in 2015 with a founding grant of $15M from the Hewlett Foundation and early support from the Ford Foundation.

Since 2015, IPRI has established a track record of technology policy leadership and government engagement on issues such as encryption and surveillance, AI governance, cybersecurity, and privacy. IPRI's work on these issues has been strengthened by our trusted working relationships with technology policy leaders in the United States (both at a national and state level), the United Kingdom, Australia, Germany, and India, as well as with international organizations, including the OECD and the World Bank.

Daniel J. Weitzner, holder of the 3Com Founders Senior Scientist chair at at the MIT Computer Science and Artificial Intelligence Lab (CSAIL), founded IPRI in 2015 as a response to the critical need for technology-informed policy making in the areas of privacy, security, networks and the Internet economy. The group plays an important bilingual role of informing policy making with technical expertise, and helping engineers build secure and privacy protecting products that are informed by policy.

IPRI is in a unique position to advance individual privacy rights through computer science research that will create new privacy-preserving technologies, and public policy research to explore technically-grounded advances in privacy policy and law. IPRI's senior leadership has strong consumer and Internet civil liberty advocacy backgrounds. Daniel Weitzner was the first staff member in Washington DC for the Electronic Frontier Foundation and founder of the Center for Democracy and Technology. He was also a senior policymaker (White House Deputy CTO for Internet Policy). While at the White House, Weitzner was responsible for developing

the Consumer Privacy Bill of RIghts in 2012. Dr. Taylor Reynolds, IPRI's Research Director, was the senior economist at the OECD responsible for the Internet economy, and his research on broadband pricing led to multimillion dollar fines against incumbent telecommunication firms engaged in deceptive advertising.

Of particular relevance, Daniel Weitzner has a long history of successful Internet civil liberties advocacy. His work led directly to amendments to the Electronic Communications Privacy Act in 1994 that offered groundbreaking protections for web browsing logs, email records, and other transactional data. (18 USC 2703(d)) Under Weitzner's leadership, the interests of the class in better privacy protection will be materially advanced.

Our research streams

IPRI's primary research efforts have historically covered six core research areas: cybersecurity, privacy, networks, AI policy, the Internet experience, and AppInventor. The IPRI team is led by a core group of 16 principal investigators. Over 20 students are involved in IPRI research at any given time. Our structure as an cross-campus entity that brings together technical experts from across fields with policymakers to tackle key challenges has produced significant societal impacts in health, voting, and privacy among others. Several of these are highlighted below:

Private Automated Contact Tracing (PACT)

- **Technology/Policy Problem:** There was a need for contact tracing applications during COVID-19 that were secure and preserved privacy.

- **IPRI Solution:** IPRI put together a consortium called PACT (pact.mit.edu) that brought together technologists and public health officials to automate parts of the exposure detection function while maintaining user privacy and ensuring equitable deployment.

- **Impact:** PACT-designed exposure notification technology, including state-of-the-art security and privacy architecture, is now included in billions of Android and iPhone products all around the world.

Voting Apps

- **Technology/Policy Problem:** There is an ever-increasing interest in online and mobile voting, but the cybersecurity profile of such services raise numerous questions.

- **IPRI Solution:** IPRI researchers published a technical paper demonstrating deep security vulnerabilities in a particular mobile voting app (Voatz), the first thorough reverse engineering analysis of a live mobile voting system to demonstrate many of the security risks long warned-of by the computer security community.

- **Impact:** Several states and other voting jurisdictions that either were using Voatz or considered doing so reversed their decisions after IPRI researchers shared their findings with the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA), Voatz themselves, and later major news publications like the New York Times.

Encryption and surveillance

- **Technology/Policy Problem:** Law enforcement agencies around the world propose redesigning Internet and smartphone infrastructure to enable government access to encrypted information. But is this secure?

- **IPRI Solution:** The Keys Under Doormats Report, produced by the world's leading cryptographers and cyber security experts showed that enabling "backdoor access" posed security risks.

- **Impact:** The report findings changed the direction of U.S. policymaking, and encouraged Australian and UK parliaments to update their legislation to address systemic risk identified by the IPRI report. IPRI remains engaged in research and dialogue with government agencies, companies and civil society to identify constructive approaches with reasonable risk levels.

Lack of cybersecurity data for decision and policy making

- **Technology/Policy Problem:** Little data exists about the most efficient means of addressing cybersecurity risk, so investment decisions are suboptimal, cyber insurance is inefficiently priced, and policymakers lack the information necessary to make sound public policy. This lack of price/risk data is because firms don't share data on cyberattacks, so we learn nothing about the attacks or the effectiveness of cyber defenses.

- **IPRI Solution:** A team at IPRI developed the SCRAM (Secure Cyber Risk Aggregation and Measurement) benchmarking platform that uses secure computation techniques (multi-party computation) to securely and privately aggregate sensitive data without requiring disclosure of the underlying inputs.

- **Impact:** The IPRI team produces new cybersecurity benchmarks, metrics, and models that are used to forecast cyber risk for various sectors of the economy. These inputs are then used to create policy recommendations and guidance for municipalities that operate critical infrastructure and federal policy making bodies.

AppInventor

- **Technology/Policy Problem:** Mobile phones have become an important interface for sharing and consuming information, but the process historically for creating apps for mobile platforms was difficult and expensive, particularly for socially beneficial applications with little to no available funding.

- **IPRI Solution:** The AppInventor team built an intuitive, visual programming environment that allows everyone, even children, to build fully functional apps for smartphones and tablets. Those new to MIT App Inventor can have a simple first app up and running in less than 30 minutes.

- **Impact:** AppIventor has over 400,000 unique monthly active users who come from 195 countries who have created almost 22 million apps. MIT App Inventor is changing the way the world creates apps and the way that kids learn about computing.

3. Describe the organization's current goals.

The Internet Policy Research Initiative's (IPRI's) mission is to lead the development of policy-aware, technically grounded research that enables policymakers and engineers to increase the trustworthiness of interconnected digital systems like the Internet and related technologies.

To achieve this mission, IPRI produces fundamental, cross-disciplinary technology and policy research (publishing 35 research papers in 2022); engages with global policymakers, industrial partners, and civil society organizations; and is building a network of students educated in the field of Internet policy.

4. Provide a brief description of the organization's current programs.

MIT is one of the top universities in the world across a number of disciplines, including engineering, computer science, and economics. MIT has 11,376 students and 13,000 employees. Recently the Institute announced the creation of the Schwarzman College of Computing which represents a new paradigm for computer science research and education that recognizes the importance of addressing the social, ethical and policy impact of computing on society. Currently, IPRI has six main research streams.

<u>IPRI by the numbers in 2023</u>

- PIs: 16
- Students doing research: 41
    - 7 PhD
    - 15 masters
    - 21 undergraduate

- Publications: Roughly 35 per year

Current research streams

1. ***Privacy,*** covering topics such as designing new databases and systems embedded with privacy protection and user control, evaluating the international privacy policy landscape and studying privacy incentives, data protection policy, web surveillance, human-computer interaction in the context of privacy, the implications of silently listening, and overarching insight into the global privacy research area.
2. ***Cybersecurity,*** covering topics like encryption policy, accountability, cryptography, data sharing, securing core economic and social infrastructure, and measuring cyber risk.
3. ***AI Policy,*** covering topics like the role of AI in financial decision-making, increasing access to new training data sets with policy, working with stakeholders on AI principles, and shaping global Internet policymaking via policymaker engagement and informing the public debate.
4. ***Networks,*** covering topics like Internet architecture, Internet security, Internet economics, Internet policy, and network management.
5. ***Internet Experience,*** covering topics decentralized privacy preserving platforms for clinical research, the trustworthiness of autonomous systems, the relationship between privacy and machine learning, complex machine and model explanations, securely aggregating distributed data, and developing smart contracts for data sharing.
6. ***App Inventor,*** involving the creation of a tool to enable anyone, especially youth, to develop mobile apps that better their communities.

In addition to the high-impact research activities described above, other relevant IPRI contributions include:

- We developed “Privacy Bridges” with European partner universities to help create a framework for data protection and usage between the US and the EU. Our report was presented at the International Conference of Privacy and Data Protection Commissioners.
- Our team contributed technical and policy guidance to the OECD as they developed the OECD’s AI Policy Principles that were adopted by 36 countries. IPRI sent three experts to participate in the OECD’s Expert Group on AI. IPRI also hosted the OECD’s AI Expert Group Meeting in January 2019.
- Daniel Weitzner was selected to be a member of the OECD’s Expert Group to revise the OECD’s long-standing privacy guidelines.
- Our researchers and leadership frequently prepare submissions to governments related to encryption policy. Our researchers have testified in front of the US Congress and were invited to testify before the Australian Parliament on these issues.

5. **Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.**

IPRI has received a cy pres award in the matter of In re Google Inc. Street View Electronic Communications Litigation, No. 10-md-2184, Northern District of California) in the amount of $1,006,582.

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity?**

Yes. MIT has a Charity Navigator rating of 96%.
https://www.charitynavigator.org/index.cfm?bay=search.profile&ein=042103594

7. **Identify Principal Investigator/Project Director**

Daniel J. Weitzner is the MIT IPRI Founding Director and holds the 3Com Founders Senior Research Scientist chair at MIT Computer Science and Artificial Intelligence Laboratory.

8. **Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.**

Introduction and Motivation:

The MIT Internet Policy Research Initiative proposes to launch a new MIT Privacy Engineering Action Lab (PEAL). PEAL will materially advance the interests of the class in In re Google Location History Litigation, No. 5:18-cv-05062-EJD (N.D. Cal.), helping to assure than members of the class, and those similarly situated in the future are far less likely to be victims of privacy harm arising from deceptive collection of personal data, the inability of users to control how their data is used, and the general lack of technical tools and design patterns that encourage respectful privacy practices.

As serious as are the harms in this case, they are only the tip of the iceberg. Internet users are surrounded by systems with equally deceptive, uncontrolled and virtually-invisible flows of personal data in the fields of health, finance, transportation, employment and other sensitive activities of our daily lives. What's more, these privacy risks are growing over time: personal data flows are becoming more complex, with many organizations moving to business models in which sensitive personal data is passed rapidly across organizational boundaries and subject to increasingly penetrating analysis through a growing variety of statistical and AI machine learning techniques. As these privacy risks grow, users' ability to exercise control over their data, and regulators' ability to detect wrongdoing are all declining, putting users at even greater risk.

We propose a coordinated package of computer science research, user education and professional development materials that will provide new technical accountability measures, quantitatively rigorous user studies that identify both new dark patterns and recommended affirmative design practices, and new educational approaches for computer science undergraduates as well as professional development education for a developing new job category, Privacy Engineers, who will contribute to much of the technical privacy environment for users in the future.

The project is divided into three components, each running concurrently for three years.

1) **Traceable Accountable Privacy Protocol (TAPP)**: Robust technical infrastructure that processes personal information at web scale in a demonstrably reliable manner. This part of the project will engage computer science faculty and students to develop a new web protocol that will facilitate sharing personal data in a fully-accountable manner, so that each user is able to attach clear consent and usage conditions for their data, know who has their data, what they are doing with it, and easily cause it to be deleted or corrected. We will publish a working description of this new protocol and make available open source libraries to enable its widespread implementation and adoption. Members of the IPRI team have extensive experience moving technical designs from the lab to the web, including PI Weitzner's leadership role at the World Wide Web Consortium (the body that sets technical standards for the Web) as well as Weitzner and Liccardi's experience developing the COVID Exposure Notification Protocol (PACT) ultimately implemented on billions of Android and Apple iOS devices during the pandemic.
2) **Learning From User's Behavior 'in-the-wild'**: We have endless privacy surveys, all of which establish that users want more control over their data and distrust many who have it today. By studying how users actually interact with different services, we will identify dark patterns in new styles of user interfaces such as voice interfaces and AI-powered chat bots. We can also develop positive user interface design patterns that encourage respectful handling of personal data. This component of the project will produce authoritative behavioral science studies (using Human Computer Interaction techniques) to identify with precision design features that are deceptive, and use these scientific insights to inform design recommendations which will be made widely available to the developer community.
3) **Privacy Engineering education**: Enterprises large and small, public and private, all face the challenge of how to handle personal data in a respectful and accountable manner. Ultimately, the technical side of this challenge will be met by a new category of engineers and software developers – the Privacy Engineer. We propose to create educational materials to guide the development of this new field, both for use in undergraduate computer science education and for those already operating in professional settings. Of course, the decision and incentive to be responsible about privacy begins with the legal system and a commitment to ethical business practices.

Once firms make this commitment, they will turn to their privacy engineers to do that work, so we want to contribute to their being ready for the challenge. MIT IPRI has been contributing to this field and studying its needs[1], so are well-positioned to contribute to its growth.

Individual Project Descriptions

Project 1: Traceable Accountable Privacy Protocol (TAPP): A new web protocol for sharing personal data in a traceable, accountable fashion

As companies collect and share vast amounts of consumer data, trust in their data stewardship practices is rapidly declining.[2] This trend is especially worrying given that in many sectors there are moves to share more, not less, personal data, and that data will increasingly flow across organizational boundaries. This will only increase consumer confusion and decrease individuals' practical ability to control their data. What's more, key sectors where sharing is increasing – healthcare, finance, employment – pose a risk for harm as great or greater than what we have seen in social media and online advertising. While cross-enterprise data sharing can bring consumer benefits and convenience, it has also led to many high-profile consumer data protection violations, exemplified recently by the Facebook-Cambridge Analytica scandal. This was among the largest known bulk misuse of personal data and it happened precisely because Facebook was careless about allowing data to flow off its platform without any controls. What's more, that fact that Facebook was under an FTC consent decree with bi-annual audit provisions raises doubts about how well our enforcement processes are working[3]. As we move toward a world in which data sharing is only likely to increase, we need better technical tools to ensure user control and accountability, along with better legal protection and enforcement. At MIT we have limited ability to influence the state of privacy law and enforcement, but do have the ability to design and deploy new privacy protection technology.

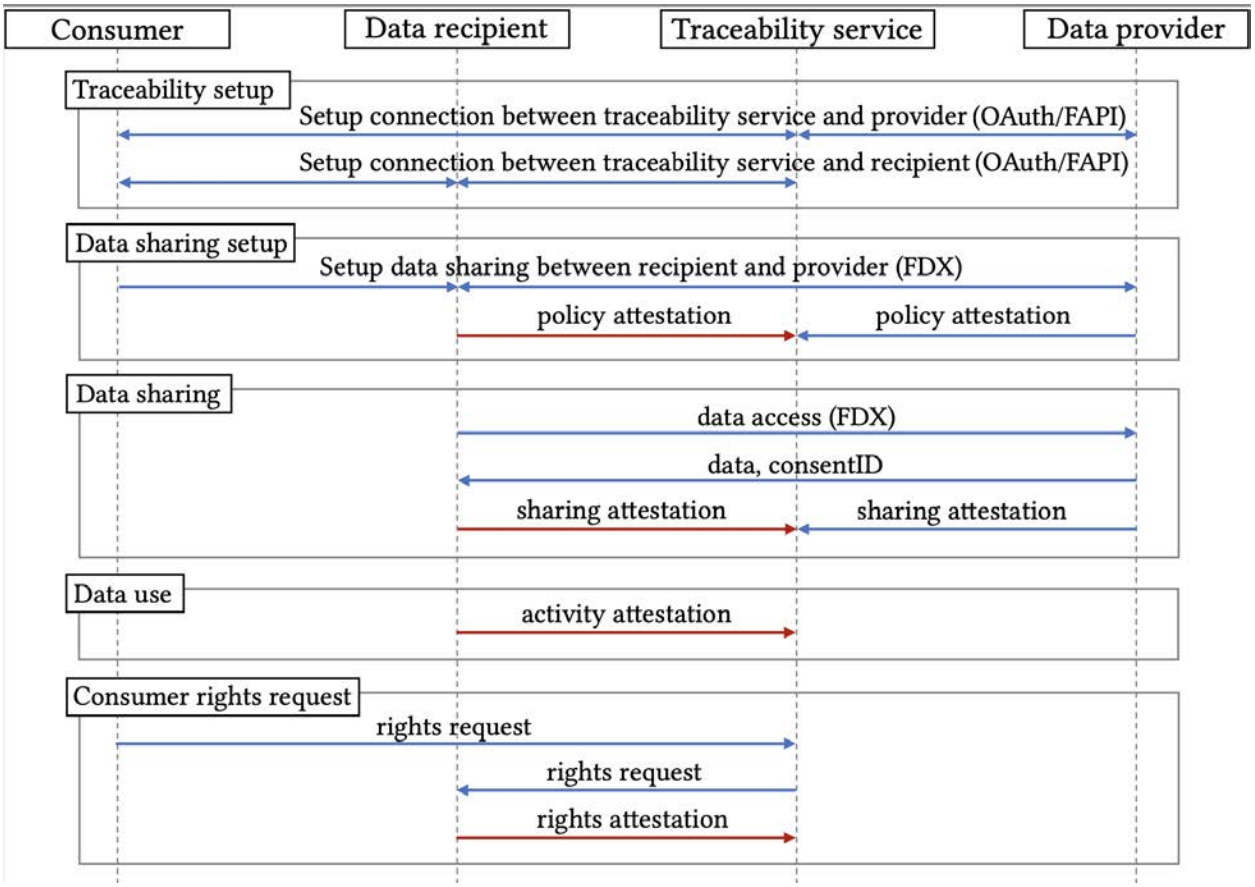
In order to regain consumer trust and provide meaningful control, it is essential for organizations to:

- obtain explicit, informed, and granular consent when processing personal data, which will give consumers greater clarity over the type of information they share and how it is used;
- offer traceability in their data use and sharing practices, which will give users control, as they know who has access to their data and how it is actually being used;

[1] Gulati, Liccardi, Weitzner, "Privacy Law in Practice: Exploring Challenges to Modern Privacy Compliance," Privacy Law Scholars Conference, June 2023.
[2] Kimberly Bella, Christophe Carugati, Cathy Mulligan, and Marta Piekarska-Geater. Data for common purpose: Leveraging consent to build trust. https://www3.weforum.org/docs/WEF_Data_for_Common_Purpose_Leveraging_Consent_to_Build_Trust_2021.pdf, 2021
[3] Weitzner, How Cambridge Analytica, Facebook and Other Privacy Abuses Could Have Been Prevented, Lawfare, April 4, 2018.

- provide mechanisms for accountability in case of any violations, which will give consumers confidence that those holding their data will be held accountable for any misuse and that regulators can identify abuse of personal data.

To give consumers a more complete understanding of how companies handle their data, we will design and prototype a suite of data governance protocols to facilitate consent, traceability, accountability, and portability across enterprise boundaries. This will unify how consumers manage consent and data lifecycles with all of their service providers, while also standardizing how different providers report on data use and sharing events. Our design goals are focused on simplicity (they should rely on established standards where possible), security (they should adopt best practices for secure data storage and transmission), and scalability (they should allow companies to scale out as their userbases and databases grow).



The figure above is our initial design sketch of this technical protocol. The key idea of this protocol is that each time data is shared with a third party, a clear statement of consumer consent should follow with it, and every time a third party uses that personal data, a record of that use should be provided to the consumer or her agent, with the ability for the consumer, her agent, or even a regulator, to easily (with machine assistance) assess whether the uses are permitted. The same mechanism should give consumers the ability to know who has their data

at any moment, as well as a mechanism to have the data deleted or corrected upon the instruction of the consumer.

Opportunity: There is a unique opportunity to change the terms on which personal data is handled because a number of business sectors are making major technology investments in new data sharing technologies. Now is the time to add explicit privacy protection and user control features while the new services are still in the design phase. For example, many banks are investing in new open banking services which will entail larger-scale and more complex flows of personal financial data. Regulators around the world are also considering modernizing personal data rules. It is essential to show that user control and accountability can be added along with these new services in a manner that enhances user privacy rights, improves the possibility of meaningful privacy enforcement, and still enables consumers to have the benefit of these new services. Our experience in design and deploying web standards and new privacy protocols in other settings positions IPRI well to have a positive impact on the privacy technology landscape.

Funding: Over the course of a three year project, we propose to fund 3 graduate students, 2 undergraduates, one postdoctoral researcher, a small part of one senior faculty member in computer science, all supervised by PI Daniel Weitzner. The cost of this component of the project is $899,000 over a three year period.

Target population: The target population for this component of the project are end users of consumer-facing services on the web such as banking, healthcare and other complex data analytic platforms. The ultimate impact of this project, if successful, would be to ensure that all personal data flowing through these new services is under the control of individual users and handled in traceable, accountable fashion.

Project 2: Learning From Users' Behavior In-the-Wild: User Experience studies

While we know users want control and we know that trust emerges from better control and more transparency, the details of what kind of control and how much information to offer users is not always well understood. The best path to designs that have these properties entails observing (under Institutional Review Board ethics control) users as they use real services to understand their behaviors and motivations. Using Dr. Ilaria Liccardi's experience sampling studies in the wild over a period of time, we will develop clear design patterns that meet user privacy expectations and build trust. These studies will begin with design sketches presented to focus groups, develop into pilot projects that observe users interacting with real world services, and ultimately mature into larger-scale deployments that engage with users as they are using new privacy features in live systems.

Looking forward, we must also extend our understanding of privacy dark patterns and respectful interface designs into other user interaction methods. Voice-activated interfaces and AI-powered chat bots are the new mode through which many users will interact with next-generation digital services. Given the intrusive data collection capability of these interfaces, we must understand the privacy risks and how to mitigate them.

The widespread adoption of smart assistants, both within the home and on smartphones, has made audio open to possible intrusion by technology providers. We propose to investigate the privacy implications of audio captured around voice activate assistants on smartphones and on stand alone devices. We aim to understand the types of audio that can be captured – across different locations – and to explore whether people understand the types of information that they are giving away when using these devices. We aim to compare people sharing preferences before and after exposing the implications of using these devices to people's privacy. In our previous work we found that regulations are lacking and in need to be amended to include possible privacy violations of these devices.[4] In particular, given the ubiquity of these devices, regulations should be considered, especially because our previous research[5] showed that these devices placed in the home capture less intrusive and privacy sensitive information compared to portable devices such as apps on smartphones and/or car applications.

This work can also be extended and provide insights into the privacy implications of AI-powered chatbots given their increasing widespreads use. Similarly to audio based commands, the privacy implications of using AI-powered chatbot applications are often opaque, unclear and misunderstood by users. We aim to investigate users' usage over time after possible implications are highlighted and communicated clearly. We believe that users' behavior and usage of this tool might change when possible intrusions are presented.

The result of this project can highlight people's actual preferences when it comes to their personal data. It can guide companies to create, adapt or re-evaluate how to use the information captured. It can help regulators create and amend regulations to safeguard people's data around these devices.

From this project we will produce several peer-reviewed papers reporting on the results of our user studies. These papers will both identify new styles of dark patterns and also recommend positive best practices for respectful privacy interface and interaction design. This rigorous scientific evidence will also help guide privacy enforcement authorities and others in the legal system to hold irresponsible data controllers to account.

---

[4] Lindsey Barrett & Ilaria Liccardi, Accidental Wiretaps: The Implications of False Positives by Always-Listening Devices for Privacy Law & Policy, 74 Okla. L. Rev. 79 (2022)

[5] Ilaria Liccardi & Jose Juan Dominguez Veiga, Wiretapping Your Friends: Privacy Implications of Voice Activated Assistants (on file with authors).

Funding: Over the course of a three year project, we propose to fund 2 graduate students, 3 undergraduates, one postdoctoral researcher, a small part of one senior faculty member in computer science, all supervised by Dr. Ilaria Liccardi and PI Daniel Weitzner. We will also have to fund the cost of working with a large number of users as study subjects. Best practice is to compensate those who are willing to participate in these long-run user studies The cost of this component of the project is $937,000 over a three year period.

Target population: The target population for this component of the project is end users of consumer-facing services on the web, especially those that use new voice-activated and AI-backed user interfaces. We also aim to influence the designers of these services and provide guidance to those who regulate them.

Project 3: Privacy Engineering Education

The long run privacy welfare of those who use digital services depends on the privacy norms that society sets and enforces through law and community demands. Designing and implementing the ever-evolving new digital services will depend on the engineering talents of software developers in general and on a new class of engineers known as Privacy Engineers. We propose a two-pronged educational approach that will enhance the privacy awareness of computer science students generally, and to help inform the development of the technical and professional standards of the new sub-field of Privacy Engineering.

Privacy awareness for computer science students: We will build on the novel, multi-disciplinary education approach of MIT's Internet Policy Research Initiative by extending two courses currently offered by IPRI faculty: 6.4590: Foundations of Internet Policy, and 6.S978: Privacy Legislation Law and Technology (offered jointly between MIT Electrical Engineering and Computer Science Department and Georgetown Law School (see New York TImes: Natasha Singer, Top Universities Join to Push 'Public Interest Technology', March 11, 2019; MIT Spectrum, Legal/Code-MIT engineering students team up with Georgetown lawyers-in-training on internet privacy legislation, Winter 2018). These courses teach 30+ computer science and engineering students each semester to develop the intellectual skills necessary to understand the complex public policy questions, including privacy, raised by computing in our society today. PEAL will add a hands-on laboratory component to each course giving students an in-depth experience of actually building and analyzing technical systems that address privacy harms.

By expanding these well-established courses, we will give our students added engineering experience needed to design and develop applications using personal data in a manner that does a better job of adhering to privacy law and best practice, thereby avoiding privacy harms suffered by the class of plaintiffs in this case. Engineering students learn good software development style through practice. We already have a well-developed curriculum for teaching our students how to understand broader issues of law and policy. By adding lab components to

the courses, we will give students concrete software development challenges that test their policy knowledge and give them the experience to make good design decisions in their careers. To help students understand and master the challenges of privacy-aware system design, we will build software platforms that simulate large-scale databases of personal information as environments within which students can experiment with different privacy designs. Developing lab teaching materials is a resource-intensive task, so support from this fund will be critical. IPRI will hire additional teaching assistants and a postdoctoral fellow to supervise the development of the new lab materials. Once these are developed, however, we will make them available freely to the rest of the academic community and professional software developers around the world.

Engagement with Privacy Engineering discipline: We know from studies of the development of the privacy engineering field that individuals who take on these jobs are passionate about building privacy-respectful systems. We will develop a series of monthly professional development seminars for early- and mid-career privacy engineers, providing them background on the latest research from our lab as well as our colleagues in universities around the world. We will also create a forum for peer interaction among privacy engineers. We know that there have been efforts to create such fora on a commercial basis that have failed. We believe MIT can be valued, trusted convenor for this new discipline.

Funding: Over the course of a three year project, we propose to fund 1 graduate teaching assistant to develop course materials, as well as supplementary faculty and lecturer time to create a new syllabus. We will also have expenses in developing and distributing the remote interactive course materials. The cost of this component of the project is $631,500 over a three year period.

Target population: The target population for this component of the project is computer science undergraduates at MIT and other universities around the world, as well as privacy engineers.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

[See individual project descriptions for opportunity assessment and discussion of organization approach]

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

We request a total of $2,467,500 to be expended over approximately a three year period. Each individual project described in paragraph 9 above shows specific funding amounts and spending categories. We summarize here:

PEAL Project Component	Funding (over 3 years)
1: Traceable Accountable Privacy Protocol (TAPP)	$899,000
2: Learning From Users' Behavior In-the-Wild	$937,000
3: Privacy Engineering Education	$631,500
Total	$2,467,500

11. Will the money be used to continue an existing project or create a new project?

PEAL will be a new activity that is part of the MIT Internet Policy Research Initiative (IPRI). IPRI is funded by the William and Flora Hewlett Foundation Cyber Program with a leadership grant of $15 Million.

12. What target population will your organization's project benefit?

[See individual project descriptions for target population of each component of the project.]

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

Overall, our most important measures of success are three-fold: First, we aim for widespread deployment of the new technical privacy protocols we are designing. If these protocols are used in a single large sector of the Internet such as financial services, healthcare or social media, we will consider our work to have a high level of impact. Even if this is not the case, we may see aspects of our protocol design in widely deployed software and services. That would also be a success. As an interim measure of impact, we will measure the number of developers who download the libraries we put out. Second, we will consider our work on user interface analysis and design to be successful if (a) our identification of new dark patterns are used in public policy development, government enforcement actions, or private litigation on behalf of individuals suffering privacy harm from deceptive practices. Finally, we will measure the impact of our

education programs based on the number of privacy engineers who use our educational materials. As soon as those materials are developed, we will provide usage statistics in our semi-annual reports.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Our research results will be published in leading peer-reviewed academic journals. Once research has been peer reviewed for quality, we will also seek to publish short-form versions of our work general audience publications such as Lawfare, the Harvard Business Review and op-ed pages so that our work receives broader impact. The technologies we develop will all be made available under open source licenses to encourage widespread usage.

* * * * *

Exhibit P

NATIONAL CYBERSECURITY ALLIANCE

Data Privacy *Cy Pres* Application

Organization Information:

1. **Name of Organization:** National Cyber Security Alliance dba National Cybersecurity Alliance

2. **Founding and History of National Cybersecurity Alliance:**
Founded in 2001, National Cybersecurity Alliance (NCA) is a nonprofit 501(c)3 organization. Our alliance stands for the safe and secure use of all technology. We encourage everyone to do their part to prevent digital wrongdoing of any kind. We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations. Only together can we realize a more secure, interconnected world.

   In 2004, NCA partnered with the Department of Homeland Security for the first Cyber Security Awareness Month to raise public knowledge of best cyber practices. Over the past twenty years, this campaign has grown from humble beginnings as a grassroots campaign, to one of the most high-profile cyber awareness initiatives in the country. The campaign is championed by over 6,000 individuals and organizations from all 50 states and 120+ countries - reaching an estimated 110,000,000 people. Last year, the campaign was mentioned in over 10,000 articles and broadcasts (3.5 billion global views).

   Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe and is officially led by NCSA in North America. NCA's goal is to help citizens understand that they have power to manage their data, and to help organizations understand why it is important to respect their users' data. NCA lead's the United States' Data Privacy Day efforts. NCA expanded this initiative to Data Privacy Week in 2021.

In 2010, NCA co-founded and launched STOP. THINK. CONNECT. along with the Anti Phishing Working Group and the US government, including the White House. STOP. THINK. CONNECT. Is a global online safety awareness campaign helping digital citizens stay safe online.

In 2016, NCA launched their CyberSecure My Business program, to help small and medium-sized businesses (SMBs) learn to be safer and more secure online. NCA is excited to launch an overhaul of this program that focuses on specific industry verticals in the coming year.

Since its founding, NCA has published a number of various research reports on security behaviors. In 2020, NCA partnered with CybSafe to craft **Oh Behave!** The Annual Cybersecurity Attitudes and Behaviors Report. This report gathers data on how attitude influences behavior, and consequently, cybersecurity risk.

In 2021, NCA brought on executive director Lisa Plaggemier, a trailblazer in cybersecurity and with her marketing prowess began several new initiatives to position NCA as a well-rounded education and program provider. Under her vision, NCA hosted its first *Convene* Conference, a Security Training and Awareness Conference held twice a year, and has launched *See Yourself in Cyber*, a HBCU Cybersecurity Career Program. NCA has also produced a comedy series called *Kubikle* - a memorable and funny training series with the goal of entertaining and educating audiences.

3. **Organizational Goals:**

Our alliance stands for the safe and secure use of all technology. We encourage everyone to do their part to prevent digital wrongdoing of any kind, with the ultimate goal of realizing a more secure, interconnected world.

Public awareness: We aim to raise public awareness about online privacy and educate citizens on how to manage their personal information and keep it secure. We aim to empower individuals and organizations to own their role in protecting their data by implementing stronger security practices.

Small Business security: With virtually all business data kept on internet-connected platforms, we aim to train small businesses on best practices and equip them with tools to evaluate their current security measures and identify areas of improvement.

Cybersecurity workforce development: As the security workforce shortage shows no sign of being resolved soon, businesses and organizations understand the importance of establishing a pipeline of young graduates to fill these critical jobs in the years ahead. Because many organizations also have initiatives to increase diversity in their workforce, we see a convergence of these two issues and have set a goal to help more minority graduates fill cybersecurity roles.

4. **Description of Organization's Current Programs:**

Cybersecurity Awareness Campaigns: These campaigns include the following:

- Cybersecurity Awareness Month (CAM) in October
- Data Privacy Week in January
- Nasdaq Cybersecurity Summit in October
- Staysafeonline.org resource library, webinars, educational articles and blog posts.

CAM, now in its 20th year, is recognized as one of the most high-profile cybersecurity education efforts in the country. NCA and CISA have worked together for nearly two decades to coordinate an accessible, easily adaptable messaging campaign for enterprises, governments, and consumers with the mission of ensuring that everyone has the information and tools needed to stay safe and secure online

NCA collaborates with stakeholders from government, industry, academia, and nonprofits to identify solutions to pressing cybersecurity concerns and encourage unified messaging.

NCA's messaging is incorporated into an updated suite of visually appealing and inspiring materials for public awareness campaigns. In coordination with public and private sector partners, NCA produces user-friendly collateral that corresponds to timely issues. Creating a steady cadence and variety of resources is the foundation needed to engage the community. Additionally, StaySafeOnline.org serves as a clearinghouse for materials provided by other partners that work with NCA on a continual basis. Collecting, organizing and disseminating these resources to various groups and stakeholders is an ongoing initiative.

NCA's events have become an integral part of the media engagement strategy. NCA has a strong track record of executing events with leading executives from both public and private sectors to discuss the hottest issues in cyber. This approach, coupled with NCA's trusted reputation, has attracted attendance and reporting by top-tier media including CNBC, Consumer Reports, Bloomberg, Forbes, Market Watch, CNN, and the New York

Post. NCA also mobilizes its online community to tweet, post and blog about these events. To engage diverse geographic areas, NCA will coordinate with trusted community partners to encourage hosting events.

***See Yourself in Cyber*: HBCU Career Program:** *See Yourself in Cyber* events help students increase their interest in cybersecurity career paths, improves their knowledge of what cyber career paths exist and entail, and help them envision themselves in a cyber job. It serves as the beginning of their cybersecurity career pathway and entry into the longer term pipeline.

Since inception, *See Yourself in Cyber* has reached 12 schools across North and South Carolina, Texas, and Alabama, engaging over 1,250 students with diverse exhibitors such as CISA, Dell, Amazon, the FBI, and local law enforcement agencies. With 142 students joining the mentor program, participants are reporting increased interest and confidence in pursuing cyber careers and interview readiness.

Collaborations with Women in CyberSecurity (WiCyS) led to the creation of new chapters in two schools, while the partnership with the OneInTech Foundation has initiated a $20,000 scholarship program for the next school year. The program has attracted local Congressmen, fostering support and participation, leading to positive press coverage, including statements from members of Congress, RSA webinars, and industry panel discussions. This program has recently received significant funding for expansion this coming year.

CyberSecure My Business: NCA's CyberSecure My Business (CSMB) program engages small businesses, academia, federal agencies, and SLTTs via virtual workshops and monthly webinars to share best practices and tools for under-resourced organizations. The interactive workshops are non-technical and based on the NIST Cybersecurity Framework 5 Steps of Identify, Protect, Detect, Respond and Recover with content in layman's terms for small- and medium-sized business leaders.

The curriculum will have a modular approach, allowing key elements like case studies and hands-on activities to be customized for specific industry verticals. With the modular agnostic content as a starting point, we will collaborate with corporations, industry associations, and government partners to create the industry-specific materials and ensure the relevance and applicability of the content.

Weekly assignments will focus on actions SMBs can take to better secure their businesses.There will be ongoing follow-up to make sure they've taken action, including

encouragement and offering further resources to help. Attendees will also leave with a custom incident response plan.

In addition to the above programs, NCA also conducts the following activities:

Cybersecurity Education and Career Resource Library

There is a critical shortage of cybersecurity professionals. NCA has compiled free resources on its website focused on fulfilling the mission of diversifying and filling the gap in the cybersecurity careerforce. For cybersecurity professionals of today and tomorrow.

***Convene*: Security Training and Awareness Conference**

NCA brings together cybersecurity experts, government leaders, industry peers, and cutting-edge exhibitors so that business professionals can elevate their cybersecurity training and awareness programs and learn from experts.

5. **Has your organization ever received a prior cy pres award?**
   No. NCA has not received a prior *cy pres* award.

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity?**
   Yes. NCA's Charity Navigator score is 96%, earning it a Four-Star rating. This means that individuals and organizations can give with confidence. In addition, NCA has a Platinum Seal of Transparency from GuideStar (https://www.guidestar.org/profile/37-1861631)

Grant Proposal:

7. **Identify the organization's principal investigator or project director.**
   Jennifer Cook - Mrs. Cook has several years of experience creating and managing national awareness campaigns. Mrs. Cook oversees strategies to engage partners and is accountable for the quality and development of surveys and metrics for the campaign. Mrs. Cook creates comprehensive marketing strategies and utilizes social media, traditional media, email and web-based platforms to amplify campaigns and activities. Mrs. Cook frequently works with industry, government and non-profit partners to cross-promote educational cybersecurity materials and form partnerships that are vital to expanding NCA's reach. She also manages NCA's communications in coordination with Crenshaw Communications to react to emerging news and to provide media opportunities

for leadership. She will work on a full-court press for media for each Data Privacy Week campaign with the goal of achieving greater success each year in terms of the reach of key messages. Mrs. Cook will work to ensure media pick-up of new research studies, the development and dissemination of media releases, generating interest and excitement for key events.

8. **Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.**

Project Name: Data Privacy Week Awareness Campaign

Issue Addressed:
All online activity generates a trail of data. Websites, apps, and services collect data on your behaviors, interests, and purchases. Sometimes, this includes personal data, like Social Security and driver's license numbers. It can even include health data.

While it's true that individuals cannot control how each byte of data is shared and processed, they are not helpless. In many cases, individuals can control how they share their data with a few simple steps.

For companies, respecting the privacy of customers, staff, and all other stakeholders is critical for inspiring trust and enhancing reputation. According to the Pew Research Center, 79% of U.S. adults report being concerned about the way their data is being used by companies. Companies need to be open about how they use data and respect individual privacy.

Project Summary: Data Privacy Day began in the United States and Canada in January of 2008. It is an extension of Data Protection Day in Europe, which commemorates the January 28, 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. While NCA has expanded Data Privacy Day to a week on its own, program expansion activities would involve working with our board, the Office of the National Cyber Director, and congress to get an official declaration from Congress to declare it Data Privacy Week (DPW).

Modeled after Cybersecurity Awareness Month (CAM), DPW uses the highly effective "Champions Program". Stakeholders approach NCA year-round, asking for details about the campaign and the Champion's program. NCA develops a comprehensive partner toolkit with creative and engaging ways to engage partners leading up to and during DPW, which includes details on messaging and activities and ways to engage with DPW

and host their own events across the country. Sample social media posts, social graphics, a sample employee email, a sample press release, downloadable logos and branding guidelines, infographics, and presentation templates are also included. The use of NCA's materials by supporters creates a coordinated messaging voice from the larger cybersecurity community.

Like CAM, DPW has the potential to saturate audiences with content over the course of a week. As additional funding allows, NCA can put more into advertising and marketing efforts, get more private sector companies involved, and have a year-round presence at privacy conferences. Typically companies have one privacy officer so it can be difficult to get out DPW materials to employees. With additional resources, NCA can build up materials that are employers and consumer friendly into bigger and broader toolkits. These toolkits with ready-made communications can be given to privacy officers to give to their internal communications officers to distribute. NCA would work throughout the year to build more connections with more data privacy contacts.

Successes:
In 2023, Data Privacy Week had

- 1,175 total people attend the Data Privacy Week virtual events on LinkedIn Live
- 2,120 registered Champions (a 28% increase from 2022)
    - When surveyed, 90% of Champions said they used NCA's materials in their campaigns
    - Champions came from a variety of sectors including tech (18%), academia (10%), government (10%), finance (8%), nonprofits (8%), and healthcare (4%)
- On Twitter, 38,000 posts from 18,000 users mentioned Data Privacy Week, resulting in 552 million potential impressions
- Data Privacy Week was shared and mentioned by large brands and entities, including Apple, Google Chrome, Intel, WhatsApp, DuckDuckGo, Firefox, the US Department of Homeland Security, the U.S. Secret Service, FEMA, the FCC, Cisco, Microsoft, LinkedIn, the SBA, Gartner and Discovery Education.

Goals and Objectives: The goal of DPW is to spread awareness about online privacy. We think data privacy should be a priority both for individuals and organizations. Our goal is twofold: we want to help citizens understand that they have the power to manage their data and we want to help organizations understand why it is important that they respect their users' data.

Project Activities and Timeline:

- **June - August: Concentrated effort to make contact with privacy officers at companies.**
- **August: Confirm Data Privacy Week theme and messaging.**
- **October - December: Create Data Privacy Week communications and social media schedule, and materials, including a toolkit, social media posts, graphics, and tip sheets. Update web pages.** This creates relevant content on data privacy tips and advice for individuals and businesses to be more informed.
- **October - December: Create robust Data Privacy Week marketing materials specifically for company privacy officers.** This material will be ready to give to their internal communications staff members to disseminate to employees as is.
- **November:** Connect with federal government and congressional contacts to see about getting a Data Privacy Week declaration from congress.
- **November: Launch Data Privacy Week Champions program and materials.** This engages public and private sector organizations and exponentially increases visibility and impact.
- **December: Host Data Privacy Week webinar.** ***To encourage partners to get involved***
- **January: Promote Data Privacy Week across all social media platforms.** Average one post a day for a total of 92 posts. Track social media engagement and growth.
- **January**: **Launch digital media campaign** to teach the general public about the importance of data privacy and provide actionable steps to protect data through video, social media and web content.
- **January: Pitch Data Privacy Week to the media**. Identify interview opportunities for leadership.
- **Data Privacy Week: Host Data Privacy Week media-genic event and release press release announcement.** Engage privacy experts and professionals in discussions around important data privacy topics.
- **February: Survey Champions, gather campaign data and results, send reports to partners.**
- **Year-round: Exhibit and/or present at privacy conferences.**

9. **Explain why the organization is approaching the issue and/or opportunity in this way.**

NCA recommends using a holistic strategy to drive privacy and cybersecurity behavior change to the American public and businesses. People and organizations have a broad range of interests, understanding, and maturity regarding privacy. No single message or

delivery method resonates with all groups at all maturity levels. An effective strategy that strengthens how individuals can monitor and be proactive with their online data is to deliver messages, tools, and resources to them in easily understood language. Capturing their attention with saturating marketing efforts that reach them where they work, live, learn, or in retirement, is also a must. Corporations also need to be aware of and responsible for their role in data privacy. The messaging to these stakeholders must be engaging and compelling enough to spur action. NCA partners with the public and private sector to execute an accessible, easily adaptable messaging campaign for enterprises, governments, and consumers with the mission of ensuring that individuals have the information and tools needed to protect their privacy all year long, and organizations take strides to protect their user data.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

Typical annual expenses for Data Privacy Week as it stands now is $110,000. This topic, however, is just as important to homeland security as NCA's October Cybersecurity Awareness Month Campaign, budgeted at $500,000 a year.

Increasing Data Privacy Week's budget to $500,000 a year can elevate this campaign into an expansive, high-profile campaign with a similar impact as Cybersecurity Awareness Month.

This additional funding can expand the reach of this campaign to the general public, involve more private sector companies, and build specialized materials for privacy officers at companies. PSA's, personalized relationship building to foster collaboration and connections between sectors, additional events, and more can be added with additional funding.

NCA has built the foundation, developed the leadership, and recruited the leadership staff, boast a very engaged and committed board of directors and have a wealth of new ideas. NCA is poised for tremendous growth as the public becomes more concerned and engaged on the topics of data privacy.

NCA has a past history of success for using extra funding for special creative projects as funds dictate and allow. NCA is happy to brainstorm special data privacy related projects with partners.

Current expenses:

a. **Personnel:** This includes portions of salaries for the Director of Marketing and Communications, Director of Partnerships and Special Initiatives, Director of Information Security and Engagement, Content Writer, Artistic Director, Executive Director, and additional support staff to plan, build relationships, create content, and disseminate content. *73% of program budget.*
b. **Consulting and Contract services:** NCA increases the efficacy of the project by contracting for a number of services with outside vendors that bring specific high-level expertise or provide a specific tool or service to deliver high-level awareness efforts and tracking. back office programmatic support, and survey and business development tools. *10% of program budget.*
c. **Advertising and Marketing expenses:** This includes a PR Firm, and Marketing companies and tools, accounting services and advertising optimization, social media listening tools, SEO consultants, advertising. *5% of program budget*
d. **Special events:** These events - in person and virtual generate media buzz and engage privacy experts and professionals in discussions around data privacy topics. *11% of program budget*

11. **Will the money be used to continue an existing project or create a new project?**
Funds will be used to continue and enhance the scope of our existing Data Privacy Week Campaign efforts.

12. **What target population will your organization's project benefit?**
Individual digital consumers, and public and private sector organizations. In 2022, the majority of participants in our champions program came from the tech sector, academia, and government organizations.

Evaluation:

13. **Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?**
Yes. NCA has 20 years of experience managing federal grants and associated fiscal responsibilities and has a proven track record of exceeding grantor expectations. NCA has extensive experience providing funders with thorough reports and updates on program statuses and outcomes. NCA can provide data as needed with the format and metrics that work best for the Court.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

NCA tracks outcomes of Data Privacy efforts through a variety of tools. The post event Champion surveys measure the impact of the campaign elements on partner activities and successes. NCA uses social media listening tools, traditional media monitoring, and web monitoring to track how widely information is being viewed and shared.

NCA tracks the following metrics to determine the success of Data Privacy Campaign efforts:

- Event unique viewers
- Event views
- # Twitter Chat authors
- # Twitter Chat tweets
- # Twitter impressions
- # Data Privacy Week Champions (individuals and organizations) and year over year growth rate.
- % of those who use NCA resources in their campaigns or activities
- Various sectors represented in Champions program
- Website metrics: Visits and Page Views
- Twitter: Posts and approximate impressions
- Notable shares and reposts by prominent individuals and companies
- NCA asks partners the following questions in a post-campaign survey
    - Has your organization participated in Data Privacy Day or Data Privacy Week prior to 2023?
    - Did you use National Cybersecurity Alliance resources in your Data Privacy Week activities?
    - If so, which resources did you use? (check all that apply)
    - In which ways did your company/organization participate in Data Privacy Week 2023?
    - Tell us about any other activities, successes or results from your campaign.
    - Do you plan to participate in Data Privacy Week next year? How can NCA help you prepare?

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

NCA staff are often panelists at industry events and speakers at various conferences, and can incorporate project results into these speaking engagements. NCA also hosts

Convene, a regional conference for cybersecurity professionals, and can share the information through workshops or panel discussions.

NCA works with a public relations firm to generate year-round press coverage. Recently, NCA issued a *See Yourself in Cyber* press release including statements from Members of Congress supporting the program. Direct press outreach has yielded multiple positive articles about the program, including an RSA webinar, panel discussions at industry events, and other positive publicity.

Organization Contact Information:

National Cybersecurity Alliance
1333 New Hampshire Ave, Floor 2, Washington, DC 20036 (physical)
717 Coliseum Dr NW, Winston-Salem, NC 27106 (mailing)
www.staysafeonline.org
EIN: 37-1861631

Lisa Plaggemier
Executive Director
lisap@staysafeonline.org
512-350-5403

Jennifer Cook
Senior Director of Marketing
jennifer@staysafeonline.org

Exhibit Q

NEW YORK UNIVERSITY
INFORMATION LAW INSTITUTE

Proposal to *In re Google Location History Litigation* Cy Pres Fund

October 3rd, 2023

Table of Contents

About the Information Law Institute at the NYU School of Law

NYU's Information Law Institute (ILI) is an interdisciplinary academic center for the study of law, policy, and digital technology. The ILI pursues its mission in three primary ways: i) convening weekly meetings of the Privacy Research Group, an interdisciplinary community of students, postdoctoral researchers, faculty, industry professionals and others; ii) supporting and mentoring a multidisciplinary group of postgraduate ILI Fellows; and iii) organizing substantive conferences and workshops to explore important issues in information law and policy. By focusing its efforts in this way, the ILI leverages a small budget to have a significant impact on training future leaders in privacy and digital information research, education, policymaking and advocacy. More detail about the ILI and its recent activities and personnel is available here: https://www.law.nyu.edu/centers/ili.

The ILI has not been separately reviewed by Charity Navigator, but New York University overall received a score of 86%. The ILI has extremely low administrative costs because it has no paid director and only supports a small portion of a law school admin's salary. The vast majority of the ILI's funding goes to support the research of ILI Fellows and ILI conferences and events. The ILI has received funding from various sources, including grants from the National Science Foundation and various private foundations and unrestricted gifts from Microsoft Corporation. While funding is sometimes granted for investigation of particular issues, the ILI's research is otherwise conducted independently, without funder influence or direction.

Current ILI Programs

Privacy Research Group

Weekly Privacy Research Group meetings revolve around presentation and discussion of members' ongoing research and relevant current events. PRG meetings draw about 45 attendees from a variety of disciplines including law students, PhD and JSD students, postdoctoral fellows, visiting global researchers, industry professionals and others. Membership is open to anyone who is interested, but members must commit to attending regularly and participating by making presentations, reporting on current privacy-related news and events, engaging in discussion of other members' presentations and so forth. These simple mutual participation requirements create a community atmosphere that is highly conducive to productive interdisciplinary conversation. Participation has held steady (and even grown) during a transition to remote — and now hybrid — format because of the pandemic. We have decided to continue in hybrid format, in part because the remote option has allowed PRG community to expand both nationally and internationally, while remaining rooted primarily at NYU. PRG membership is a particularly important opportunity for students. It offers exposure to interdisciplinary

research and a pathway to mentorship and collaborative relationships with faculty and postgraduate researchers. PRG Student Fellows and other students often have the opportunity to work on summer research projects with ILI researchers and sometimes to co-author publications. A list of recent PRG presentation abstracts is available here: https://www.law.nyu.edu/centers/ili/privacy_research_group

ILI Fellowship Program

ILI Fellows produce cutting- edge independent research during two-year paid postgraduate fellowships in an interdisciplinary setting and then apply their interdisciplinary perspective and research skills in academia, non-profit groups and the corporate world. ILI Fellows also anchor the Privacy Research Group and participate in weekly Fellows Meetings of about a dozen researchers, including selected JSD students, researchers affiliated with other NYU centers, and visiting global faculty and doctoral students. Fellows Group meetings provide an opportunity for more intensive discussion of members' research projects. ILI Fellowship training not only prepares fellows for successful interdisciplinary careers, but also creates a community of researchers and advocates who continue to collaborate, both informally and formally, after fellows leave the ILI.

Since 2011, the ILI has hosted 35 postgraduate fellows with graduate degrees in more than fifteen disciplines. Of this group, 23 are currently in tenured or tenure-track academic positions, 3 work in full-time policy-related positions, 3 work in industry or at law firms, three are currently ILI Fellows and three are in other academic positions (postdoctoral researcher, visiting assistant professor, etc.) All 35 ILI Fellows and former fellows (and many others who attended PRG or ILI Fellows meetings) remain active in the areas of privacy, AI and/or information law and policy.

ILI Fellows pursue self-selected research projects in the general areas of privacy, AI and information law and policy. Some current and recent topics include:

- Theoretical and empirical investigations of the efficacy of data breach notification laws
- Theoretical and empirical studies of online misinformation
- Empirical studies of online privacy policies
- Tradeoffs between privacy, fairness and accuracy in machine learning
- Privacy and the efficacy of contact tracing apps
- Knowledge commons perspective on privacy as governance of information flows
- Fiduciary duties as a model for regulating internet intermediaries

- Financial regulation as a potential model for privacy regulation
- How companies dodge sectoral privacy regulation and whether omnibus regulation is the answer
- Economic and social power dynamics (including market power and antitrust) associated with digital platforms
- Explanation and predictive algorithms
- Trade secrecy and algorithmic decision-making
- Potential approaches to privacy remedies and governance

Information about current and former ILI Fellows and affiliates is available here: https://www.law.nyu.edu/centers/ili/people

Conferences and Workshops

The ILI regularly hosts conferences and workshops on current privacy-related topics. After taking a pandemic-related break, ILI hosted the Northeast Privacy Scholars Conference during Fall 2022. In 2023, we have hosted a conference on Tackling Digital Market Power: Antimonopoly and Regional Regulatory Action and a Roundtable on Large Language Models, Law and Policy. We will host a symposium on children's online privacy this October. Previous conference topics have included: Cybersecurity and Digital Supply Chains, Trade Secrets and Algorithmic Systems, Face Recognition (with NYU's Policing Project), Governing Privacy in Knowledge Commons, Economics and Data Science in Conversation About Algorithms, Privacy Localism, Algorithms and Explanations.

More details about past ILI events is available here: https://www.law.nyu.edu/centers/ili/events.

Founding and History of ILI

The ILI was founded as a research institute at NYU School of Law in 2000. It coalesced into its current form as a hub of privacy and information policy research, education, discussion and debate through the leadership of former ILI Director Helen Nissenbaum (now director of Cornell Tech's Digital Life Initiative) and current ILI Director Katherine Strandburg.

Prior *Cy Pres* Awards

The ILI has used prior *cy pres* awards to support the research of ILI Fellows and to fund conferences and events on topics related to consumer privacy. We have been a *cy pres* recipient (or proposed recipient) in the following cases:

- Lundy v. Meta, 3:18-cv-06793-JD, N.D. Ca. (proposed recipient pending final approval)
- Fraley v. Facebook, CV 11-0126 LHK, N.D. Ca. ($501K received in 2017)
- Digital Trust Foundation (Fund designated in Lane v. Facebook, 5:08-cv-03845, N.D. Ca.) ($125K received in 2015)
- In re Netflix Privacy Litigation, 5:11-cv-00379, N.D. Ca, ($331K received in 2014)

Grant Proposal

We propose to use *cy pres* funds to support the core programs of the ILI by offering two two-year ILI Fellowships to postdoctoral researchers who submit outstanding proposals to conduct research on personal data privacy online, and by organizing two workshops to convene privacy experts at NYU. In particular, we hope to seek one fellow with a technical degree (e.g., computer science, data science, information science) and one with a degree in law, policy or related fields, who would complement each other's expertise while working on independent and, potentially, collaborative projects.

We propose to leave the specific topic of research open at this point for two reasons. First, given that issues of privacy and digital technology evolve extremely rapidly while it is hard to predict the timing of an eventual *cy pres* award realistically, we believe that soliciting research proposals from prospective fellows will give us the opportunity to aim our efforts at the most timely and important research questions. Second, allowing candidates to propose research directions will help us to attract (and evaluate) the best candidates with the most interesting, relevant and complementary research interests. Of course, those project directions will be honed in light of feedback from the principal investigators and other members of the ILI community.

We are particularly excited about offering this combination of fellowship opportunities in light of the ILI's addition of Prof. Sunoo Park, newly hired member of the Computer Science Department at the NYU Courant Institute of Mathematical Sciences, to the ILI's affiliated faculty roster. Professor Park, who also holds a J.D. degree, will serve as co-principal investigator alongside ILI Faculty Director Katherine Strandburg on this project, providing invaluable mentoring support for both fellows. Given the ILI's longstanding commitment to interdisciplinary research that addresses issues at the intersection of technology and law, and considering the inherently interdisciplinary nature of the

privacy harms central to the *In re Google Location History* litigation, we believe this collaboration between principal investigators across the School of Law and the Computer Science department at NYU will best position us to conduct research that sheds light on and improves the protection of personal data online, taking into account the full range of legal and technological mechanisms that may be available today and in the future.

Principal Investigators

Alfred Engelberg Professor of Law Katherine J. Strandburg is the Faculty Director of the Information Law Institute. Prof. Strandburg specializes in the law and policy of information privacy, algorithmic decisionmaking, knowledge commons governance, and innovation, focusing on the interplay between social behavior and technological change. She has authored amicus briefs to the Supreme Court and federal appellate courts on these issues. Prof. Strandburg graduated with high honors from the University of Chicago Law School and served as a law clerk to the Honorable Richard D. Cudahy of the U.S. Court of Appeals for the Seventh Circuit. Prior to her legal career, she was a physicist at Argonne National Laboratory, having received her Ph.D. from Cornell University and conducted postdoctoral research at Carnegie Mellon.

Prof. Sunoo Park is an Assistant Professor in Computer Science at the NYU Courant Institute of Mathematical Sciences, Affiliated Interdisciplinary Faculty at the NYU School of Law, and a Faculty Affiliate at the Information Law Institute. Prof. Park's legal scholarship is in technology law and policy, with a particular interest in the security, privacy, and transparency of digital technologies. In computer science, she does research in cryptography, privacy technologies, and computer security. She received her J.D. at Harvard Law School, her Ph.D. in computer science at the Massachusetts Institute of Technology, and her B.A. in computer science at the University of Cambridge.

Curriculum vitae for both principal investigators are attached at the end of this proposal.

Summary of Plan

Two ILI Fellows with Synergistic Expertise

We propose to offer two ILI Fellowships to postdoctoral researchers who submit outstanding proposals to conduct original academic research on personal data privacy online. Fellowships would be offered for an initial one-year term, with the opportunity (and in most circumstances expectation) for a one-year extension. Our experience suggests that two years is ordinarily an optimal time frame for a fellowship; it is long enough to complete a significant project and to create a trade record for seeking an appropriate "next" position—often, in our experience, a faculty position where the fellow builds upon

and broadens their fellowship research, while also teaching and mentoring students interested in privacy and other topics in technology policy. We would solicit submissions through a public posting on the ILI website as well as through social media outreach and professional networks that reach junior scholars in privacy and related areas. Ideally, in order to promote diverse and multidisciplinary approaches to the challenges of protecting personal data online, as well as to promote cross-disciplinary dialogue on these topics, we would seek one researcher with a background in law, policy, or related fields, and another researcher with a background in computer science, information science, or related fields. We would, however, be flexible about the disciplinary backgrounds of the two fellows depending on the strengths of the submissions that we receive.

Our call for proposals would describe the ILI and its programs and the goals of these particular fellowship positions. We would ask each applicant to provide a cover letter, a research proposal, a CV and transcripts, and at least one relevant publication or dissertation chapter. In evaluating applications, we will take into consideration the applicants' research interests and potential, communication skills, and any previous experience in public interest or charitable work. In light of the context of this litigation, we will favor strong proposals that address issues of importance to the class by, for example, focusing on location privacy specifically, addressing specific communities adversely impacted by a lack of protection of their personal data online, and/or including a public communication or outreach component. We will also consider the timeliness and urgency of the problems tackled: as also noted above, this aspect cannot be predicted in advance, and this is a reason that we favor an open-ended solicitation of proposals upon award of funding.

Taking all of the above into account, we will form a short list of at least three strong candidates to interview for each position. After identifying the strongest two candidates, we will make offers. If a fellowship offer is declined, we may extend an offer to another shortlisted candidate, or we may postpone the fellowship by a year.

Two Workshops

We would also propose to organize two workshops at NYU convening appropriate academic, policy and industry experts. These workshops would focus on topics and themes that are i) significant to Internet users and ii) relevant to the fellows' research projects. We would anticipate that the funded ILI Fellows would be significantly involved in organizing these workshops, both because they will be developing expertise on the topics and because organizing a workshop will provide useful experience and networking opportunities for the fellows. We will expect the Fellows, perhaps with the assistance of PRG Student Fellows, to produce a summary write-up of each workshop, focusing on and summarizing policy-relevant aspects, for posting on the ILI website.

As an additional outreach and educational contribution, we would encourage the funded ILI Fellows to give at least one guest lecture in a graduate or undergraduate class related to their research area.

Timeline

As outlined below, our timeline would begin in the summer/fall after we receive the funding, in order to support fellowships that are synchronized with the academic calendar and hiring seasons. The hiring schedule may need to be adjusted depending on whether competitive candidates have other constraints (e.g., job offers) that we feel justify adjustments. Depending on the strength of applications and the circumstances of the applicants in a given year, we may also decide to postpone one or both of the fellowship positions to the following academic year.

- *Summer/Fall after funding is received (year X):* Publish and disseminate Call for Proposals, asking potential fellows to submit their research proposals and other materials.
- *The following January (year X+1):* Deadline for proposals to be submitted. Profs. Strandburg and Park will then review the applications over the following month and decide on a short list of candidates with the most competitive proposals.
- *The following February (year X+1):* Profs. Strandburg and Park will contact shortlisted candidates to arrange interviews, which will take place during February (probably by Zoom). Once interviews are complete, Profs. Strandburg and Park will meet to finalize the selection of candidates, and then send fellowship offers to the selected candidates.
- *The following August (year X+1):* Fellowships begin. Fellows will be encouraged to give a guest lecture in a class related to their research during the first academic year.
- *The following year (year X+2):* Each fellow organizes a conference or workshop on a topic related to their research, that will take place sometime in the calendar year after they start their fellowships. If the fellows' interests align sufficiently, they may co-organize either a single larger conference or two workshops.
- *The following summer (year X+3):* Each fellow writes a short essay to be posted on the ILI website, aimed at a broad (non-legal, non-technical) audience, which summarizes work they have done during their fellowship and the problems that their work studies or addresses.
- *The following August (year X+3):* Fellowships end.

Funding Needs

We anticipate the following funding needs for the fellowships, workshops, and other support needed to effectively conduct and disseminate the research projects funded. We would use the funding towards new fellowships within the existing ILI Fellowship Program, and towards supporting new projects proposed by the fellows themselves in their fellowship applications. If the fellows' projects overlap with existing ILI projects, the funds may be used in a way that benefits existing projects, as long as the primary purpose of the use of funds is to support the fellows' new projects.

- Salary of $85K/yr plus benefits for two two-year fellowships:$222,700
- Administrative support costs for fellows: $22,270
- Two 2-day workshops ($50,000 each) including meals and travel expenses for approx. 50 participants, AV, administrative support : $100,000
- Other incidental costs (e.g., for travel, equipment, experiments, interviews, hiring student research assistants, etc.) incurred by the fellows or other ILI personnel in connection with the projects: $60,000
- TOTAL: $404,970

Who Will Benefit

Our projects will benefit Internet users whose privacy is affected by the activities of tech companies, as well as policymakers and the public more broadly: our primary expected outputs will be research publications and conference presentations that disseminate new insights about the current state of protection of personal data online and/or suggest new legal, policy, or technological approaches towards better protecting personal data online. Our Fellows' guest lectures would also benefit (undergraduate or graduate) students taking classes related to technology law/policy or privacy, who would gain additional awareness of the problems of data privacy online, and gain exposure to a cutting-edge research perspective on our Fellows' focus areas. A more specific and complete description of beneficiaries will depend on the particular research projects that our funded Fellows conduct. Because of the pace of change in this arena, and our commitment to supporting original research by outstanding junior scholars that we select for our fellowships, we believe that it is wiser to wait to determine the most effective use of research funds until the time of the award.

Evaluation

If awarded funding for this proposal, we agree to provide a report to the Court and the parties every six months informing the Court and the parties of how the allocated funding has been used up to the time of reporting, and how we plan to use the remaining funds. We will evaluate the success of the grant in terms of outcomes of the research and workshops in terms of publications, policy proposals and policy outcomes, as well as in terms of our success in training privacy researchers who go on to work in this arena.

Public-Facing Outputs

Publications and presentations are, of course, a primary output of any academic research institution. We would expect our Fellows to publish their research output in relevant scholarly venues. Fellows are encouraged to publish preprints whenever possible in open access forums such as Arxiv and SSRN. We also expect Fellows to present their research results at appropriate academic conferences such as the Privacy Law Scholars Conference and, where possible, in policy forums such as the Federal Trade Commission's PrivacyCon (see, for example, https://www.ftc.gov/news-events/events/2024/03/privacycon-2024). In addition, as mentioned above, we would require fellows supported by *cy pres* funds to create summary write-ups of their work and of the workshops for posting on the ILI website.

Appendix: Curriculum Vitae of Principal Investigators

Sunoo Park J.D., Ph.D.

60 Fifth Avenue, Office 316, New York, NY 10011 · (+1) 510-292-1138 · sunoo.park@nyu.edu

Current Position

NEW YORK UNIVERSITY, Assistant Professor, September 2023–
- **NYU Courant Institute of Mathematical Sciences,** Assistant Professor
- **NYU School of Law,** Affiliated Interdisciplinary Faculty

Education

HARVARD LAW SCHOOL, J.D., June 2021
Study abroad: **INSTITUT D'ÉTUDES POLITIQUES DE PARIS (SCIENCES PO)**, Paris, France (Spring 2020)
Other: Pro Bono Certificate (over 1000 hours of pro bono service)

MIT, Ph.D., Computer Science, June 2018
Advisor: **Shafi Goldwasser**
Dissertation: *Cryptography for Societal Benefit*
Affiliations: MIT Computer Science & Artificial Intelligence Laboratory (primary)
MIT Internet Policy Research Initiative
MIT Media Lab, Digital Currency Initiative

MIT, S.M., Computer Science, June 2015
Advisor: **Shafi Goldwasser**
Dissertation: *On Time and Order In Multi-Party Computation*

UNIVERSITY OF CAMBRIDGE (Trinity College)**,** B.A., Computer Science, June 2013
Advisor: **Ross Anderson**
Dissertation: *Secure Practical Image Steganography* (Highly Commended)
Other: President of C.U. Computing & Technology Society, 2011–13

Interest Areas

Technology law, security, cryptography, privacy, transparency.

Bar Admission

Member of the New York State Bar.

Experience

COLUMBIA UNIVERSITY & COLUMBIA LAW SCHOOL, Postdoctoral Fellow, 2022–23
Hosted by Steven Bellovin & Daniel Richman
CORNELL TECH, Digital Life Initiative, Postdoctoral Fellow, 2021–22
Hosted by James Grimmelmann & Helen Nissenbaum
MIT MEDIA LAB, Digital Currency Initiative, Researcher, 2018–20
Hosted by Neha Narula
BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY, Affiliate, 2017–20
FEDERAL TRADE COMMISSION (FTC), Bureau of Consumer Protection, Division of Privacy and Identity Protection (DPIP), Summer Law Clerk, 2020
KNIGHT FIRST AMENDMENT INSTITUTE, Summer Legal Intern, 2019
THE NEW YORK TIMES, Summer Intern, 2017
UCLA, Visiting Ph.D. Student, 2016
SIMONS INSTITUTE FOR THE THEORY OF COMPUTING, Visiting Ph.D. Student, 2015
WEIZMANN INSTITUTE OF SCIENCE, Visiting Ph.D. Student, 2015
MICROSOFT RESEARCH NEW ENGLAND, Summer Ph.D. Intern, 2014

Publications (Law)

The Right To Vote Securely
Sunoo Park
In: the **UNIVERSITY OF COLORADO LAW REVIEW (forthcoming 2023)**.

A Researcher's Guide to Legal Risks of Security Research (associated blog post)
Sunoo Park and Kendra Albert
Jointly published by: the **Cyberlaw Clinic at Harvard Law School** & the **Electronic Frontier Foundation (EFF), 2020.**

Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries
Aloni Cohen and Sunoo Park
In: 32 **HARVARD JOURNAL OF LAW & TECHNOLOGY** 169 **(2018)**.

Publications (Computer Science)

[click title to view]

Cryptography, Trust, and Privacy: It's Complicated
Ero Balsa, Helen Nissenbaum, & Sunoo Park
In: **ACM Symposium on Computer Science and Law (CSLAW) 2022.**

KeyForge: Non-Attributable Email from Forward-Forgeable Signatures
*Michael Specter, Sunoo Park, & Matthew Green
In: **USENIX Security Symposium 2021.**

Going From Bad to Worse: From Internet Voting to Blockchain Voting
*Sunoo Park, Michael Specter, Neha Narula, & Ronald L. Rivest
In: **Journal of Cybersecurity, 2021.**

Fully Deniable Interactive Encryption
Ran Canetti, Sunoo Park, & Oxana Poburinnaya
In: **IACR International Cryptology Conference (CRYPTO) 2020.**

Data Structures Meet Cryptography: 3SUM with Preprocessing
Alexander Golovnev, Siyao Guo, Thibaut Horel, Sunoo Park & Vinod Vaikuntanathan
In: **Symposium on Theory of Computing (STOC) 2020.**

It Wasn't Me! Repudiability and Claimability of Ring SIgnatures
Sunoo Park and Adam Sealfon
In: **IACR International Cryptology Conference (CRYPTO) 2019.**

How To Subvert Backdoored Encryption: Security Against Adversaries That Decrypt
Thibaut Horel, Sunoo Park, Silas Richelson, & Vinod Vaikuntanathan
In: **Innovations in Theoretical Computer Science (ITCS) 2019.**

Practical Accountability of Secret Processes
*Jonathan Frankle, Sunoo Park, Daniel Shaar, Shafi Goldwasser, & Daniel J. Weitzner
In: **USENIX Security Symposium 2018.**

Static-Memory-Hard Functions and Modeling the Cost of Space vs. Time
Thaddeus Dryja, Quanquan C. Liu, & Sunoo Park
In: **IACR Theory of Cryptography Conference (TCC) 2018.**

SpaceMint: A Cryptocurrency Based on Proofs of Space
*Sunoo Park, Albert Kwon, Georg Fuchsbauer, Peter Gaži, Joël Alwen, & Krzysztof Pietrzak
In: **Financial Cryptography 2018.**

Proactive Secure Multiparty Computation Against a Dishonest Majority
Karim Eldefrawy, Rafail Ostrovsky, Sunoo Park, & Moti Yung
In: **Security and Cryptography for Networks (SCN) 2018.**

Public Accountability vs. Secret Laws: Can They Coexist?
Shafi Goldwasser and Sunoo Park
In: **Workshop on Privacy in the Electronic Society (WPES) at the ACM Conference on Computer and Communications Security (CCS) 2017.**

Towards Secure Quadratic Voting
Sunoo Park and Ronald L. Rivest
In: **Public Choice 2017.**

How To Incentivize Data-Driven Collaboration Among Competing Parties
Pablo Daniel Azar, Shafi Goldwasser, & Sunoo Park
In: **Innovations in Theoretical Computer Science (ITCS) 2016.**

Adaptively Secure Coin-Flipping, Revisited
Shafi Goldwasser, Yael Tauman Talai, & Sunoo Park
In: **Int'l Colloquium on Automata, Languages, and Programming (ICALP) 2015.**

Cryptographically Blinded Games: Leveraging Players' Limitations for Equilibria & Profit
Pavel Hubáček and Sunoo Park
In: **ACM Conference on Economics and Computation (EC) 2014.**

** In computer science, conferences and symposia are peer reviewed, and they are the primary publication outlets. In law, journals are the primary publication outlets. Certain subfields order authors alphabetically; others order primarily by contribution. Here, author order is alphabetical except where asterisked.*

Manuscripts

A Systematization of Voter Registration System Security
Jack Cable, Andrés Fábrega, Sunoo Park, & Michael Specter
In submission.

Scan, Shuffle, Rescan: Two-Prover Election Audits
Douglas W. Jones, Sunoo Park, Ronald L. Rivest, & Adam Sealfon
In submission.

The Superlinearity Problem in Post-Quantum Blockchains
Sunoo Park & Nicholas Spooner
In submission.

Honors & Awards

Computing Innovation Fellowship, Computing Research Association & Computing Co
Berkman Klein Fellowship, Berkman Klein Center at Harvard University, 2017–18
Akamai Presidential Fellowship, MIT, 2013–14
Deputy Leader of UK Team, International Olympiad in Informatics (IOI), 2011
UK Team Member, International Olympiad in Informatics (IOI), 2010

Teaching & Advising Experience

Guest lecture, at Columbia Law School on *Cybersecurity* (2022).
Guest lecture, at Cornell Tech on *Information Privacy & the 4th Amendment* (2022).
Co-advisor (with Prof. Ronald Rivest), MIT M.Eng. student *Andrés Fabrega* (2021–22).
Co-instructor, MIT graduate class on *Advanced Cryptography* (2016).
Teaching assistant, MIT graduate class on *Cryptography* (2016).

Academic Service

- **Program committee member** for:
  - IEEE Security & Privacy ("Oakland") 2022 & 2023
  - IEEE Security & Privacy 2022 & 2023 — Research Ethics Committee
  - Neural Information Processing Systems (NeurIPS) 2022 — Ethics Committee
  - ACM Symposium on Computer Science and Law (CSLAW) 2022
  - ACM Conference on Fairness, Accountability, and Transparency (FAccT) 2021
  - Journal of Cryptoeconomic Systems 2020
  - IACR Theory of Cryptography Conference (TCC) 2020
- Co-organizer of **Workshop on Encryption, Surveillance, & Transparency** held at Johns Hopkins University, August 2018.

Selected Invited Talks

The Right To Vote Securely
At: Digital Life Initiative Seminar, ***Cornell Tech***, 2022
Math & Democracy Seminar, ***NYU Center for Data Science***, 2022 (upcoming)

Public Accountability of Secret Processes (Inspired By ECPA and FISA)
At: Future of Encryption Committee, ***National Academies of Sciences, Engineering, and Medicine***, 2020

The Power of Repudiation: Ring Signatures & Non-Attributable Email
At: BU Security Seminar, ***Boston University***, 2019
MIT Digital Currency Initiative, ***MIT Media Lab***, 2019

Elections, Blockchains, and Maybe Catastrophes
At: Program on Proofs, Consensus, and Decentralizing Society, ***Simons Institute for the Theory of Computing, UC Berkeley***, 2019

Short Writing

- On Sovereignty in Cyberspace, *Berkman Klein Center Collection*, March 2018
- Decentralize all the things?, *MIT Media Lab Digital Currency Initiative*, August 2017
- Theory of Blockchains, *MIT Media Lab Digital Currency Initiative*, December 2016

Other

- Attended **Summer School on EU Policy Making** at the Brussels School of Governance, Institute for European Studies in July 2023.
- Coauthored 2 cryptography puzzles in **The Boston Globe** in 2017 (links here).
- **Languages:** English (native); French, Italian, Spanish (intermediate).
- **Citizenship:** UK & USA.

KATHERINE J. STRANDBURG
New York University School of Law
40 Washington Square South, New York, NY 10012

EMPLOYMENT

New York University School of Law, ***Alfred Engelberg Professor of Law*****,** 2013-, ***Professor*****,** 2009-13, ***Visiting Associate Professor*****,** 2007-08
Faculty Director, Information Law Institute, 2016-
Faculty Co-Director, Engelberg Center on Innovation Law and Policy, 2009-,

Fordham University School of Law, ***Visiting Professor*****,** Fall Semester 2008

University of Illinois College of Law, ***Visiting Associate Professor*****,** Fall Semester 2005

DePaul University College of Law, ***Professor*****,** 2008-09, ***Associate Professor,*** 2005-08 ***Assistant Professor***, 2002-05, Outstanding Achievement in Scholarship, 2004

Mulroy Scandaglia Marrinson Ryan, ***Associate,*** 2001-02

Jenner & Block, ***Associate***, 1996-2001

Judge Richard Cudahy, United States Court of Appeals Seventh Circuit, ***Law Clerk,*** 1995-96

Northwestern University, ***Visiting Professor, Department of Physics***, 1990-92
Recipient of Visiting Professorships for Women grant from the National Science Foundation

Argonne National Laboratory, ***Condensed Matter Theory Group***, 1987-92
Conducted scientific research using computer simulation techniques

Carnegie-Mellon University, ***Postdoctoral Research Associate, Physics,*** 1984-87

EDUCATION

University of Chicago Law School, ***J.D., with high honors,*** **1995**
Order of the Coif; Edwin F. Mandel Award for Exceptional Contributions to the Clinical Program
Olin Foundation Scholarship for Law and Economics; Law School Scholarship

DePaul University College of Law, 1992
College of Law Scholarship; American Jurisprudence Awards – Contracts, Legal Writing

Cornell University, ***Ph.D., Physics,*** **1984**
Thesis topic: Computer simulations of statistical mechanical models; National Science Foundation Graduate Fellowship

Stanford University, ***B.S., Physics, with distinction*****, 1979**
Phi Beta Kappa; David S. Levine Award for Excellence in Physics

BAR ADMISSIONS

Supreme Court of the United States, Federal Circuit, Seventh Circuit, Northern District of Illinois, Illinois, U.S. Patent & Trademark Office

RESEARCH GRANTS

Co-PI (with Joshua Epstein, Erez Hatna, Michael Tschantz and Sebastian Benthall), *DASS: Agent Based Modeling at the Boundary of Law and Software*, NSF Grant # 2131532, $545,000 (2021-24)

Co-PI (with Brett M. Frischmann, Michael J. Madison and Madelyn Sanfilippo), *RCN: The Governing Knowledge Commons Research Coordination Network*, NSF Grant #2017495, $350,000 (2020-23)

Mentor and Co-PI for Sebastian Benthall, NSF Postdoctoral Fellowship, Heterogeneous Agent Modeling of the Personal Data Economy, NSF Grant #2015301 (2021-23)

BOOKS

Madelyn Sanfilippo, Brett M. Frischmann and Katherine J. Strandburg, eds., GOVERNING PRIVACY AS COMMONS (Cambridge University Press 2021)

Katherine J. Strandburg, Brett M. Frischmann and Michael J. Madison, eds., GOVERNING MEDICAL KNOWLEDGE COMMONS (Cambridge University Press 2017) (Introduction & Chapter 1 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3053025

Brett M. Frischmann, Michael J. Madison, and Katherine J. Strandburg, eds., GOVERNING KNOWLEDGE COMMONS (Oxford University Press 2014) (Introduction & Chapter 1available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490622

Rochelle C. Dreyfuss and Katherine J. Strandburg, eds., THE LAW AND THEORY OF TRADE SECRECY (Edward Elgar 2011)

Katherine J. Strandburg and Daniela Raicu, eds., PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION (Springer 2005)

ARTICLES AND BOOK CHAPTERS

Ignacio Cofone and Katherine J. Strandburg, *Unjustifiable Algorithmic Opacity* (in preparation)

Ashley Gorham, Helen Nissenbaum, Madelyn Sanfilippo, Katherine J. Strandburg, and Mark Verstraete, *Legitimacy in Context* (in preparation)

Salome Viljoen, Helen Nissenbaum and Katherine J. Strandburg, *The Great Regulatory Dodge* (forthcoming Harvard JOLT 2024)

Sebastian Benthall, Erez Hatna, Joshua M. Epstein and Katherine J. Strandburg, *Privacy and Contact Tracing Efficacy*, J. R. SOC. INTERFACE 19:20220369, https://doi.org/10.1098/rsif.2022.0369 (peer reviewed)

Sebastian Benthall, Michael Carl Tschantz, Erez Hatna, Joshua M. Epstein and Katherine J. Strandburg, *At the Boundary of Law and Software: Toward Regulatory Design with Agent-Based Modeling*, PROCEEDINGS OF THE 1ST WORKSHOP ON AGENT-BASED MODELLING AND POLICY-MAKING (AMPM 2021), http://ceur-ws.org/Vol-3182/ (peer reviewed)

Michael J. Madison, Brett M. Frischmann, Madelyn R. Sanfilippo, and Katherine J. Strandburg, *Too Much of a Good Thing? A Governing Knowledge Commons Review of Abundance in Context,* 7 FRONTIERS IN RESEARCH METRICS AND ANALYTICS 959505 (2022). DOI: 10.3389/frma.2022.959505. (peer reviewed)

Eli Siems, Nicholas Vincent and Katherine J. Strandburg, *Trade Secrecy and Innovation in Forensic Technology,* 73 HASTINGS LAW JOURNAL 773 (2022)

Madelyn Sanfilippo and Katherine J. Strandburg, *Participatory Privacy: How Privacy Governs Community Boundaries and Inclusion in Online Social Movements*, 10 JOURNAL OF SOCIAL MEDIA IN SOCIETY, VOL. 2 (2021) (peer reviewed)

Sebastian Benthall and Katherine J. Strandburg, *Agent-Based Modeling as a Legal Theory Tool*, FRONTIERS IN PHYSICS, RESEARCH TOPIC: THE PHYSICS OF THE LAW: LEGAL SYSTEMS THROUGH THE PRISM OF COMPLEXITY SCIENCE (June 21, 2021) https://doi.org/10.3389/fphy.2021.666386 (peer reviewed)

Katherine J. Strandburg, *Adjudicating with Inscrutable Decision Rules, in* MACHINES WE TRUST: PERSPECTIVES ON DEPENDABLE AI (Teresa Scantamburlo and Marcello Pelillo, eds., MIT Press 2021)

John Nay and Katherine J. Strandburg, *Generalizability: Machine Learning and Humans-in-the-Loop*, RESEARCH HANDBOOK ON BIG DATA LAW (R. Vogl, ed., Edward Elgar 2021)

Madelyn Sanfilippo and Katherine J. Strandburg, *Public Facebook Groups for Political Activism* in GOVERNING PRIVACY AS COMMONS, M. Sanfilippo, K.J. Strandburg and B.M. Frischmann, eds; Cambridge University Press, 2021)

James Dempsey, Chris Jay Hoofnagle, Ira Rubinstein and Katherine J. Strandburg, Breaking the Privacy Gridlock: A Broader Look at Remedies, https://ssrn.com/abstract=3839711, (white paper summarized at Lawfare (April 7, 2021)

Yafit Lev-Aretz and Katherine J. Strandburg, *Privacy Regulation and Innovation Policy,* 22 YALE J.L. & TECH. 256 (2020)

Yafit Lev-Aretz and Katherine J. Strandburg, *Regulation and Innovation: Approaching Market Failure from Both Sides*, 38 YALE J. REG. BULLETIN 1 (2020)

Ignacio Cofone and Katherine J. Strandburg, *Strategic Games and Algorithmic Secrecy*, 64 MCGILL L. J. 623 (2019) (reprinted in c102 Sup. Ct. L. Rev. 39 (2021) in association with Cofone's receipt of the 2021 Canadian Institute for the Administration of Justice's Research Fellowship)

Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 COLUMBIA L. REV. 1851 (2019)

Madelyn Sanfilippo and Katherine J. Strandburg, *Privacy Governing Knowledge in Public Facebook Groups for Political Activism,* 24 INFORMATION, COMMUNICATION AND SOCIETY 960-977, DOI: 10.1080/1369118X.2019.1668458. (May 19, 2021) (online publication 2019) (peer reviewed)

Madeline Byrd and Katherine J. Strandburg, *CDA 230 for a Smart Internet,* 88 FORDHAM L. REV. 405 (2019)

Michael J. Madison, Brett M. Frischmann and Katherine J. Strandburg, *Knowledge Commons,* in ROUTLEDGE HANDBOOK OF THE STUDY OF THE COMMONS (Blake Hudson et al., eds.), Ch. 7 (2019)

Michael J. Madison, Katherine J. Strandburg and Brett M. Frischmann, *Knowledge Commons*, in RESEARCH HANDBOOK ON THE ECONOMICS OF INTELLECTUAL PROPERTY LAW (VOL. II – ANALYTICAL METHODS) (Peter Menell & David Schwartz, eds.), Ch. 30, pp. 656-76 (Edward Elgar Publishing 2019*)*

R. Boyd, P.J. Richerson, R. Meinzen-Dick, T. De Moor, M.O. Jackson, K.M. Gjerde, H. Harden-Davies, B.M. Frischmann, M.J. Madison, K.J. Strandburg, A.R. McLean, C. Dye, *Tragedy Revisited*, 362 SCIENCE 1236 (2018)

Katherine J. Strandburg, *Users, Patents and Innovation Policy*, THE OXFORD HANDBOOK OF INTELLECTUAL PROPERTY LAW (Rochelle C. Dreyfuss & Justine Pila, eds., Oxford University Press 2018)

Madelyn Rose Sanfilippo, Brett M. Frischmann, and Katherine J. Strandburg, *Privacy as Commons: Case Evaluation through the Governing Knowledge Commons Framework,* 8 JOURNAL OF INFORMATION POLICY 116 (2018) (peer-reviewed)

Katherine J. Strandburg and Brett M. Frischmann, *The North American Mitochondrial Disease Consortium: A Developing Knowledge Commons,* in Katherine J. Strandburg, Brett M. Frischmann and Michael J. Madison, eds., GOVERNING MEDICAL KNOWLEDGE COMMONS, pp. 348-389 : (Cambridge University Press 2017), doi:10.1017/9781316544587.016

Katherine J. Strandburg and Stefan Bechtold, *The Consortium of Eosinophilic Gastrointestinal Disease Researchers (CEGIR): An Emerging Knowledge Commons* in Katherine J. Strandburg, Brett M. Frischmann and Michael J. Madison, eds., GOVERNING MEDICAL KNOWLEDGE COMMONS, pp. 390-420 (Cambridge University Press 2017), doi:10.1017/9781316544587.017

Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison, *Governing Knowledge Commons: An Appraisal,* in Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison, eds., GOVERNING MEDICAL KNOWLEDGE COMMONS, pp. 421-430 (Cambridge University Press 2017), doi:10.1017/9781316544587.018

Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison, *The Knowledge Commons Framework*, in Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison, eds., GOVERNING MEDICAL KNOWLEDGE COMMONS, pp. 9-18 (Cambridge University Press 2017), doi:10.1017/9781316544587.002

B.R. Jasny, N. Wigginton, M. McNutt, Tania Bubela, S. Buck, Robert Cook-Deegan, T. Gardner, B. Hanson, C. Hustad, V. Kiermer, D. Lazer, A. Lupia, A. Manrai, L. McConnell, K. Noonan, E. Phimister, Brenda M. Simon, Katherine J. Strandburg, Z. Summers, D. Watts, *Fostering Reproducibility in Industry-Academia Research*, 357 SCIENCE 759 (2017).

Derogatory to Professional Character? Physician Innovation and Patents as Boundary-Spanning Mechanisms in CREATIVITY WITHOUT LAW: CHALLENGING THE ASSUMPTIONS OF INTELLECTUAL PROPERTY, Ch. 3, pp. 63-87 (K. Darling and A. Perzanowski, eds.) (NYU Press 2017)

Katherine J. Strandburg, *Intellectual Property at the Boundary in* REVOLUTIONIZING INNOVATION: USERS, COMMUNITIES AND OPEN INNOVATION (Dietmar Harhoff and Karim Lakhani, eds.), Ch. 12, pp. 63-87 (MIT Press 2016)

Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, Symposium on NSA Surveillance: Issues of Security, Privacy, and Civil Liberty, 10 ISJLP 327 (2014)

Katherine J. Strandburg, *Monitoring, Datafication and Consent: Legal Approaches to Privacy in the Big Data Context* in PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (J. Lane, V. Stodden, S. Bender and H. Nissenbaum, eds.), Ch. 1, pp. 5-43 (Cambridge University Press 2014)

Mark McKenna and Katherine J. Strandburg, *Progress and Competition in Design*, Symposium on Design Patents in the Modern World, 17 STANFORD TECH. L. REV. 1 (2013)

Brett M. Frischmann, Michael J. Madison and Katherine J. Strandburg, *Governing Knowledge Commons*, in GOVERNING KNOWLEDGE COMMONS (B. Frischmann, M. Madison, and K. Strandburg, eds.), Ch. 1 (Oxford University Press 2014)

Brett M. Frischmann, Michael J. Madison and Katherine J. Strandburg, *Conclusion*, in GOVERNING KNOWLEDGE COMMONS (B. Frischmann, M. Madison, and K. Strandburg, eds.), Ch. 15 (Oxford University Press 2014)

Katherine J. Strandburg, Brett M. Frischmann and Can Cui, *The Rare Disease Clinical Research Network and the Urea Cycle Disorders Consortium as a Nested Knowledge Commons* in GOVERNING KNOWLEDGE COMMONS (B. Frischmann, M. Madison, and K. Strandburg, eds.), Ch. 5 (Oxford University Press 2014)

Katherine J. Strandburg, *Legal But Unacceptable: Pallin v. Singer and Physician Patenting Norms,* in INTELLECTUAL PROPERTY AT THE EDGE: THE CONTESTED CONTOURS OF IP (R. Dreyfuss and J. Ginsburg, eds.), Ch. 15, pp. 321-342 (Cambridge University Press 2014)

Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, Frontiers of Consumer Protection, 2013 U. CHI. L. FORUM 95

Katherine J. Strandburg, *Much Ado about Preemption*, 50 HOUSTON L. REV. 563 (2013)

Péter Érdi, Kinga Makovi, Zoltán Somogyvári, Katherine J. Strandburg, Jan Tobochnik, Péter Volf, László Zalányi) *Prediction of Emerging Technologies Based on Analysis of the U.S. Patent Citation Network*, 95 SCIENTOMETRICS 225-242 (April 2013) (DOI) 10.1007/s11192-012-0796-4

Katherine J. Strandburg, *Rounding the Corner on Trade Dress: A Tribute to the Jurisprudence of Judge Richard D. Cudahy*, 29 YALE J. ON REG. 387 (2012)

Michael J. Madison, Brett M. Frischmann and Katherine J. Strandburg, *Constructing Commons in the Cultural Environment*, in THE WEALTH OF THE COMMONS: A WORLD BEYOND MARKET AND STATE (Silke Helfrich and David Bollier, eds.) (2012)

Katherine J. Strandburg, *Patent Fair Use 2.0,* 2 UC IRVINE L. REV. 266 (2011)

Katherine J. Strandburg, *Home, Home on the Web: The Fourth Amendment and Technosocial Change*, 70 MD. L. REV. 614 (2011)

Katherine J. Strandburg, *Comments on Designing the Microbial Research Commons: Digital Knowledge Resources* in NRC Board on Research Data and Information, DESIGNING THE MICROBIAL RESEARCH COMMONS: PROCEEDINGS OF AN INTERNATIONAL SYMPOSIUM, Paul F Uhlir, ed. (2011)

Michael J. Madison, Brett M. Frischmann and Katherine J. Strandburg, *Constructing Commons in the Cultural Environment*, 95 CORNELL L. REV. 657 (2010) (lead article in special edition with commentary)

Michael J. Madison, Brett M. Frischmann and Katherine J. Strandburg, *Reply: The Complexity of Commons*, 95 CORNELL L. REV. 839 (2010)

Katherine J. Strandburg, *Norms and the Sharing of Research Materials and Tacit Knowledge* in WORKING WITHIN THE BOUNDARIES OF INTELLECTUAL PROPERTY (Rochelle C. Dreyfuss, Harry First, and Diane L. Zimmerman, eds.), Ch. 4 (Oxford University Press 2010)

G Csárdi, KJ Strandburg, L Zalányi, J Tobochnik and P Érdi, *Estimating the Dynamics of Kernel-Based Evolving Networks*, in UNIFYING THEMES IN COMPLEX SYSTEMS, Minai A., Braha D., Bar-Yam Y. (eds.), pp. 90-97 (Springer 2010), https://doi.org/10.1007/978-3-540-85081-6_12

Katherine J. Strandburg, *User Innovator Community Norms at the Boundary Between Academic and Industrial Research*, 77 FORDHAM L. REV. 2237 (2009)

Katherine J. Strandburg, Gábor Csárdi, László Zalányi, Jan Tobochnik and Péter Érdi, *Patent Citation Networks Revisited: Signs of a Twenty-First Century Change*, 87 NORTH CAROLINA L. REV. 1657 (2009)

Katherine J. Strandburg, *Evolving Innovation Paradigms and the Global Intellectual Property Regime*, 41 CONN. L. REV. 861 (2009)

Michael J. Madison, Brett M. Frischmann and Katherine J. Strandburg, *The University as Constructed Cultural Commons*, 30 WASH. U. J. LAW & POLICY 365 (2009)

Katherine J. Strandburg, *Accommodating User Innovation in the International Intellectual Property Regime: A Global Administrative Law Approach*, 2009 ACTA JURIDICA 283 (2009)

Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B. C. L. REV. 741 (2008)

Katherine J. Strandburg, *What If There Were a Business Method User Exemption to Patent Infringement?*, 2008 MICH. ST. L. REV. 245

Michael J. Meurer and Katherine J. Strandburg, *Patent Carrots and Sticks: An Economic Model of Nonobviousness*, 12 LEWIS & CLARK L. REV. 549 (2008)

Katherine J. Strandburg, *Users as Innovators: Implications for Patent Doctrine*, 79 U. COLO. L. REV. 467 (2008)

G. Csárdi, K.J. Strandburg, J. Tobochnik, and P. Érdi *The Inverse Problem of Evolving Networks — with Application to Social Nets,* in HANDBOOK OF LARGE-SCALE RANDOM NETWORKS (B. Bollobás, R. Kozma, and D. Miklós, eds.), pp. 409-443 (Springer-Verlag 2008)

Katherine J. Strandburg, *Surveillance of Emergent Associations: Freedom of Association in a Network Society*, in DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES (Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis, eds.), pp. 435-458 (Auerbach 2007)

Gabor Csárdi, Katherine J. Strandburg, László Zalányi, Jan Tobochnik and Peter Érdi, *Modeling Innovation by a Kinetic Description of the Patent Citation System*, 374 PHYSICA A 783-793 (2007)

Katherine J. Strandburg, Gábor Csárdi, László Zalányi, Jan Tobochnik and Péter Érdi, *Law and the Science of Networks: An Overview and an Application to the "Patent Explosion*, 21 BERKELEY TECH. L. J. 1293-1362 (2006)

Katherine J. Strandburg, *The Research Exemption to Patent Infringement: The Delicate Balance Between Current and Future Technical Progress*, in INTELLECTUAL PROPERTY AND INFORMATION WEALTH (Peter Yu, ed.), Ch. 4 (2006)

Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1237 (2005)

Katherine J. Strandburg, *Social Norms, Self Control, and Privacy in the Online World*, in PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION (Katherine J. Strandburg and Daniela Raicu, eds.), Ch. 3, pp. 31-54 (2005)

Katherine J. Strandburg, *Curiosity-Driven Research and University Technology Transfer*, in UNIVERSITY ENTREPRENEURSHIP AND TECHNOLOGY TRANSFER: PROCESS, DESIGN, AND INTELLECTUAL PROPERTY, ADVANCES IN THE STUDY OF ENTREPRENEURSHIP, INNOVATION, AND ECONOMIC GROWTH : VOL. 16, (Gary D. Libecap, ed.), pp. 93-122 (2005)

Katherine J. Strandburg, *What Does The Public Get? Experimental Use and the Patent Bargain*, 2004 WISC. L. REV. 81Katherine J. Strandburg, *Deterrence and the Conviction of Innocents*, 35 CONN. L. REV. 1321 (2003)

Katherine J. Strandburg, *Official Notice of Changed Country Conditions in Asylum Adjudication: Lessons from International Refugee Law*, 11 GEORGETOWN IMMIGR. L. J. 45 (1996)

List of physics publications from 1983-1992 is attached; physics research also reported in the New York Times, Scientific American, Nature, and Science

ONLINE PUBLICATIONS

Katherine J. Strandburg, *Who's in the Club?: A Response to Oliar and Sprigman*, 94 VIRGINIA L. REV. IN BRIEF 1 (2009)

Katherine J. Strandburg, *Cross-Licensing and Injunctions - the Interplay Between Big Business, Small Business, and Non-Practicing Inventors: A Panel Discussion,* 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 925 (2009) (co-panelists Lisa M. Ferri,, John M. Griem, Jr. and Jonathan Putnam)

Katherine J. Strandburg, *Debate, The Obviousness Requirement in the Patent Law*, 155 U. PENN. L. REV. PENNUMBRA 96 (2006)

SCHOLARLY PRESENTATIONS

Invited Lecturer, *Privacy as Knowledge Commons Governance*, EOAR (Enabling Openness in Australian Stem Cell Research) Seminar, February 28, 2023

Invited Lecturer, *Explainability*, AI and Law Bridge Program, Association for the Advancement of Artificial Intelligence, Washington, DC, February 8, 2023

Invited Lecturer, *Justifying Automated Decisionmaking Systems*, Algorithms // A Brave New World? Series, University of Frankfurt, January 25, 2023

Program Committee and Commentator, Northeast Privacy Scholars Conference, NYU, November 11, 2022

Panelist, *Big Data Consumer Class Actions: A Problem in Need of a Solution or a Solution in Need of a Problem?* ABA Class Actions and Mass Torts Regional CLE Program, Chicago, IL , June 17, 2022

Program Committee and Moderator, Open and User Innovation Conference, June 21-22, 2022

Invited Participant, Penn Symposium on Innovation and Criminal Justice, January 28, 2022

Commentator, ABA Next Generation of Antitrust, Data Privacy and Data Protection Scholars, NYU, January 28, 2022

Moderator, The Next Wave of Corporate Enforcement, NYU, November 5, 2021

Panelist, Scoping Tech Accountability, Power and Accountability in Tech, UCLA, November 5, 2021

Co-Organizer, Beyond Facial Recognition: Our Biometric Future, NYU, October 5-6, 2021

Program Committee and Co-Author, Open and User Innovation Conference, June 21-22, 2021

IASC Knowledge Commons Conference, June 9-11, 2021

Privacy Law Scholars Conference, June 3-4, 2021

Faculty Workshop, Duke Law School, November 18, 2020

The Physics of the Law: Legal Systems Through the Prism of Complexity Science, November 12-13, 2020

Algorithm Design, Law, and Policy Virtual Kick-Off, Simons Institute, July 20 -21, 2020

Workshop on Frameworks for Integrative Data Systems (FIDES) and Foundations of Responsible Data Science (FORDS), March 25-26, 2020

2020 Social Innovation Symposium, NYU, February 28, 2020

2020 Next Generation of Antitrust, Data Privacy and Data Protection Scholars Conference, NYU School of Law, January 31, 2020

Penn Law and Innovation Symposium, University of Pennsylvania Law School, January 24, 2020

Mind Bytes 2019: Research Computing Symposium and Expo, University of Chicago, November 5, 2019

Law, Economics and Politics Colloquium, NYU School of Law, September 3, 2019

Workshop on the Ostrom Workshop, University of Indiana, Bloomington, June 22, 2019

Privacy Law Scholars Conference, UC Berkeley, May 30-31, 2019

Common Law for the Age of AI Symposium, Columbia Law School, April 5, 2019

Innovation Policy Colloquium, NYU School of Law, April 4, 2019

Seminar and Academic Roundtable, Microsoft Corporation, March 21-22, 2019

Seminar, Wharton Legal Studies & Business Ethics Department, March 14, 2019

Ohio State University Faculty Workshop**,** February 21, 2019

Privacy and Economics Workshop**,** University of Arizona, December 7, 2018

Artificial Intelligence in a Democratic Society, Panel on Automation in Daily Life (moderator), Trade Secrecy and Algorithmic Systems**,** NYU Center on Civil Justice, November 16-17, 2018

Programming Governance / Governing Programming: Regulatory Challenges on the Edge of Technology, McGill University Faculty of Law, November 4, 2018

Workshop on Privacy as Commons Governance**,** Villanova School of Law, October 12-13, 2018

Legal Implications of the Platform Economy**,** Zicklin School of Business, Baruch College, CUNY, October 3, 2018

Panel: Privacy v. Benefit: The Trade-off between Consumer Privacy and the Benefits Provided through Big Data**,** NYU JLI/ILB Conference, October 2, 2018

Workshop on Collective Behavior, Social Media, and Systemic Risk**,** Princeton University Friday-Saturday, August 17-18, 2018

Privacy Law Scholars Conference**,** George Washington University School of Law, May 30-31, 2018 (two co-authored presentations)

Workshop on Algorithmic Discrimination**,** University of Oxford Faculty of Law, April 24, 2018

Seminar @ Cornell Tech, Cornell Tech-NYC, February 12, 2018

Keynote Speaker, 2nd TILEC Conference on "Competition, Standardization, and Innovation**",** Tilburg University, Netherlands, December 18-19, 2017

Workshop on Technical Applications of Contextual Integrity**,** Center for Information Technology Policy, Princeton University, December 11, 2017

Commentator, After the Digital Tornado**,** The Wharton School, University of Pennsylvania, November 17-18, 2017

Governing Medical Commons Book Presentation**,** New York University School of Law, October 26, 2017

Seminar, Max Planck Institute for Software Systems**,** Saarbruecken, Germany, July 6, 2017

Fifteenth Annual Open and User Innovation Conference, University of Innsbruck, Austria, July 9-13, 2017

Privacy Law Scholars Conference**,** UC Berkeley Boalt School of Law, June 1-2, 2017 (three co-authored presentations)

Commentator, Design 2 Conference**,** New York University School of Law, May 11, 2017

Algorithms and Explanations, Information Law Institute, New York University School of Law, April 27-28, 2017

Distinguished Lecture Series: Users, Patents and Innovation Policy, Center for Intellectual Property Center for Intellectual Property Law and Innovation, Indiana University McKinney School of Law, Indianapolis, IN, April 10, 2017

Commentator, International Intellectual Property Roundtable, New York University School of Law, New York, NY, April 7-8, 2017

Predictive Analytics, Law and Policy: Mapping the Terrain, Ohio State University Moritz College of Law, Columbus, OH, March 24, 2017

Commentator, Patent Scholars Roundtable II, sponsored by Vanderbilt Law School, Atlanta, GA, February 3, 2017

Commentator, Seventh Annual Tri-State Region IP Workshop, NYU School of Law, New York, NY, January 13, 2017

IEEE Workshop on The Human Use of Machine Learning, European Centre for Living Technology, Venice, Italy, December 16, 2016

Bridges II: The Law-STEM Alliance & Next Generation Innovation, Northwestern Pritzker School of Law, Friday, October 28, 2016

Privacy Law Scholars Conference, George Washington University, June 2-3, 2016

Gruter Institute Conference on Innovation in Institutions, Squaw Valley, CA, May 23-27, 2016

Commentator, Patent Scholars Roundtable I, sponsored by Vanderbilt Law School, Atlanta, GA, February 12, 2016

Colloquium in Legal, Political, and Social Philosophy, NYU School of Law, New York, NY, November 19, 2015

IP Scholars Conference, DePaul University College of Law, Chicago, IL, August 6-7, 2015

Symposium on Access to Data in the Cloud, New York University School of Law, May 26-27, 2015 (Co-organizer)

Commentator, American Law and Economics Association Annual Meeting, Columbia University Law School, May 15, 2015

IP Theory Colloquium, An Institutional Approach to Patentable Subject Matter, Loyola Law School, Los Angeles, April 13, 2015

109th Annual American Society of International Law Meeting, The Right to Privacy in the Digital Age, Washington, DC, Apr. 8-11, 2015

Intellectual Property and the Public Domain – Results and Perspectives, Beyreuth University, Bayreuth, Germany, Feb. 6-7, 2015

3D Printing and Beyond Seminar: Emerging IP Issues with 3D Printing and Additive Manufacturing, Cardozo Law School, Feb. 2, 2015

Commentator, Tri-State Region IP Workshop, New York University School of Law, January 9, 2015

Third Annual Patent Colloquium, University of Toronto Faculty of Law, November 21, 2014

Empirical IP Research Conference, New York University School of Law, October 24-25, 2014 (Co-organizer)

Commentator, MSU Junior Scholars in Intellectual Property Workshop, MSU Law, October 17-18, 2014

Blouin Creative Leadership Summit: Business Innovation – Rethinking Organizational Design and Culture, New York, NY, September 23-24, 2014

2nd Thematic Conference on Knowledge Commons: Governing Pooled Knowledge Resources, International Association for the Study of the Commons, New York University School of Law, September 5-6, 2014 (Co-organizer)

Personalized Medicine and Intellectual Property Conference, Boston University School of Law, August 25, 2014

12th Annual Open and User Innovation Workshop, Harvard Business School, July 28-30, 2014

Workshop on the Ostrom Workshop – WOW 5, University of Indiana, June 18-21, 2014

Workshop on Medical User Innovation and Medical Knowledge Commons, New York University School of Law, May 15-17, 2014 (organizer)

Smart Law for Smart Cities, Fordham Law School, February 27-28, 2014

Patents 101: Eligibility from Computer Code to Genetic Code, Vanderbilt Law School, January 24, 2014

Thomson Reuters Speaker Series, Information Society Project, Yale Law School, November 14, 2013

Expectations and Guarantees: Privacy vs. 1st Amendment Roundtable, Drones & Aerial Robotics Conference, New York University School of Law, October 11-13, 2013

Open and User Innovation Workshop, University of Brighton, Brighton, UK, July 15-17, 2013

Faculty Workshop, Hebrew University Faculty of Law, June 12, 2013

Law and Technology Seminar, Hebrew University Faculty of Law, June 6, 2013

Design Patents in the Modern World Conference, Stanford Law School, April 6, 2013 (with Mark McKenna)

Faculty Workshop, Suffolk University School of Law, January 24, 2013

Program of the Intellectual Property Section, AALS Annual Meeting, New Orleans, January 6, 2013

Frontiers of Consumer Protection Symposium, University of Chicago Legal Forum, November 2, 2012

Ostrom Workshop in Political Theory and Policy Analysis, Indiana University, October 1, 2012 (with Brett Frischmann)

IP in Motion, 7th Annual Conference of the EPIP Association, University of Leuven, Belgium, September 27-28, 2012

Seminar, Católica Lisbon School of Business & Economics, Lisbon, Portugal, September 24, 2012

Global Thematic Conference on the Knowledge Commons, International Association for the Study of the Commons, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, September 12-14, 2012

Open and User Innovation Workshop, Harvard Business School July 30-August 1, 2012

Privacy Law Scholars Conference, George Washington University School of Law, June 7-8, 2012 (commentator)

Houston Law Center Institute for Intellectual Property & Information Law Conference, Santa Fe, New Mexico, June 2012

Gruter Institute Annual Conference on Innovation, Growth, and Human Behavior, Squaw Valley, California, May 21-22, 2012

PatCon, Boston College Law School, May 11, 2012

Anonymity and Identity in the Information Age, Cardozo Law School, April 4, 2012 (commentator)

IP at the Edge Workshop, Columbia Law School, April 13, 2012

NYU/Princeton Conference on Mobile and Location Privacy, NYU School of Law, April 12, 2012 (co-organizer)

Faculty Workshop, Washington University School of Law, April 11, 2012

13th Congress of the European Intellectual Property Institutes Network, Max Planck Institute, Munich, Germany, February 2-5, 2012

Faculty Workshop, Seton Hall Law School, October 24, 2011

Convening Cultural Commons, New York University School of Law, September 23-24, 2011 (co-organizer and presenter)

Privacy Law Scholars Conference, UC Berkeley, June 2-3, 2011 (commentator)

Panelist, The Many Forms of Commons: Regulation and Incentivization of Creativity on the Margins of IP, Law and Society Association Annual Meeting, San Francisco, California, June 4, 2011

Gruter Institute Annual Conference on Innovation, Growth, and Human Behavior, Squaw Valley, California, May 25-27, 2011

Platforms and Power Roundtable, New York University School of Law, May 6, 2011 (co-organizer)

Some Modest Proposals 4.0: A Conference About Pouring Academic Ideas into Legislative Bottles, Cardozo Law School, April 8, 2011

Symposium on Mobile Devices, Location Technologies and Shifting Values, Fordham University School of Law, March 25, 2011

IP Speaker Series, Cardozo Law School, March 2, 2011

Patent Unrest Symposium, Vanderbilt University Law School, February 24, 2011

Second Annual Research Roundtable on Empirical Studies of Patent Litigation, Northwestern University School of Law, November 18-19, 2010

38th Research Conference on Communication, Information and Internet Policy (TPRC), George Mason University School of Law, October 1-2, 2010 (program committee)

Patent Scope Revisited, Indiana University Maurer School of Law, September 23-24, 2010

Edward D. Manzo Scholar, DePaul University College of Law, September 1, 2010

Open and User Innovation Workshop, MIT Sloan School of Management, August 2-4, 2010 (collaborative work with Christiana Iyasere, Harold Demonaco, and Eric von Hippel presented by Christiana Iyasere)

IP Workshop: Communication of Technical Knowledge, Boston University School of Law, June 17-18, 2010

Privacy Law Scholars Conference, George Washington University School of Law, June 3-4, 2010 (commentator)

User and Open Innovation: How Should Intellectual Property Law Respond? NYU Engelberg Center on Innovation Law and Policy and UC Berkeley Center for Law & Technology, St. Helena, CA, May 28-29, 2010 (co-organizer)

Workshop on Computational Political Science and Legal Studies, Center for Complex Systems Studies, Kalamazoo College, March 5, 2010

Access to Knowledge 4, Yale Law School, February 11-13, 2010

Bend or Break: Tailoring the Patent System to Promote Innovation, UC Irvine School of Law, January 22, 2010

Research Roundtable on Empirical Studies of Patent Litigation, Searle Center on Law, Regulation, and Economic Growth, Northwestern Law, November 12-13, 2009 (commentator)

Workshop & Lecture Series on the Law & Economics of Intellectual Property, ETH Zurich, October 27-28, 2009

Research Roundtable on Laws of Creation: Property Rights in The World of Ideas, Searle Center on Law, Regulation, and Economic Growth, Northwestern Law, October 22-23, 2009 (participant)

Cyberlaw 2.0: Legal Challenges of an Evolving Internet, DePaul University College of Law, October 15-16, 2009 (commentator)

Workshop on Federal Privacy Legislation, NYU School of Law, October 2, 2009 (co-organizer)

37th Research Conference on Communication, Information and Internet Policy (TPRC), George Mason University School of Law, September 25-27, 2009 (program committee)

Workshop on Intellectual Property Law and Open & User Innovation, MIT Sloan School of Management, May 18-19, 2009 (presenter and co-organizer)

Enough is Enough!: Ceilings on Intellectual Property Rights, New York University School of Law, May 1-2, 2009

Faculty Workshop, University of Southern California School of Law, April 20, 2009

Junior Scholars in IP 2009, Michigan State University College of Law, March 26-28, 2009 (commentator)

Workshop on Trade Secrecy, NYU Engelberg Center, February 20-21, 2009 (co-organizer)

Wharton Business School Impact Conference: Information Security Best Practices 2009, January 29-30, 2009

Wharton Business School Impact Conference: Modeling Social Network Data, January 28-29, 2009

Faculty Workshop, University of Minnesota Law School, December 10, 2008

Faculty Workshop, George Washington University School of Law, November 20, 2008

Faculty Workshop, Fordham University School of Law, November 6, 2008

Yale Information Society Project Fall Speaker Series, November 4, 2008

Fordham Law Review Symposium: When Worlds Collide: Intellectual Property Laws at the Interface Between Systems of Knowledge Creation, Fordham University School of Law, October 31-November 1, 2008 (presenter and co-organizer)

North Carolina Law Review Symposium, October 24-25, 2008

36th Research Conference on Communication, Information and Internet Policy, George Mason University School of Law, September 26 – 28, 2008

Intellectual Property Scholars Conference, Stanford University, August 7-8, 2008

User and Open Innovation Workshop, Harvard Business School, August 4-6, 2008

International Association for the Study of Commons Conference, Cheltenham, England, July 14-18, 2008 (co-author of peer-reviewed paper with Brett Frischmann and Michael Madison)

Privacy Law Scholars Conference, George Washington University Law School, June 12-13, 2008 (commentator)

Conference on Education, Culture and the Knowledge Economy, University of Toronto, Canada, June 6, 2008

Conference on Science and Technology Studies and Intellectual Property Law, St. Helena, CA, March 9-10, 2009

Workshop on IP Without IP, Radcliffe Institute for Advanced Study, May 2-3, 2008

Granular and Multiphase Flows Colloquium, New Jersey Institute of Technology, April 28, 2008

Information Technology and Society Colloquium, New York University, April 25, 2008

Annual Conference on Intellectual Property Law and Policy, Fordham University, March 27-28, 2008, remarks published at 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 925 (2009)

NYU-Capetown Workshop on Global Administrative Law, University of Capetown, South Africa, March 18-20, 2008

Ignoring the Norm: A Way to Deal with Unacceptable Norms in Science?, Centre for Intellectual Property Rights, Catholic University of Leuven, Belgium, March 7, 2008 (keynote lecturer)

Advanced Patent Law Seminar, Temple University School of Law, March 4, 2008

Faculty Workshop, New York University School of Law, February 4, 2008

Conference on Empirical Legal Studies, New York University Law School, November 8-9, 2007 (commentator)

Lewis and Clark Business Law Forum: Nonobviousness -- the Shape of Things to Come, Lewis and Clark Law School, October 5-6, 2007

Intellectual Property Scholars Conference, DePaul University College of Law, August 9-10, 2007

User Innovation Conference 2007, Copenhagen Business School, Copenhagen, Denmark, June 27-28, 2007

Research Seminar: Law, Society and Technology, Haifa University, June 14, 2007

Working Within the Boundaries of Intellectual Property, Conference of the NYU Engelberg Center on Innovation Law and Policy, La Pietra, Italy, June 5-6, 2007

What Ifs and Other Alternative Intellectual Property and Cyberlaw Stories, Michigan State University, March 30-31, 2007

March Meeting, American Physical Society, March 5-9, 2007 (with Jan Tobochnik, Gábor Csárdi, László Zalányi, Péter Érdi)

Networks Seminar, University of Michigan, February 22, 2007

Intellectual Property Colloquium, University of Michigan Law School, February 21, 2007

Modest Proposals IP/IT 3.0, Benjamin N. Cardozo School of Law, February 20, 2007 (commentator)

Faculty Workshop, Northwestern University Law School, February 15, 2007

Faculty Workshop, Santa Clara University Law School, February 2, 2007

Faculty Workshop, Fordham University School of Law, January 30, 2007

Information Security Economics Workshop, Center for Discrete Mathematics and Theoretical Computer Science, Rutgers University, January 18-19, 2007

Faculty Workshop, Emory Law School, December 15, 2006

Symposium on Patent Policy in the Supreme Court and Congress, Santa Clara University High Tech Law Institute and Berkeley Center for Law and Technology, October 27, 2006

Intellectual Property Scholars Conference, Boalt Hall School of Law, University of California, Berkeley, August 10-11, 2006

AALS Workshop on Intellectual Property Law, Panel on the Politics of Patent Reform, Vancouver, Canada, June 14-16, 2006

AALS Workshop on Intellectual Property Law, Discussion Session on the Fourth Amendment and Privacy, Vancouver, Canada, June 14-16, 2006 (moderator)

NetSci 2006 International Workshop on Network Science, Indiana University, May 22-25, 2006

Princeton University-Microsoft Intellectual Property Conference, Princeton University, May 18-20, 2006

Innovation Policy Colloquium, New York University College of Law, March 30, 2006

Law and Economics Workshop, Boston University College of Law, March 20, 2006

7th Annual CIPLIT® Symposium: Patents and Progress: Reflections in the Midst of Change, March 15-16, 2007 (co-organizer)

March Meeting American Physical Society, March 16, 2006 (with Jan Tobochnik, Gábor Csárdi, László Zalányi, Péter Érdi,)

Law in the Age of Networks: Implications of Network Science for Legal Analysis Symposium, University of Illinois College of Law, March 10, 2006 (presenter and organizer)

Colloquium on Technology, Innovation, and Intellectual Property Policy, University of Arizona Law School, November 14, 2005

Faculty Workshop, University of Illinois College of Law, October 19, 2005

Symposium on Innovation and its Discontents: Patents and Innovation Policy in the 21st Century, John Marshall Law School, October 14, 2005

Midwest Law and Economics Association, October 14-15, 2005

2005 Technology Transfer Society (T2S) Meeting, Kauffman Foundation, September 28-30, 2005 (with Patrick L. Jones)

IP Scholars Conference, Cardozo Law School, August 11-12, 2005

Panel on Patents and Their Sociolegal Futures, Law and Society Association, June 2-5, 2005

W(h)ither the Middleman: The Role and Future of Intermediaries in the Information Age, Michigan State University Law School, April 7-9, 2005

Faculty Workshop, Loyola Law School Los Angeles, March 28, 2005

March Meeting, American Physical Society, March 21-25, 2005 (with Gábor Csárdi, Jan Tobochnik, László Zalányi, and Péter Érdi)

Modest Proposals IP/IT 2.0, Benjamin N. Cardozo School of Law, February 24-25, 2005 (commentator)

Colloquium on University Technology Transfer and Entrepreneurship, Karl Eller Center, University of Arizona, January 20-23, 2005

Symposium on Complexity and Advanced Analytics Applied to Business, Government and Public Policy, University of Michigan-Dearborn Center for Study of Complex Systems, October 23, 2004 (with Gábor Csárdi, Jan Tobochnik, Péter Érdi)

Intellectual Property Speaker Series, Benjamin N. Cardozo School of Law, October 21, 2004

Symposium on Privacy and Identity: The Promise and Perils of a Technological Age, DePaul University College of Law and School of Computer Science, Telecommunications, and Information Systems, October 14-15, 2004 (presenter and co-organizer)

Works in Progress in Intellectual Property Law Conference, Boston University, September 10-11, 2004

Intellectual Property Scholars Conference, DePaul University College of Law, August 2-3, 2004

Privacy, Information, and Speech Panel, Law and Society Association, May 27-30, 2004

Henry R. Luce Lecturer on Networks, Laws, Actors, Center for Complex Systems Studies, Kalamazoo College, May 19, 2004

Some Modest Proposals: A Conference About Pouring Academic Ideas into Legislative Bottles, Benjamin N. Cardozo School of Law, March 14-15, 2004

Intellectual Property & Communications Law and Policy Scholars Roundtable, Michigan State University DCL College of Law, February 20-21, 2004

Works-in-Progress Intellectual Property Colloquium, Tulane Law School, October 17-18, 2003

AMICUS BRIEFS, POLICY ENGAGEMENT AND SERVICE

New York Area Working Group on Trade Secrecy and Forensic Technology (ongoing)

Advisory Board, Patient Innovation (ongoing)

Program Committee, Northeast Privacy Scholars Workshop (ongoing)

Presenter, Privacy Regulation and Innovation Policy, California Courts of Appeal Judicial Education, December 7, 2021

Panelist, Artificial Intelligence (AI) and the Law: Ethical Considerations and Its Impact on the Future of the Practice of Law, New York County Lawyers Association CLE, May 12, 2021

Panelist, Advancing Commercialization from Federal Labs, National Academies of Science, Engineering and Medicine, March 2, 2020

Program Committee, ACM Conference on Fairness, Accountability, and Transparency (2017, 2018)

Panelist, 2016 IP Institute, Cravath, Swaine and Moore, November 29, 2018

Co-Organizer (with Hila Lifshitz-Assaf), 2018 Open and User Innovation Conference, August 6-8, 2018

Co-Convenor (with Ignacio Cofone and John Nay), Economics and Data Science in Conversation about Algorithms Roundtable, NYU School of Law, June 11, 2018

Panelist, Powering Change: Women in Innovation and Creativity, World Intellectual Property Day, Licensing Executives Society, April 25, 2018

Presenter, INGRES Zurich IP Retreat 2017 "The Hindsight Bias in Patent Law", September 8-9, 2017

Panelist, A Road-Map to Transform the Structure and Accessible Use of Data for High Impact Program Management, Policy Development, and Scholarship, National Press Club, Washington, DC, January 23, 2017

Panelist, IV Arnold Workshop on Reproducibility and Transparency in Research, AAAS, Washington, DC, October 24, 2016

Panelist, Policing and Accountability in the Digital Age, Brennan Center for Justice and Policing Project, NYU School of Law, New York, NY, September 15, 2016

Retreat on Cybersecurity, NYU, New York, NY, September 11, 2016

Tyranny of the Algorithm? Predictive Analytics & Human Rights, Bernstein Institute for Human Rights, New York, NY, March 21-22, 2016

National and International Intellectual Property Practices and Policies: Assessing the Impact of Political, Economic and Technological Pressures, National Academies of Sciences, Washington, DC, December 11, 2015

4th Annual Privacy Law Salon: Policymaker Roundtable, George Washington University School of Law, Washington, DC, September 10-11, 2015

Workshop on Privacy for the Intelligence Community: Emerging Technologies, Academic and Industry Research and Best Practices, National Academies of Sciences, Washington, DC, July 21-22, 2015

Public Meeting on Executive Order 12333, Panel on First and Fourth Amendment Implications of EO 12333 Activities: The Impact of New Technologies, National Constitution Center, Philadelphia, PA, May 13, 2015

Panel on Cloud Data Access: A Transnational Perspective, New York University School of Law, Mar. 13, 2015

MIT Innovation Lab, Sloan School of Management, Cambridge, MA, November 13-14, 2014

Principal Author, Law Professor Amicus Brief, *In re National Security Letter*, Nos. 13-15957 & 13-16731, Ninth Circuit Court of Appeals, April 14, 2014

MIT Innovation Lab, Sloan School of Management, Cambridge, MA, November 4-5, 2013

Gene and Diagnostic Patents at the Interface between Industry, Academia, and Medical Practice, Patenting in the Life Sciences Symposium, Cold Spring Harbor Laboratory, March 10-13, 2013

Counsel of Record, Amicus Brief on the Merits on behalf of the American College of Medical Genetics et al., *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, No. 10-1150, Supreme Court of the United States, September 9, 2011

Counsel of Record, Amicus Brief on Petition for Certiorari on behalf of the American College of Medical Genetics et al., *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, No. 09-490, Supreme Court of the United States, April 20, 2011

Consumer Federation of America Cloud Computing Retreat, New York University School of Law, June 21-22, 2010 (participant), (Retreat report available at www.consumerfed.org/pdfs/Cloud-report-2010.pdf

Designing the Microbial Research Commons: An International Symposium, National Academy of Sciences, Washington, DC, October 8-9, 2009

Counsel of Record, Amicus Brief on behalf of the American Medical Association et al., *Bilski v. Kappos*, No. 08-964, Supreme Court of the United States, October 2, 2009

Co-Author, Amicus Brief on Petition for Certiorari on behalf of AARP, Patients Not Patents, and the Public Patent Foundation, *Apotex, Inc. v. Sanofi-Synthelabo*, No. 09-117, Supreme Court of the United States, August 27, 2009

Counsel of Record, Amicus Brief on behalf of the American College of Medical Genetics et al., *Prometheus Laboratories, Inc. v. Mayo Collaborative Services*, No. 2008-1403, Federal Circuit Court of Appeals, April 6, 2009

Chair and Chair-Elect, AALS Section on Intellectual Property Law, 2009-10 (successful proposal for Mid-Year Meeting of the Intellectual Property, Internet and Computer Law, and Biolaw Sections in 2012)

Current Issues in Patentable Subject Matter, Connecticut Intellectual Property Law Association, May 14, 2008

Lesson Author, Patent Law, Center for Computer-Assisted Legal Instruction (2007-08)

Patent Law After *KSR v. Teleflex*: Are Your Patents Still Valid?, ABA-CLE Teleconference, May 31, 2007

KSR v. Teleflex: Obviousness: On Point, Obfuscated, Outdated or Out of Hand, AIPLA Spring Meeting, Boston, MA, May 9-11, 2007

Current and Future Trends in Patent Law Symposium, Suffolk University Law School, April 20, 2007

Topics in Cyberlaw, Intellectual Property Law Ass'n of Chicago, January 24, 2007

Recent Developments in Intellectual Property Law - A Global Perspective, Association of Patent Law Firms, September 21, 2006

Principal Co-Author, Law Professor Amicus Brief on the Merits, *KSR International Co. v. Teleflex, Inc.*, No. 04-1350, Supreme Court of the United States ((with Joseph Miller), August 22, 2006

Seventh Annual Institute on Privacy Law: New Developments & Compliance Issues in a Security Conscious World, Practicing Law Institute, July 17-18, 2006 (faculty member, chapter in textbook co-authored with Douglas Burda)

Current Issues in Cyberlaw, McAndrews, Held, and Malloy, Chicago, April 13, 2006

Use of Patented Subject Matter in Research, Lab to Market: Building Sound Patent Practices, University of Buffalo, May 17, 2005

Principal Co-Author, Law Professor Amicus Brief on Petition for Certiorari, *KSR International Co. v. Teleflex, Inc.*, No. 04-1350, Supreme Court of the United States (with Robert Brauneis), May 12, 2005

Counsel of Record, Law Professor Amicus Brief, *Merck KGaA v. Integra Lifesciences I, Ltd et al.*, No. 03-1237, Supreme Court of the United States (with Rochelle Cooper Dreyfuss, John F. Duffy, Arti K. Rai), February 22, 2005

Katherine J. Strandburg, *Restating the Obvious: The Federal Circuit Has Gone Too Far with Its Standard for Finding Nonobviousness*, 3 IP LAW & BUSINESS 34 (October 28, 2005)

Privacy Task Force, Chicago Bar Association, Summer 2005.

Panel on Implications of Federal Circuit Knorr-Bremse En Banc Decision, Intellectual Property Law Association of Chicago, October 28, 2004

Working Group on Developing a Research Exemption to Intellectual Property Protections, American Association for the Advancement of Science, October 2004

Amicus Committee, Federal Circuit Bar Association, June 2003 –April 2013

The Internet - A Great Frontier for Free Speech or Orwellian Control over the Marketplace of Ideas?, We the People: The State of the First Amendment in 2004, KAM Isaiah Israel Congregation, Chicago, February 27-29, 2004

Is Patenting Business Methods Patently Absurd?, IP Law Week, Northwestern University Law School, April 15, 2003

Cyber-Liberties: How Much Government Surveillance is Too Much?, Northwestern University Law School, January 29, 2003

Trademark Trial Advocacy Workshop, International Trademark Association, July 2000

APPENDIX: SCIENTIFIC PUBLICATIONS (1983-1992)

BOND-ORIENTATIONAL ORDER IN CONDENSED MATTER PHYSICS
Springer-Verlag (New York, 1992). K.J. Strandburg, editor.

Monte Carlo simulations of the Curie temperature of ultrathin ferromagnetic films.
K.J. Strandburg, D.W. Hall, C. Liu, S.D. Bader
Physical Review B 46, 10818-10821

Phase transitions in dilute, locally connected neural networks
K.J. Strandburg, M.A. Peshkin, D.F. Boyd, C. Chambers and B. O'Keefe
Physical Review A 45, 6135-6138 (1992)

First-order melting transition of the hard-disk system
J. Lee and K.J. Strandburg
Physical Review B 46, 10818-10821 (1992)

Roughening of two-dimensional quasicrystals: A study on the Penrose tiling
A. Garg, M. Shin and K.J. Strandburg
Physical Review B 46, 769-786 (1992)

Critical fields of Josephson-coupled superconducting multilayers
J. Garner, M. Spanbauer, R. Benedek, K.J. Strandburg, S. Wright and P. Plassman
Physical Review B 45, 7973-7983 (1992)

Entropic predictions for cellular networks
M.A. Peshkin, K.J. Strandburg and N. Rivier
Physical Review Letters 67, 1803-1806 (1991)

Quasicrystals and Aperiodic Tilings
K.J. Strandburg
Computers in Physics (Sep./Oct. 1991)

Entropy of a three-dimensional random-tiling quasicrystal
K.J. Strandburg
Physical Review B 44, 4644-4646 (1991)

Random-tiling quasicrystal
K.J. Strandburg
Physical Review B 41, 2469-2478 (1990)

Thermodynamic behavior of a Penrose-tiling quasicrystal
K.J. Strandburg and P.R. Dressel
Physical Review B 41, 2469-2478 (1990)

Phason elasticity in entropic quasicrystals
K.J. Strandburg, L. Tang and M.V. Jaric
Physical Review Letters 63, 314-317 (1989)

Two-dimensional melting
K.J. Strandburg
Reviews of Modern Physics 60, 161 (1988)

Why the Brazil nuts are on top: Size segregation of particulate matter by shaking
A. Rosato, K.J. Strandburg, F. Prinz and R.H. Swendsen
Physical Review Letters 58, 1038-1040 (1987)

Monte Carlo renormalization-group study of the discrete Gaussian model
K.J. Strandburg
Physical Review B 35, 7161-7163 (1987)

Quasicrystal equilibrium state
M. Widom, K.J. Strandburg and R.H. Swendsen
Physical Review Letters 58, 706-709 (1987)

Crossover from a hexatic phase to a single first-order transition in a Laplacian roughening model for two-dimensional melting
K.J. Strandburg
Physical Review B 34, 3536-3539 (1986)

Comment on "Two-dimensional pressure of 4He monolayers: First-order melting of the incommensurate solid"
K.J. Strandburg, R.M. Suter, N.J. Colella, P.M. Horn, S.A. Solla, R.J. Birgeneau, S.G.J. Mochrie, K.L. D'Amico and D.E. Moncton
Physical Review Letters 55, 2226 (1985)

Bond-angular order in two-dimensional Lennard-Jones and hard-disk systems
K.J. Strandburg, J.A. Zollweg, and G.V. Chester
Physical Review B 30, 2755 (1984)

Monte Carlo studies of a Laplacian roughening model for two-dimensional melting
K.J. Strandburg, S.A. Solla, and G.V. Chester
Physical Review B 28, 2717 (1983)

Exhibit R

Privacy Rights Clearinghouse

October 5, 2023

Privacy Rights Clearinghouse *Cy Pres* Award Proposal:
In re Google Location History Litigation

Thank you for inviting Privacy Rights Clearinghouse to submit a *cy pres* award proposal in the *In re Google Location History Litigation* settlement. Please see the information below regarding our organization, grant proposal, and commitment to evaluating the success of any project funded by a *cy pres* award.

Organization Information

Privacy Rights Clearinghouse (PRC) is an independent 501(c)(3) nonprofit organization. Our mission is to increase access to information, policy discussions, and meaningful rights so that data privacy can be a reality for everyone.

History

Privacy Rights Clearinghouse was one of the first, and remains one of few, organizations focused exclusively on consumer privacy rights and issues. The organization serves as a longstanding leader in data privacy education and advocacy.

From our founding in 1992 until 1996, PRC was a program of the University of San Diego School of Law's Center for Public Interest Law. Our team operated a telephone help hotline and published printed educational fact sheets—assisting tens of thousands of individuals.

From 1996 until 2014, PRC was a fiscally sponsored program of the Utility Consumers' Action Network. We launched and built out our widely-recognized educational website (privacyrights.org) with detailed content covering laws, rights, and issues as they emerged in response to technological and societal changes. Our founder, Beth Givens, was among the first advocates to raise public awareness of identity theft and create a program to provide direct victim assistance. She also recognized the impact of corporate data practices on individuals' lives and began tracking data breaches in 2005. Our Data Breach Chronology project has informed the work of advocates, researchers, and policymakers for almost two decades.

In 2014, PRC became an independent 501(c)(3) nonprofit organization. Our team developed an online consumer complaint center to better inform our education and advocacy priorities, published an early and widely cited report examining the privacy practices of health and fitness

apps, studied data broker privacy policies and practices, and has continued to serve as an expert voice in data privacy advocacy in California and nationally. To this day, PRC continues to adapt to the evolving privacy landscape and build upon our founding principles and body of work.

Current Goals

Privacy Rights Clearinghouse was founded on the belief that people deserve the opportunity to be informed of their rights and be heard by those who represent them. This continues to serve as our team's motivation as we work toward a future where privacy rights are meaningful and accessible to all people, available choices are clear, and both are reflected in the products and services people use and interact with on a daily basis.

Current Programs

Consumer Education and Outreach

PRC increases access to understandable information and expands public understanding of existing data privacy rights and choices by

- Publishing clear overviews of complex data privacy laws
- Creating educational resources that provide context for rights and choices that lie at the intersection of data privacy and health, employment, finance, education, and housing
- Engaging in community outreach

Consumer and Policy Advocacy

PRC advocates to defend and advance consumer data privacy protections by

- Providing policy analysis and input at the state and national level, with a focus on agency proceedings
- Focusing strategic advocacy in California, a state that has long served as a driver of data privacy protections nationwide
- Coordinating advocates to enhance their public policy capacity for consumer data privacy issues that impact those they represent

Privacy Research Tools

PRC provides researchers, journalists, policymakers, and advocates with access to issue-relevant data and information to better and more efficiently understand data privacy issues by

- Building databases and interactive tools to help analyze the data
- Publishing reports analyzing emerging issues and trends

***Cy Pres* Awards**

Cy pres awards are a critical source of funding for our organization, and PRC is in a strong position to benefit the class in privacy-related settlements. We focus exclusively on consumer data privacy with no competing priority issues, and we accept funding only from sources that align with our mission.

Over the past decade, PRC has received the *cy pres* awards listed below.

2023

IN RE PLAID INC. PRIVACY LITIGATION, 4:20-cv-03056, (N.D. Cal.) Plaintiffs alleged that defendant used consumers' banking login credentials to harvest and sell detailed financial data without their consent. In October 2023, PRC will receive funds to support our programs.

In re Toll Roads Litigation, No. 8:16-00262-ODW (ADSx) (C. D. Cal.) Plaintiffs alleged that defendants improperly provided personally identifiable information to third parties in violation of California Streets and Highways Code § 31490. PRC will receive funds in October 2023.

2022

Larson v. Harman-Management Corp. Plaintiffs alleged that Harman sent unauthorized, automated text messages to class members' cell phones in violation of the Telephone Consumer Protection Act. PRC received $27,876.09 for general program support.

Bailey v. Great America LLC, d/b/a Six Flags Great America, No. 17 CH 1118 (19th Jud. Cir. Lake Cnty., Ill.) Plaintiffs alleged defendants violated the Fair and Accurate Credit Transactions Act. PRC received $584.80 for general program support.

2021

Vizio, Inc., Consumer Privacy Litigation, 8:16-ml-02693, (C.D. Cal.) Plaintiffs alleged that defendant violated the Video Privacy Protection Act. PRC received $12,357.80 and used the funds to publish educational materials.

Hashw v. Dep't Stores Nat'l Bank, No. 0:13-cv-00727-RHK-BRT (D. Minn.). Plaintiffs alleged that defendant violated the Telephone Consumer Protection Act. PRC received $136,371.03 for general program support.

Virgine v. CR England No. 1:19-cv-02011-SEB-MJD (S.D. Ind.) Plaintiffs alleged that defendant violated the Telephone Consumer Protection Act. PRC received $7,208.73 for general program support.

2020

Robert Cohen v. Foothill Eastern Transportation Corridor Agency, 8:15-cv-01698, (C.D. Cal.) Plaintiffs alleged that defendants violated the Fair Credit Reporting Act. PRC received $6,447.86 for general program support.

Simms v. ExactTarget LLC, No. 1:14-cv-00737-WTL-DKL (S.D. Ind.) Plaintiffs alleged that defendants violated the Telephone Consumer Protection Act. PRC received $27,624.43 for general program support.

Seegert v. P.F. Chang's China Bistro, Inc., et al, No. 37-2017-00016131-CU-MC-CTL (Cal. Super. Ct., San Diego Cnty.) Plaintiffs alleged that defendant violated the Song-Beverly Credit Card Act. PRC received $30,838.97 for general program support.

Johnson v. American Finance & Associates Corp and Does 1-50, Case No. 56-2013-00436494-CU-BT-VTA. PRC received $1,580.44 for general program support.

2019

In Re: Collecto, Inc., Telephone Consumer Protection Act (TCPA) Litigation, 1:14-md-02513, (D. Mass.) Plaintiffs alleged that defendant violated the Telephone Consumer Protection Act. PRC received $166,674 for general program support.

Gutierrez-Rodriguez v. R.M. Galicia, Inc., 3:16-cv-00182, (S.D. Cal.) Plaintiffs alleged that defendant violated the Telephone Consumer Protection Act. PRC received $33,119.42 for general program support.

Connolly v. Umpqua Bank, NO. 2:15-CV-00517-TSZ (U.S. Dist. Ct., W.D. Wash.) Plaintiffs alleged that Umpqua violated the Fair Credit Reporting Act. PRC received $10,409.67 to publish educational materials.

2018

Robinson v. Paramount Equity Mortgage, No. 2:14-cv-02359-TLN-CKD (U.S. Dist. Ct., E.D. Cal.) Plaintiffs alleged that Paramount Equity called individuals for marketing purposes without prior express written consent and called individuals registered on the Do Not Call Registry without prior consent. PRC received $411,014.67 for general program support.

Mount v. Wells Fargo Bank, N.A., No. BC395959 (Super. Ct. Cal., County of Los Angeles) Plaintiffs alleged that Wells Fargo illegally recorded customer service phone calls. PRC received $46,665.26 for general program support.

2016

People of Calif. v. Wells Fargo Bank, N.A., No. BC611105 (Super. Ct. Cal., County of Los Angeles) Wells Fargo settled claims brought by the California Attorney General and five other state regulators alleging that the bank failed to properly notify consumers that their phone calls were being recorded. PRC received $250,000.00 for general program support.

Stone v. Howard Johnson International Inc., No. 12-cv-01684 (U.S. Dist. Ct., C.D. Cal.) Plaintiffs alleged that Howard Johnson illegally recorded telephone calls without the consent of the caller. PRC received $54,557.49 for general program support.

Doe v. Twitter, No. CGC-10-503630 (Super. Ct. Cal., County of San Francisco) Plaintiffs alleged that Twitter violated users' privacy rights by disclosing full names of users without warning, sharing users' public Tweets and public profile information with third parties without adequate disclosure, and failing to adequately warn or instruct users that their Tweets would be public by default. PRC received $302,914.26 for general program support.

2015

The Digital Trust Foundation (created from settlement funds in an action concerning Facebook's "Beacon" program) funded projects and initiatives to "promote the cause of online privacy, safety, and security." PRC submitted a proposal and was awarded $275,000.00 to design and publish new educational materials, redesign the organization's website to improve usability, build outreach capacity, and hire a staff outreach coordinator.

Nicolucci v. Sephora USA, Inc., No. CGC-11-508450 (Super. Ct. Cal., County of San Francisco) Plaintiffs alleged that Sephora illegally collected customers' zip codes, putting consumers at risk of possible identity theft and fraud. PRC received $105,330.00 for general program support.

2014

In. re: Netflix Privacy Litigation, No. 5:11-cv-00379 (U.S. Dist. Ct., N.D. Cal.) Plaintiffs alleged that Netflix violated the Video Privacy Protection Act by storing the financial information and viewing history of former customers who had canceled their accounts. PRC received $175,558.50 to publish educational materials on mobile payment systems, mobile apps, data brokers, and location-based services.

Holmes v. NCO Financial Systems, Inc., No. 11-56969 (U.S. Ct. App., 9th Cir.) Plaintiffs alleged that NCO Financial Systems violated the Fair Debt Collection Practices Act by contacting individuals whose debts were contested. PRC received $20,924.06 for general program support.

2013

Syran v. LexisNexis Group, No. 05-cv-0909-LAB-KSC (U.S. Dist. Ct., S.D. Cal.) Plaintiffs alleged that LexisNexis violated various federal (including Fair Credit Reporting Act) and California (including California's Information Practices Act) statutes and common law rights when information about plaintiffs and other consumers was obtained by unauthorized persons. PRC received $172,805.75 for general program support.

Kaye et. al. v. Aesthera Corp, No. 3:09-cv-01947 (U.S. Dist. Ct., Conn.) Plaintiffs alleged that Aesthera sent unsolicited facsimile advertisements in violation of the Telephone Consumer Protection Act. PRC received $5,012.44 for general program support.

Wang v. Asset Acceptance, et. al., No. 09-4797 (U.S. Dist. Ct., N.D. Cal.) Plaintiffs alleged that Asset Acceptance violated the California Consumer Credit Report Agencies Act and the Fair Credit Reporting Act when it placed debts on plaintiffs' credit reports without reporting that the alleged debts were disputed. PRC received $130,025.39 for general program support.

Main et. al. v. Wal-Mart Stores, Inc., No.: 3:11-cv-01919-JSW (U.S. Dist. Ct., N.D. Cal.) Plaintiffs alleged that defendant violated the Song-Beverly Act. PRC received $368,512.50 for general program support.

Charity Navigator Rating

Privacy Rights Clearinghouse has been rated a four-star charity by Charity Navigator with a 97% rating.

Grant Proposal

Project Director

Meghan Land, Executive Director

Project Summary

The internet plays a role in nearly every aspect of people's daily lives in the U.S. Its ubiquity means that the internet not only affects people's privacy when they actively engage online, but it also influences how data is collected, shared, sold, and stored in ways that affect health, education, finances, safety, employment, and the ability to obtain housing in people's physical lives.

PRC promotes the protection and advancement of internet privacy through each of our programs. Generally speaking, our approach is to listen to people and those who represent them, identify patterns, research and analyze the issue and existing protections, inform people, and advocate where we see gaps. Our organization's work is intended to benefit U.S. consumers, and will specifically benefit the class and advance internet privacy by providing access to information about data privacy rights for individuals and the community organizations that serve them directly, creating data-privacy-centered resources to inform public policy and privacy research, and advancing access to privacy rights for all people.

With the funds requested, PRC will be able to accomplish the following over a three-year period. Please note that we are able to scale this proposal up or down depending on available *cy pres* funds.

1. **Enhance Educational Content and Outreach Capacity**

   a. *Expand and update published consumer education materials*

   All educational materials we publish on privacyrights.org are free and licensed under Creative Commons so they may be widely shared. They can stand alone (to provide brief answers to questions, for instance) or be used in combination with one another to create a custom or more comprehensive resource. With the funding requested, we will be able to accomplish the following over the course of three years.

   Privacy Law Overviews. Our goal is to have a consumer-focused overview of every U.S. privacy law available on our site by 2026. These overviews are intended to help advocates and direct service organizations, journalists, researchers, and interested individuals better understand existing data privacy rights. They require issue expertise, legal research, and continuous updating.

Common Data Privacy Q/A. We regularly publish common questions and answers we have received from individuals and their advocates over the years. These are intended to help those seeking a quick answer or starting point and are typically accessed by online search. Our goal is to have staff capacity to publish, update, and communicate these on a monthly basis.

Know Your Rights. We publish these to help people understand privacy rights in context. Our goal is to have staff capacity to publish one of these each month, and review for updates and accuracy on an annual basis.

Guides. These publications are intended to provide people with actionable instructions for exercising a privacy right or making a choice grounded in privacy rights. Our goal is to publish these in conjunction with the Privacy Law Overviews.

b. *Build outreach capacity*

We will expand our team to enhance community outreach capacity, allowing us to dedicate more resources to building strong relationships with community-based organizations. Our goal is to understand how internet-privacy-related issues affect individuals' lives and create helpful and actionable resources with the input of those who work with them directly.

In addition to new resources on privacyrights.org, deliverables may include presentations and custom content for community-based organizations on internet-related privacy issues, choices, rights that are important to the populations they serve.

c. *Improve website and content design and development*

We will improve our website accessibility and add translation capability and/or possibly create materials in additional languages and media formats.

2. Support and Enhance Consumer and Policy Advocacy

a. *Advocate for strong privacy protections and improved data practices*

In addition to our current work, funding will allow us to increase our capacity to analyze and weigh in on federal and state policy proceedings such as agency rulemakings and calls for comment. We will also expand our reach among advocates focusing on issues that intersect with data privacy to build issue understanding that helps drive positive change.

b. *Offer paid legal internships*

We maintain a competitive legal internship program and are committed to providing an experience that equips students with privacy law knowledge and consumer advocacy skills regardless of their career paths after law school. Funding will allow us to pay interns for their meaningful contributions rather than relying on course credit alone.

3. Improve Existing Research Tools and Create New Tools and Reports

A critical aspect of promoting consumer privacy, particularly with respect to internet privacy, is gaining a better understanding of how personal data is collected, stored, shared, and protected. Through this program, our team builds and maintains issue-relevant databases, creates interactive dashboards, and writes reports to inform the work of researchers, advocates, journalists, and policymakers to better understand data privacy and its impacts on individuals.

a. Maintain and improve PRC's Chronology of Data Breaches and Data Broker Directory, and possibly develop new tools and databases based on identified needs during the funding period

With the funding requested, we will create a data science fellowship or staff position (depending on funding received) to enhance these projects.

We prioritize issues surrounding data breach and data brokers (companies that collect and sell consumer data that is often generated online—such as geolocation data—without ever interacting with individuals). Both issues influence and are heavily influenced by internet privacy protections.

Our Chronology of Data Breaches provides information on reported consumer data breaches in the U.S. since 2005. It is the only publicly available resource of its kind. Since its relaunch in April 2023, the interactive dashboard has been accessed over 80,000 times and we have provided the underlying database to over 100 academic researchers.

Our Data Broker Directory will be redesigned and relaunched in early 2024, and provides information on data brokers that have registered in California and Vermont (the two states with registration requirements). The purpose of this resource is to take largely unusable registration information, and develop a resource that can be used to better understand the data broker industry and practices.

b. Publish new reports and update existing reports on an annual basis

We publish reports and comparative visual dashboards on various privacy laws and issues to help advocates and policymakers understand where strengths and gaps exist for consumers. We currently have consumer-focused reports on data breach notification laws and data broker registration, and we have a report in progress that

will analyze student data privacy protections in higher education focused on online courseware and digital instructional materials.

Funding will support annual updates to our existing reports as well as the legal, technical, communications, and design expertise needed to identify needs and generate new reports.

Project Funds Requested

We have outlined a proposal that we can easily scale up or down based on available *cy pres* funding. The amounts requested include all staff, contractors, services, and materials necessary to accomplish the work summarized above over the course of three years.

Program	Activity	Year 1	Year 2	Year 3	Total
Consumer Education and Outreach	Research, educational content publication	$115,000	$115,000	$115,000	$345,000
	Website and content design and development	$80,000	$40,000	$40,000	$160,000
	Community outreach and external communications	$55,000	$95,000	$95,000	$245,000
Consumer and Policy Advocacy	Policy research, analysis, advocacy	$115,000	$115,000	$115,000	$345,000
	Paid legal internship program	$35,000	$35,000	$35,000	$105,000
Research Tools and Reports	Database design, development, maintenance, and management	$100,000	$100,000	$100,000	$300,000
	Interactive dashboard design, creation, improvements, maintenance	$50,000	$50,000	$50,000	$150,000
	Report research, publication, communications	$100,000	$100,000	$100,000	$300,000
Total		$650,000	$650,000	$650,000	**$1,950,000**

Evaluation

If funded, Privacy Rights Clearinghouse will provide the Court and parties with a report every six months informing them of how any portion of the Settlement Fund has been used, of deliverables that have been completed, and how remaining funds will be used. We also plan to publish any written product we create as part of this proposal, and it is likely we would use at least one to form the basis of conference or community presentations.

We will continually evaluate our project and program success using a combination of quantitative and qualitative measures. We will

- design new or modified initiatives with input from the project's target audience or audiences to form a baseline against which to measure success;
- solicit formal feedback from target audiences annually and informal feedback on a more frequent basis, and include questions and discussion specific to internet privacy and the interests of the class; and
- measure the number of people we reach through various communications channels; people who might benefit from advocacy efforts; and researchers, policymakers, journalists, and advocates using our information and data to inform their published work.

Exhibit S

ROSE FOUNDATION FOR COMMUNITIES & THE ENVIRONMENT

201 4TH STREET, SUITE 102
OAKLAND, CALIFORNIA 94607
TELEPHONE 510.658.0702

October 3, 2023

Benjamin Berkowitz
Thomas E. Gorman
Christina Lee
Keker, Van Nest, and Peters LLP
633 Battery Street
San Francisco, CA 94111-1809

Tina Wolfson
Theodore Maya
Ahdoot & Wolfson, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505

Melissa Gardner
Michael Sobol
Lieff Cabraser Heimann & Bernstein, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339

Dear Counsel:

Re: Google Location History Litigation *Cy Pres* Proposal

The Rose Foundation for Communities and the Environment respectfully submits the following Cy *Pres* Recipient Proposal in accordance with the Plaintiffs' Motion for Preliminary Approval on September 14, 2023.

Sincerely,

Jodene Isaacs
Mitigation Funds Director
jisaacs@rosefdn.org

Tim Little
Executive Director
tlittle@rosefdn.org

The Rose Foundation for Communities and the Environment

Google Location History Litigation *Cy Pres* Proposal

Organization Information

1. Name of organization

Rose Foundation for Communities and the Environment (*hereinafter* 'Rose Foundation')

2. Discuss the founding and history of the organization.

Founded in 1992, Rose Foundation, a 501(c)3 Grantmaking Public Charity based in Oakland, California, supports grassroots initiatives that inspire community action to protect consumers, the environment and public health. Rose Foundation is built on the belief that people need to be involved in the decisions that affect their health, lives, families, and environment. We work towards a future where nature is protected, people's rights are ensured, and social and environmental justice is advanced. Building community capacity to enable robust participate in our nation's social and environmental decision making has been at the root of everything we have done since our launch 30 years ago. Our issues have ranged across a broad spectrum of consumer protection, conservation, health and social justice, and economic equity, and specific projects have included consumer rights education and advocacy, policy development around environmental sustainability and climate resilience, and grassroots advocacy for social and environmental justice. All of our programs embrace our overarching mission of fostering stewardship, building community, and demanding justice, and we achieve these goals by supporting initiatives that help communities more effectively participate in decision-making – especially at the local and regional level in communities throughout the United States.

Rose Foundation specializes in directing consumer class action *cy pres* and environmental remediation payments back to affected communities. Guided by the settlement instructions and our community funding boards, our extensive grantmaking programs direct money to organizations focused on protecting consumer rights and the environment. Our grantmaking emphasizes community equity and social justice, and we strive to deliver the greatest benefits and impacts towards vulnerable populations who need the most help. We manage more than 20 grantmaking funds powered by *cy pres* awards or environmental settlements, and we have distributed over $60 million to date from over 700 legal settlements. In addition, Rose has administered another $30 million in donor advised funds as well as regranting programs with partner foundations.

3. Describe the organization's current goals.

The overall mission of the Rose Foundation recognizes that better decisions are made when the communities most affected by social and environmental injustices are at the center of the decision-making process. The Rose Foundation seeks to significantly increase investment in the protection of consumer rights, especially vulnerable underserved communities - by supporting a range of community-based projects and organizations that are building long-term solutions that benefit people, their rights, the environment, and the economy.

Most of the larger domestic foundations only focus their support on nationwide organizations. The Rose Foundation takes a different approach – we provide grant opportunities to small and mid-size organizations which represent underserved communities and unheard voices and provide them with support to engage in emerging issues, including AI, data security and internet privacy issues. While the Parties and the court are aware of all the leading national consumer privacy nonprofit organizations,

extending the *cy pres*' full benefits across the entire range of a huge national class means going much deeper than simply supporting well-known organizations. We aim to ensure that notice of the availability of these *cy pres* funds is widely circulated into various affected communities to broadly benefit the entire class.

Rose Foundation's goal for this *cy pres* opportunity would be to reach out to hundreds of privacy organizations throughout the country and to solicit proposals squarely aimed at the on-line privacy and data security nexus in this matter. We also strive to ease post-settlement burdens by efficiently directing funds to support the interests of settling parties into communities affected by the alleged claims or violations while providing accountability by rigorously tracking grantee activities and accomplishments, and then reporting back to the parties and the court documenting how the grants tied into nexus and benefited the class.

4. Provide a brief description of the organization's current programs.

Rose Foundation for Communities and the Environment is a community-led, community-focused public foundation that provides regional and national grantmaking in the environmental and consumer advocacy sector. We have an extensive track record as a 3rd party administrator trusted by federal courts, California state regulators, and numerous plaintiff organizations and colleague foundations. Rose Foundation has been appointed as trustee in over 700 mitigation and *cy pres* funds related to consumer and environmental issues. By entrusting Rose with the duties of administrator, the class would benefit from everything we have learned in 30 years of grantmaking fueled by settlement funds.

Rose Foundation is unique relative to many other foundations in that we actively develop grantmaking programs which take the direction of the Parties in determining how to best meet the interests of the class. Further, a core part of our grantmaking mission is to ensure equity and justice are at the forefront of the process, and thus, all members of the class – especially the most vulnerable members – stand a better chance of having their privacy needs and interests represented in our grantmaking process. We also routinely conduct our grantmaking with the assistance of external expert funding boards to guide funding decisions. They allow us to identify nonprofits and university organizations whose work is at the cutting edge of a class action nexus, but which may not be immediately known to the court or the parties at the time of settlement.

5. Has your organization ever received a prior *cy pres* award? If yes, please cite the applicable. case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) Funded.

Rose currently has three consumer funds that have been developed in response to consumer advocacy related *cy pres*. They include:

- The Rose Foundation's **Consumer Privacy Rights Fund** was launched in 2002 and has received awards from 15 privacy class action settlements to date – including Bank of America, Union Bank, American Express, Cal Fed, MBNA, Fleet Bank, Chase/Manhattan, Washington Mutual, TD Bank, NDC Health, Netflix, Google, Facebook, Experian, and Total Merchant Services. To-date, the Fund has awarded over $7.3 million in privacy grants to more than 100 consumer privacy non-profits through the United States with an additional $1+ million scheduled to be awarded this fall. According to the Electronic Privacy Information Center, this has made the Rose Foundation one of the nation's leading supporters of consumer privacy rights and earned EPIC's *Champion of Freedom* award. All grant cycles are open-application and highly competitive, and the grantmaking

is advised by a funding board of consumer privacy education experts. For a list of past grantees, please visit: https://rosefdn.org/consumer-privacy-rights-fund/grantees

- **Consumer Financial Education Fund** was launched in 2012 with a $4 million *cy pres* from Bank of America and has also received $1+ million awards from HSBC and TD Bank, and a *cy pres* from a matter involving Chase Bank is pending. To date, the fund has awarded 90 grants totaling over $5 million to organizations throughout the United States teach basic financial literacy to some of the United States' most underbanked and vulnerable citizens. For reports on the impacts of this *cy pres* fund, please visit: https://rosefdn.org/wp-content/uploads/2016/10/CFEF-Report-Rose-Fdn-9-23-2016.pdf https://rosefdn.org/wp-content/uploads/2019/06/A-Cy-Pres-Impact-Report-2018.pdf

- **Consumer Products Fund** was originally launched in 2000 as the Environmental Health and Toxics Fund and rebranded as the Consumer Products Fund in 2014. It has received 18 *cy pres* awards including a $6.2 million award from Apple, as well as significant *cy pres* awards from Neutrogena, Nvidia, Badger Meter, and Johnson & Johnson. To date, it has awarded $5.7 million in support of organizations specializing in educating consumers about truth in advertising and technological performance of mobile devices, as well as the health impacts of product ingredients. A grant cycle is pending which will award an additional $2.2 million. For a list of past grantees focused on technological performance and truth in advertising issues, please visit: https://rosefdn.org/consumer-products-fund/grantees

6. Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?

Rose Foundation for Communities and the Environment has received a 4-Star Rating from Charity Navigator and is listed as a Platinum Level Nonprofit by Guidestar recognizing transparency and efficiency. Both ratings are the highest possible and are only attained by less than 5% of all charities, and we have held them for the past 10 years running.

Grant Proposal

7. Identify the organization's principal investigator or project director.

Our Mitigation Funds Director, Jodene Isaacs, is a public interest attorney who has represented non-profits in numerous federal enforcement cases related to water and toxic waste pollution. She has extensive experience analyzing and managing technical information used to support complex litigation as well as drafting and negotiating settlement agreements. Ms. Isaacs oversees all our grantmaking funds that are derived from legal settlements and ensures that the restrictions set by the Court and Parties are met.

Concerning fiscal management of the Fund, Rose Foundation's Director of Finance, Pamela Arauz, has an MBA and background in business accounting for large international corporations and over 10 years' experience working in nonprofit financial management. She is skilled in handling court orders and mitigation funds and developed an accounting system able to manage and track large amounts of restricted funding. Rose Foundation's Finance Department also helps organize and prepare agreements, reports, and financial documents for Rose Foundation's annual audit.

The Consumer Privacy Rights Fund is also advised by Executive Director Tim Little, who developed the Foundation's grantmaking programs fueled by mitigation and *cy pres* awards, and who draws on his 40+ years of philanthropic, policy development, grassroots advocacy, and non-profit organizational development experience to guide all the Rose Foundation's programs.

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

A. Goals and Objectives

All monies entrusted to the Rose Foundation will be dedicated solely to fulfilling the nexus of the enabling the settlement of *In Google Location History Litigation, No.5:18-cv-05062-EJD (N.D. Cal.*) and the funds will be disbursed to fund projects that are reasonably designed to mitigate, address, or support matters revolving around on-line privacy and data security issues.

B. Activities

Restricted Fund/Preservation of the Nexus*:* Any cy pres funds awarded to the Rose Foundation will be held in a restricted internal account dedicated only to fulfilling the purposes of the Google Location History settlement and *cy pres* order. We regard the court approval and related settlement documents as the equivalent of a Deed of Gift. As directed by the settlement and underlying body of charitable law, the Rose Foundation assumes full liability for meeting the proscribed nexus with all grants enabled by the fund.

Fund Announcement: Our consumer protection funds are all managed through a competitive open-application process which promotes a fair distribution of both large and small groups representing varying interests across the privacy field will have the opportunity to apply, thereby benefiting the entire class and extending the funding opportunity far beyond organizations which may already be known to the Parties and the Court. The open-application process is also a crucial component of how we select the most impactful proposals for funding and thus the opportunity to select the most effective strategies and projects. We also often see applicants who are working on different aspects of the same strategy, or who otherwise might achieve greater impact by collaborating with each other, and in these instances, we may be able to broker cooperative relationships which amplify the project's benefits to the class. While we approach administering the Google Location History *cy pres* educated by our two decades of experience as a leading grantmaking in the privacy field, we know that community-based applicants working at the cutting edge of privacy protection will have fresh ideas in this fast-moving field. The open-application process provides those groups with a robust channel to teach us about the latest developments and provides a dimension which simply cannot be achieved in a more limited invitation-only process.

A Request for Proposals (RFP) would be developed and circulated to our national distribution list of privacy and consumer education non-profit organizations and educational institutions. The RFP will detail the source of funding and set forth specific application guidelines related to on-line privacy as well as data tracking and security issues. With a maximum grant amount in the $200,000 range, we would expect to distribute around $3 million dollars per grant round. This would entail a range of grant sizes, from approximately $50,000 to $200,000, which are tailored to the organization's capacity and project needs.

We broadcast our Consumer Privacy Rights Fund RFPs to a distribution list that includes close to 400 organizations that do privacy-specific work nationwide. We would also target the 400+ organizations on

our Consumer Products List since many of them have focused on privacy related concerns in the context of consumer electronics – a key audience given this matter's implications around mobile devices. In addition, we have an even larger distribution list of about 700 organizations that do consumer advocacy and education related to financial empowerment. We would also share the RFP with those groups because they have conducted privacy related education related to mobile banking and other customer security issues. While there is some cross-over between these different lists, Rose Foundation will directly reach more than 800 separate consumer education organizations through this process, and over half of them address issues that are squarely at the nexus of the Google Location History matter. The RFP notice would also be made broadly available on our website (www.rosefdn.org), and via social media channels and the appropriate foundation directories as well. Our goal will be to broadcast this opportunity as widely as possible, and we would welcome additional mechanisms suggested by the Parties. We understand that broadly broadcasting notice of the grant opportunities is important given the nationwide aspect of the class, and we would also expect to take direction from the Court and Parties on any particularly vulnerable communities within the class harmed by privacy violations which the funding should target.

To ensure we receive proposals from well-qualified applicants with strategic ideas, Rose Foundation will conduct targeted outreach to past grantees who have been high performers with projects related to internet privacy and data security. In addition to engaging with well-known, high-capacity organizations, we will specifically target some of our outreach towards smaller organizations which serve vulnerable and impacted communities. We advise community-based applicants who may need guidance in designing a competitive proposal targeting the nexus, and where appropriate, we help locally based organizations collaborate with more prominent privacy experts, thereby helping to extend the reach of the *cy pres* into communities which otherwise may not be served by more established privacy groups. By actively engaging with applicants, Rose Foundation can help worthy organizations "find the bullseye" and submit strategic proposals. We also discourage applications from groups that do not seem well poised to submit qualifying applications.

Grant Awards Process: All applications for the Consumer Privacy Rights Fund would require: 1) detailed project descriptions that explain proposed use of funds, 2) full organizational profiles that help us evaluate the applicants' capacity to successfully complete the project, including descriptions of key staff and board of directors, 3) explanation of communities served and key collaborators, 4) detailed financial information from the applicants and a specific project budget, and 5) a project timeline, identification of key deliverables, and evaluation metrics. We then provide the opportunity for funding board members to give feedback on proposals and obtain clarifications from organizations as needed. In addition to the funding board members' deep issue-based expertise, Rose staff conducts full diligence on applicant organizations' financial capacity, staff capability and track record in the field. We examine their past work product, check their references, examine the depth of their community outreach plans, and interview applicants who reach the finalist stage to make sure we fully understand their entire project. Once all the applications have been fully vetted and a slate of grantees has been chosen for each round of grants, we would then submit it to the Court for final approval.

Expert Funding Board: All our Consumer Funds are advised by expert funding boards whose members provide strategic guidance, review grant applications, and make funding recommendations. The funding boards are a cornerstone of our vetting process to help us select the most strategic and robust projects, and we would constitute a specific funding board to help oversee this *cy pres*. Members of the funding board may not be closely affiliated with any grant applicants and will be governed by the Foundation's conflict of interest policy.

Rose Foundation is presently overseeing a *cy pres* resulting from the In Re Google LLC Street View Electronic Communications Litigation class action settlement (Case No. 10-md-02184-CRB), and our Consumer Privacy Rights funding board members currently include:

- Alan Bulter, Executive Director, Electronic Privacy Information Center
- Jeff Chester, Executive Director, Center for Digital Democracy
- Nicole Ozer, Technology and Civil Liberties Director, ACLU of Northern California
- Emily Tucker, Executive Director at the Center on Privacy & Technology at Georgetown Law

Given the technical expertise required to assess cutting edge privacy advocacy and the potential for multiple grant cycles, we anticipate adding or replacing funding board members depending on the number of rounds of grantmaking we are selected to oversee. We will aim to include board members who understand both how software and apps collect private data across platforms, the contexts where opportunities for breaches lie, as well as the relevant legal requirements to effectively select projects that have the most impact. However, we are comfortable with working out a selection process that would involve recommendations from counsel in this matter, including the participation of counsel in addition to the privacy experts.

Accountability and Transparency: Once the grants are fully approved, we execute binding contracts with each organization that allow ongoing oversight of grantee progress. The default period for grant contracts is one-year, but the applicants can structure their awards over a shorter or longer timeframe based on their activities and project deliverables. Larger grants, such as those over $200,000, may be for 2- or 3-year terms for which we require interim reports that allow grantees to document progress on their milestones and deliverables as well as provide an accounting of funds spent. We pay these multi-year grants in instalments, which allows us to maintain administrative control over the projects since we only pay the next instalment of the grant after approving the interim report. Then, after their projects are fully complete, grantees are required to submit final overall reports documenting activities, accomplishments, and expenses. These reports also ask grantees to share key insights gained during their project, and in addition to documenting direct impact, they form an important part of our knowledge base in educating future grantmaking decisions.

Although we may learn confidential strategic information from applicants and grantees during the application process – and fully honor such confidentiality, once grants have been awarded, we publicly announce the issuance of grants after every fund cycle and publish a comprehensive database of grants of all our funds on our website. We may also highlight significant accomplishments of various grants funds or specific grantees in our newsletter and communications. Unlike many other foundations, we also engage in frank conversations with denied applicants. In some instances, this can lead to a much improved and fundable future proposal. But even if there is no future pathway to funding because the fit with the fund's bullseye simply is not there, we find that most applicants appreciate the honest feedback.

Administrative Fee: The Rose Foundation charges a program administration fee to recover our costs of exercising stewardship over the funds, creating and servicing the funding board, publicizing the availability of the funds, conducting competitive grant cycles, administering grant awards, evaluating grantee progress, as well as providing reports to the parties and Court, conducting our annual audit, filing IRS and state charitable tax returns, and other related program administration and general foundation overhead. This fee is comprehensive – there are no other surcharges or annual fees. Our fee is typically scaled based

on the size of the award as well as complexity of the restrictions and reporting, and the proposed fee schedule is set forth under Question 10 and ranges from 5% to 7%.

C. Timeline

From the time of receipt of the *cy pres* award through grantee selection and the award of grant contracts, a *cy pres* grant cycle generally takes 9 – 12 months to complete. The Rose Foundation's preference is to expend larger *cy pres* awards (generally those exceeding $3 million) in multiple grant cycles. This allows us to learn from the first round and reward the highest performers with targeted renewal grants which help them build on their first wave of success. Analyzing results from the initial round of grants also enables us to fine-tune our strategy and maximize impact in the seceding grant round(s). Depending on the grant periods, which are most typically one to two years, our oversight function over the grants awarded usually then extends for the duration of the grantee's project.

Our timeline for this *cy pres* depends on the overall amount awarded. For a *cy pres* of $6 million dollars, we expect two grant cycles would be administered over a period of approximately two- and one-half years. If the *cy pres* award were closer to the $3 million dollar range, we would expect to distribute that in about a year. Scaling upwards, an award in the $10 million dollar range would be best distributed over three cycles administered over a period of approximately four years.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

Given the size of the Google Location History *cy pres*, combined with the breathtaking evolutionary pace of technological developments such as AI which have significant privacy implications, the interests of the class will be best served by the selection of a 3rd party administrator that can distribute the award to many different groups working on disparate issue areas related to internet privacy. The Rose Foundation is best positioned to serve that role for several reasons.

First, while the Parties and the court are certainly aware of all the leading national consumer privacy nonprofit organizations, extending the *cy pres*' full benefits across the entire range of a huge national class means going much deeper than simply supporting well-known organizations. We believe the class would be well served by an administrator capable of identifying and contacting hundreds of privacy organizations throughout the country and asking them to tailor proposals squarely aimed at the on-line privacy and data security nexus in this matter.

Second, depending on the size of the *cy pres* award to the Rose Foundation, the total award may simply too much money to be awarded to privacy activists in a single stroke – especially since we achieve maximum class benefit by extending the funding opportunity to include smaller organizations working on a local or regional scale. Managing a series of national funding opportunities over the next few years that reaches privacy organizations large and small, conducting the needed diligence to ensure that applicants who are offering promising ideas have the needed capacity to complete their projects, and then actively administering the grants including follow-up reporting to assess and document results are all critical steps to an effective use of the funds. We have years of experience conducting specialized grantmaking of this nature.

Finally, none of us can accurately predict what the fast-developing technologies which impact consumer privacy will look like in the future. Thus, you need an administrator capable of assembling and facilitating a

team of privacy experts who can not only help guide strategic awards with this *cy pres* today, but can guide grants awards at the cutting edge of the privacy field throughout the entire life of the *cy pres*.

As discussed above, we have a 30-year track record as a 3rd party administrator trusted by federal courts, California state regulators, and numerous plaintiff organizations and colleague foundations that will ensure the settlement fund will be impactful in terms of privacy rights and consumer issues. California Lawyer magazine has hailed the Rose Foundation for, "its reputation for transparency and a no-nonsense approach to the competition for funds." (September 2011). We have been honored with the Electronic Privacy Information Center's prestigious Champion of Freedom award in recognition of our leadership in supporting consumer privacy rights, and have sponsored major conferences on consumer privacy issues, including the Future of Privacy Rights conference – a two-day convening of national privacy activists and scholars, as well as the California Consumer Privacy Symposium. Thus, our experience with grantmaking and specifically with privacy related funding results in a structured program that meets the needs of the underlying class.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

We envision awarding the funds in a series of national grantmaking opportunities. We believe that an award of $6 million dollars would serve the class most efficiently as we could offer two grant cycles over a period of about two and a half years. Multiple cycles allow the most impactful grantees from the initial rounds to return with larger, multi-year proposals which provide us with the opportunity to invest in them with anchor funding that unlocks their full strategic potential.

That said, we can scale up or down from that amount as deemed appropriate by the Court. We could alternatively run a single grant cycle with a $3 million dollar award or ramp up to a total of three funding cycles over four years with a $10 million dollar award. As there are economies of scale operating multiple rounds, the administrative fees associated with each option are as follows:

Fee Schedule (based on the size of the *cy pres* award):
- Awards up to $3 million: 7%
- Awards up to $6 million: 6%
- Awards up to $10 million: 5%

Again, Rose is amenable to working out a shorter or longer disbursement schedule that meets the goals of the Parties.

11. Will the money be used to continue an existing project or create a new project?

The *cy pres* will be distributed through our existing **Consumer Privacy Rights Fund** as outlined above in Question 7.

12. What target population will your organization's project benefit?

Since the nexus of the Google Location History matter revolves around on-line privacy and data security issues, we will target application outreach and grant awards towards organizations and projects which emphasize solutions in those areas, including projects related to protection of internet privacy on both desktop and mobile devices. Guided by our national database of containing hundreds of consumer

education and consumer rights advocacy organizations that we have developed, Rose Foundation will work with experts whom we recruit to advise our consumer funds and identify nonprofits and university organizations whose work is on point with the class action nexus, but which may not be immediately known to the court or the parties at the time of settlement.

Diversity, equity, justice, and inclusion are core organizational values that are expressed in all our grantmaking. We have worked hard over the years to build outreach lists and maintain a mosaic of grantees that reflects our values, and we practice active engagement with applicants to help community-based applicants shape competitive funding proposals. We therefore give preference to applicants that are doing work that specifically benefits underserved and BIPOC communities which are part of the overall class.

As discussed above, our goal will be to broadcast this opportunity as widely as possible, and we would welcome additional mechanisms suggested by the Parties. We understand that broadly broadcasting notice of the grant opportunities is important given the nationwide aspect of the class, and we would also expect to take direction from the Court and Parties on any particularly vulnerable communities within the class harmed by privacy violations which the funding should target.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how will the remaining funds be used?

Rose Foundation is very experienced in providing reporting to the Court and litigants on the distribution of funds including project descriptions and grant terms. We do this on nearly every one of our settlements involving federal environmental statues as well as for larger *cy pres* where we routinely report back to the Court and parties as dictated by their terms. Rose Foundation agrees to report back to the Court and the parties every six months informing the Court and the parties on the following the number, size, and short summary of grants awarded, and the timeline for distributing remaining funds.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

The interim or final reports provided by the grantees will form an important part of documenting impact. This is a standard part of our accountability mechanism, and these reports provide the parties and the court assurance that the grants awarded conform with the settlement requirements for all mitigation and *cy pres* payments entrusted to the Rose Foundation. We also publish a description of all grants we have made on our website on an ongoing basis. However, our reporting process goes beyond merely documenting performance. We also ask grantees to share key insights gained during the project, and we regularly share this knowledge broadly to build the entire field, as well as to fuel Rose's knowledge base, evaluate our impact, and help us make educated grant decisions in future rounds. Since the Rose Foundation will track our grantees throughout the life of their projects, we provide a robust accountability mechanism that is often lacking in many other settlement award processes. This benefits the underlying parties because it ensures that the money is spent to the best effect.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

After the grant cycle supported by this *cy pres* has been completed and the grants are awarded, the Rose Foundation shall publish on its website a list of grantees along with descriptions of projects funded, and Rose Foundation shall supply reports to the parties describing the grants awarded and their conformity with the *cy pres* nexus. Periodically, the Rose Foundation also publishes more general reports that highlight significant accomplishments, best practices, and/or lessons learned of various grants funds or specific grantees on our website (https://rosefdn.org/reports) which we may share with other grantees. However, we do not expect to use the results of the project in any outside publications, conference papers, or external presentations.

Exhibit T

Organization Information

1. Name of organization

UCLA Institute for Technology, Law & Policy.

2. Discuss the founding and history of the organization

The Institute for Technology, Law & Policy (ITLP) is a partnership between the UCLA School of Law and UCLA Samueli School of Engineering which undertakes cross-disciplinary research and analysis to ensure that new technologies are developed, implemented, and regulated in ways that are socially beneficial, equitable, and accountable. ITLP was launched in January 2020 with a $10.25 million gift agreement. ITLP has pursued a diverse programming agenda, including direct engagement with government, civil society, and private sector stakeholders working across the public policy ecosystem. ITLP also prioritizes robust engagement with students, through a range of curricular offerings for law and engineering students as well as collaborative interdisciplinary research projects aimed at developing policy and technological solutions to emerging law and technology challenges.

3. Describe the organization's current goals

ITLP leverages its interdisciplinary nature, as well as its location on the doorstep of both innovation and technology regulatory policy, to serve as a hub for creative problem solving and engagement. ITLP works to address the next generation of accountability and human rights challenges flowing from the disruptive impact of new technologies through three distinct areas of programmatic focus:

1. Elevate policy development and multidisciplinary research in works interconnecting technology and law;
2. Foster the next generation of inventors, scholars and policy-makers through student enrichment and support;
3. Support faculty, civil society, and government collaborators to develop pathbreaking research targeting policy, ethics, and human rights challenges at the intersection of technology and law.

4. Provide a brief description of the organization's current programs

ITLP's current programs which are relevant to the current award can be summarized in three broad categories: a) privacy research, b) education and curricular development, and c) governance and policymaking.

a. Privacy Research

ITLP has a strong and growing presence in privacy-related scholarship and research and has invested significant resources into this space. In June 2023, ITLP was awarded $750,000 in funding from the National Science Foundation, shared between two researchers at UCLA and one from the Johns Hopkins School of Engineering, for a collaborative law-engineering project to assess the impact of privacy legislation on small and medium-sized online applications. ITLP is also piloting a project to develop new security and features for privacy-friendly communications apps, including private location sharing, lockdown and remote wipe features, and physical and geo-triggered "panic button" features.

Since its founding in 2020, ITLP has emerged as a significant hub for privacy scholarship and engagement, including our 2022 "Big Ideas in Privacy" workshop, which presented four books that had been published by prominent members of the privacy law community, namely Danielle Citron, Woodrow Hartzog, Neil Richards and Ari Waldman. In June 2024, ITLP is organizing a transatlantic workshop in Ireland bringing together leading privacy scholars with privacy regulators from the European Union and the U.S. UCLA Law has also applied to host the 2025 Privacy Law Scholars' Conference, through an application developed by ITLP.

b. Education and curricular development

ITLP organizes a number of curricular offerings for both law and engineering students, which are broadly clustered around regulatory, ethics, and policy challenges related to technological disruption. At the School of Law, ITLP's Information Policy Lab is an innovative experiential course which introduces students to the practical challenges of careers in the technology policy space, including through a government, non-profit, or industry lens.

At the Samueli School of Engineering, ITLP offers a range of classes aimed at exposing engineering and computer science students to policy and ethics questions related to the technologies they are likely to be working on, including "Technology and the Law", "Technology and Society", and "Ethics and Responsibility in Technology". In 2023, the engineering and computer science departments asked ITLP to build on these offerings to revamp their mandatory ethics curriculum. The first new class, "Ethics for Computer Scientists", was recently approved by the Faculty Council and will be offered for the first time in Fall 2024, taught by one of ITLP's resident fellows. The course, which draws on an innovative practicum merging app development with evolving ethical considerations, equips students with a deep understanding of ethical challenges in contemporary technology, applying foundational ethical theories to ongoing technological advancements. It will focus on responsible innovation, societal impact, and sustainable practices in computer science. Students will understand the ramifications of technology on core ethical principles, encompassing agency, responsibility, and privacy, and be prepared to address these harmful impacts before they arise in their own work.

c. Governance and policymaking

ITLP maintains strong links to ongoing public policy debates, and regularly hosts leading government, industry, and civil society stakeholders. Over the Fall 2023 term, ITLP hosted a special hearing of the California Senate Judiciary Committee on the proposed *California Journalism Preservation Act*, as well as a visit from United States Congressman Ted Lieu, to discuss his proposed *National AI Commission Act*. We also hosted government delegations from Singapore and South Korea, as well as industry representatives from Amazon and Apple.

ITLP has also weighed in on important public policy questions, with ITLP scholars participating in multiple amicus briefs in Supreme Court cases, including about the First Amendment and copyright, regulation of social media companies, and the intersection between trademark and the First Amendment. In addition, ITLP scholars recently filed a formal comment in the Copyright Office's Notice of Inquiry about artificial intelligence. ITLP scholars have also testified before Congress and write regularly for broader interest publications in order to further the public dialog on technology policy questions.

5. **Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded**

As a relatively young research institute launched in 2020, UCLA ITLP has never previously applied for a cy pres award.

6. **Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?**

Charity Navigator's most recent assessment rated the UCLA Foundation at 4 stars out of 4, with a score of 92%.

7. **Identify the organization's principal investigator or project director.**

Michael Karanicolas, the Executive Director of ITLP, will serve as the project director. Michael has been the inaugural Executive Director of ITLP since 2021, and is an affiliated fellow with the Yale Information Society Project. Michael has ten years of experience working with governmental and non-governmental stakeholders on efforts to advance digital rights across a range of global contexts, and extensive experience in legislative design and reform processes. He has authored over a dozen academic articles, and has been quoted widely in the media on issues of technology regulation, including ABC News, NBC News, and the Wall Street Journal.

ITLP works with an outstanding roster of faculty collaborators at UCLA, including faculty co-directors John Villasenor and Mark McKenna, and affiliated faculty across the law and engineering schools, including Yuan Tian, Andrew Selbst, Jerry Kang, Achuta Kadambi, Prineha Narang, all of whom will play a role in the development and execution of programming described here.

8. **Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.**

ITLP requests $2,982,000 in funding to support two inter-related projects, each of which has transformative potential on the global privacy landscape: 1) Developing new proactive enforcement models for privacy regulators; and 2) Establishing and scaling a new model of ethics and social responsibility for electrical and computer engineering and computer science education.

1. Proactive Privacy Enforcement

ITLP is currently in the second year of a three-year National Science Foundation-funded project to assess the operational impact of privacy legislation on small and medium-sized enterprises. Traditional paradigms of privacy enforcement are fundamentally reactive, and are typically triggered in response to well-publicized security or operational breaches. Enforcement actions generally target major offenders with heavy fines, under the assumption that such high-profile enforcement actions will serve to chill misconduct across the industry. However, the resource-intensive nature of these enforcement actions means that they typically only target the largest and most serious offenders. As a result, it is unclear what impact, if any, privacy legislation has on small and medium-sized enterprises, who are both too small to access dedicated legal support on privacy compliance and who are not likely to be targets of an enforcement action.

In the privacy realm, an ounce of prevention is worth a pound of cure. Measures to promote the widespread adoption of privacy and data protection best practices are far more effective, from a systemic perspective, than sporadic and targeted enforcement in the aftermath of a breach.

However, such proactive enforcement is challenging because regulators lack the resources to engage with companies at that scale, nor the ability to assess where problematic practices may be found in advance of a breach.

ITLP's current project focuses on the development of a machine learning-powered tool capable of carrying out rapid and automated assessments of web applications' compliance with privacy best-practices. Within the parameters of our existing funding, the tool will be used to conduct a longitudinal analysis of patching data to assess the impact of privacy regulation in the European Union and in California on operational approaches to privacy among online applications.

However, ITLP's research has significant transformative potential beyond the scope of the current project as a way of facilitating a new proactive model of privacy enforcement. Because the tool that is being developed allows for automated assessments of privacy compliance at scale, it has the potential to birth an entirely new model of enforcement, where regulators issue automated notifications of potential non-compliance in advance of an enforcement action. Such a notification could inform targets of specific aspects of their privacy or security posture which fell below industry best-practices, and offer instructions for the problems that need to be remedied in order to avoid a potential future enforcement action. By issuing these notifications proactively, and at scale, regulators could effectively "nudge" companies, especially smaller companies, towards compliance with privacy best practices in advance of either a breach or an enforcement action.

While this application grows intuitively from our current project, it is beyond the scope of our existing funding, and would require additional resources to develop our existing tool to suit this specific application, as well as to promote engagement with regulators in leading jurisdictions to support its adoption.

As part of this application for additional funds, we would propose an additional three years of research and salary support for key ITLP operations related to this project, running from January 2025 – December 2028. The project would commence in Year 1 with an expansion of the current research project to include specific and targeted engagement with leading privacy regulators in the European Union, Canada and the United States, to carry out a comprehensive scoping of the strengths and weaknesses of existing enforcement paradigms, and perspectives on the potential, as well as any technical or legislative obstacles that might stand in the way of a new structure of proactive enforcement. Starting in Year 2, we will build on the initial research to support an expansion of our machine learning-powered tool with a suite of new capabilities specifically targeted to suit the needs of regulators. In Year 3, we will promote the resulting product to global regulators, as well as fine tune based on the results of early feedback from regulators on how to maximize practical utility. We will also disseminate the results through the development of educational curricula, including a new course on Privacy Law and Techniques, which will be taught by Professor Yuan Tian at the UCLA Samueli School of Engineering, as well as the new ethics classes described below. We also intend to submit our research results to top tier security and law conferences and journals, as well as leading civil society fora such as RightsCon and the Internet Governance Forum.

2. Re-imagining Ethics for Computer Scientists

The past two decades have been a time of unprecedented technology transformation. These changes have been driven by an ethos of creative disruption, captured most famously, or infamously, by Facebook's early unofficial slogan of "Move Fast and Break Things". While there have been enormous benefits flowing from new digital communications technologies, society is

still also coming to grips with a range of harms, including an erosion of privacy as a result of the data-hungry models which underlie the modern surveillance economy.

We believe that one of the key drivers underlying the steady erosion of privacy protection by recurring generations of new technologies is a lack of sufficient engagement, by creators and innovators, with the social and ethical cost of their products. The result has been an era of technological creation which focused entirely on technical and economic opportunities, while paying insufficient attention to moral or ethical concerns. In response, we propose investing in early-stage intervention through a robust training in ethics and social responsibility for engineering and computer science students. Our aim is to foster a new generation of creators and innovators who enter the market with an ability to think critically about the impact of their products on the world around them.

UCLA, like most universities, has an ethics curriculum in place for its engineering students. However, this curriculum contains little relevance to the specific ethical challenges underlying the modern information society. In part, this is because of a lack of research on the intersection between emerging technological challenges and the practical professional responsibility questions that computer science and electrical and computer engineering graduates are likely to face.

As a research institution which straddles the fields of law and engineering, including a specific focus on the human rights impacts of new technologies, ITLP is uniquely well-situated to make substantial contributions to this space. Over the past two years, ITLP has piloted a class for first-year engineering students on the social impact of new technologies. The class has been fully subscribed in both of the years that it was offered, and it received strongly positive student reviews. Building on this interest, ITLP developed a proposal for a new ethics class which can be delivered as part of the mandatory engineering and computer science curriculum. There is strong buy-in from both faculties to this program, but a dearth of instructors which have the requisite experience, and commitment to the ethics and social responsibility space, as well as a need for more original research to fill out the curriculum.

Starting in Spring 2025, ITLP aims to use funding from this award to launch the Initiative for Responsible Innovation, which will be dedicated to advancing research and understanding of ethics for computer science and engineering students, as well as offering comprehensive ethics education to the next generation of creators and innovators. The Initiative will host two resident fellows between Fall 2025 – Spring 2027, with an additional two fellows from Fall 2027 – Spring 2029. There will also be a rotating cohort of research assistants, drawn from the engineering, law, and computer science schools, as well as a diverse cross-section of affiliated faculty, participating under the auspices of ITLP. The core purpose of the initiative will be to provide an ethics framework for engineering and computer science students, through course offerings, guest speakers, and other direct engagement. It will also develop original research, host conferences, symposia, and workshops, and engage with relevant professional standard-setting bodies, private sector partners, and regulators to support the incorporation of strong ethics standards in official policy. Although our initial focus will be aimed at supporting educational offerings at UCLA, once an appropriate research baseline has been established we will aim to scale this programming externally, first across the UC-system, and then to other leading engineering and computer science schools across the United States.

Ultimately, the goal of this program is to develop actionable ideas for managing risks that manifest through the development of new engineering and computer science projects, and train the next

generation of engineers and computer scientists to think critically about the societal impacts of what they are applying their talents to. By developing a solid baseline of professional ethics, and focusing on responsible innovation, we see this as a long-term project to encourage better protections for privacy and human rights online.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

For both of the components of the project, ITLP will leverage its existing expertise and momentum to scale out proven programming areas to significantly enhance their impact on privacy and responsible innovation. For the engineering ethics component, ITLP will leverage its experience in developing innovative and effective curricula, as well as significant administrative buy-in from the engineering and computer science departments, to ensure that the program is comprehensive and maximally applicable for students. On the proactive privacy research, ITLP will use the additional funds to springboard our original NSF-funded project to move beyond theoretical research applications to tools which lend themselves to direct use by regulators around the world, and which ultimately support the adoption of more responsible privacy practices across the tech sector.

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

We request $2,982,000 over 4 years, with a breakdown as follows:

1. Re-imagining Ethics for Computer Scientists

- Resident Fellow Salaries: $950,000
- Salaries for ITLP Staff and Researchers: $800,000
- Support for Conferences, Convenings, and other promotional activities: $250,000.

2. Proactive Privacy Enforcement

- Support for ITLP Researchers: $300,000
- Support for Researchers from Yuan Tian's Lab: $300,000
- Support for Conferences, Convenings, and other promotional activities: $200,000.

+ UCLA Foundation fee (6.5%) = $182,000

11. Will the money be used to continue an existing project or create a new project?

As described above in Question 8, the funds will be used to significantly expand two projects where the early conceptual work has been done, but which require additional resources in order to scale them out to their full potential.

12. What target population will your organization's project benefit?

The engineering ethics curriculum component will most immediately benefit students, who will learn from the curriculum, and we also anticipate benefits across the technology sector, as employers are able to recruit more thoughtful employees. Ultimately, however, our goal for this program is to drive broader shifts in attitudes towards privacy, surveillance and innovation across the relevant industries, with the benefits accruing to the consumers of digital technology products and the public as a whole.

The updating privacy enforcement paradigm component will most immediately benefit privacy enforcement agencies, who will have a faster and more effective way to monitor privacy at scale, and small- and medium-sized organizations, who will have assistance in knowing they satisfy privacy regulations. But again, this component will ultimately benefit the public, by creating a world where more of the organizations that deal with data have appropriate privacy safeguards in place.

Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes.

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

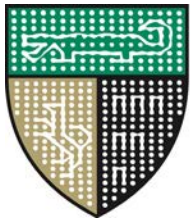
For the engineering ethics curriculum, early success will be measured by the reach of the curriculum and the degree of student engagement, as assessed through student evaluations. However, over the medium term, we intend to apply a comprehensive methodology to track and survey graduates, and asking them to report back on the relevance of our educational offerings to their workplace experiences, providing for progressive improvements to the curriculum over the course of the project.

For the proactive privacy enforcement component of the project, success will be measured by engagement and uptake among regulatory agencies of our tools. Here, too, we will employ a methodology of progressive improvement throughout the life of the project, as negative feedback or a lack of engagement among regulators will be interpreted as a need to shift our outreach tactics or the substance of our tool's functionality.

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Yes. ITLP will share the engineering ethics research and our new curricula broadly, including through publications, conference papers, and presentations, to make it available for other universities to replicate, and to encourage other institutions to consider revising their own approach to ethics for engineering and computer science students. ITLP will also create publications, conference papers, and presentations about the updating privacy enforcement paradigm component, to better socialize this project with privacy regulators and the scholarly community.

Exhibit U



Information Society Project
Yale Law School

October 17, 2023

Tina Wolfson,
Ahdoot & Wolfson PC.

Michael Sobol,
Lieff Cabraser Heimann & Bernstein, LLP.

Dear Ms. Wolfson and Mr. Sobol,

Thank you for inviting a proposal from the Informational Society Project at Yale Law School for the cy pres award in the *In re Google Location History Litigation*. We have attached a detailed proposal, having framed it in the manner you advised. We have also attached a budget to help with planning, with tabs that propose different options depending on funds that can be made available to us.

Broadly, our proposal consists of:

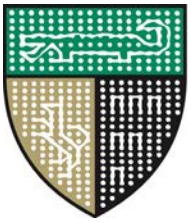
(1) Two research fellows whose work will promote the protection of internet privacy.
(2) A technology accountability project targeted at improving the law on privacy and algorithmic justice, involving law students supervised by lawyers consisting of:
    a. clinical director who leads the project
    b. two clinical fellows
    c. costs of filing, transportation and other activities that are a part of a clinic

Please do let us know if we can share any additional information. We look forward to hearing from you.

Best,

Chinmayi Arun

Executive Director,
Information Society Project, Yale Law School.



Information Society Project
Yale Law School

1. **Name of organization**

The Information Society Project at Yale Law School.

2. **Discuss the founding and history of the organization.**

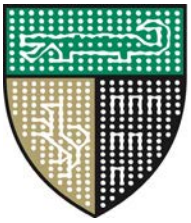
The Information Society Project (ISP) is an intellectual center at Yale Law School, founded in 1997 by Professor Jack Balkin. Over the past quarter century, the ISP has grown from a handful of people gathering to discuss internet governance into an international community working to illuminate the complex relationships between law, technology, and society.

The Yale ISP is home to the The Media Freedom and Information Access Clinic (MFIA) , which was established in 2009 by four Yale Law School students who recognized that the migration of investigative reporting from newspapers, network news departments and other traditional news organizations to online websites, blogs, and other start-up operations, was leaving many journalists without access to the legal services needed for effective reporting, and that the settled legal principles protecting our robust and independent press would need to be re-established for these journalists in very different digital contexts. In August 2023, MFIA added the Tech Accountability Project (TAP), which works with students to engage in litigation, legislative drafting, and policy proposals aimed at regulating digital platforms and their use of artificial intelligence, prediction products, data collection, and related technologies.

3. **Describe the organization's current goals.**

At its core, the ISP is an intimate community of interdisciplinary scholars—comprised of resident fellows, visiting fellows, student fellows, and Yale University faculty—exploring cutting-edge issues at the intersection of law, technology, and society. Our fellows have diverse academic backgrounds and practical experience in law, communications, computer science, medicine, journalism, economics, political science, art, cognitive psychology, sociology, and film studies. ISP alumni who hold academic positions join our international network of nearly one hundred ISP affiliate fellows; other alumni have become legal practitioners, activists, entrepreneurs, and policymakers. While members of the ISP community have diverse areas of expertise, the center's work focuses primarily on technology law and policy, which includes privacy and artificial intelligence.

The ISP's clinics and research fellows, in turn, work on a wide range of legal issues related to platform regulation. These include in addition to privacy intellectual property, telecommunications law, consumer protection, labor and employment law, antitrust and competition law, and civil rights and civil liberties. Our approach to technology law and policy is wide-ranging because important issues in the field change over time.



Information Society Project
Yale Law School

4. Provide a brief description of the organization's current programs.

Each academic year the ISP hosts nearly 100 educational events designed to promote novel scholarship, foster the cross-pollination of ideas, and spark new collaborations. Several of these focus on privacy and AI. In addition to the MFIA clinic and the Tech Accountability Project mentioned above, the ISP is also home to a variety of initiatives with complementary educational and advocacy aims:

a. The Floyd Abrams Institute for Freedom of Expression promotes freedom of speech, freedom of the press, access to information, and government transparency.

c. The Knight Law and Media Program (LAMP) is designed to foster a deeper understanding of the issues at the intersection of law, media, and journalism and to encourage students to pursue careers in media law.

d. The Wikimedia/Yale Law School Initiative on Intermediaries and Information (WIII) has two main aims: to raise awareness of threats to an open internet, especially those affecting online intermediaries and their users, and to make creative policy suggestions that protect and promote internet-facilitated access to information.

e. The Program for the Study of Reproductive Justice (PSRJ) is an incubator of novel litigation strategies and legal theories designed to advance reproductive rights and justice.

f. Privacy Lab is a nexus for workshops and discussions concerning software, hardware, and spectrum freedom, as well as a resource for cryptographic and anonymity tools.

5. Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.

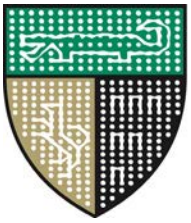
No

6. Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?
Yale has been rated on Charity Navigator, at 86%

Grant Proposal

7. Identify the organization's principal investigator or project director.

Jack M. Balkin, Knight Professor of Constitutional Law and the First Amendment, Director, ISP, jack.balkin@yale.edu.



Information Society Project
Yale Law School

8. Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.

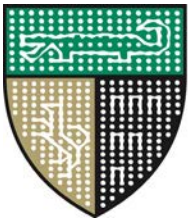
We propose to address privacy and related rights through work that has long term and short term influence. Our long term focus is growing and nurturing scholars and advocates in the field. To this end, we have asked for funds to support two research fellows per year who will focus on privacy and related questions in the algorithmic society. The ISP fellowship has a long and successful history of producing highly influential scholars and scholarship. Supporting the development of young scholars is central to our mission. Each ISP fellow stays in New Haven for a few years after which they remain in our larger academic network, supporting and mentoring those who come after them.

We also work directly to influence policy through the Tech Accountability Project (TAP) which is part of the larger Media Freedom and Information Access Clinic (MFIA); it focuses on the regulation of social media companies and digital platforms. The Clinical Director and clinical fellows are experienced lawyers who work with law students on drafting legislation, producing comments for administrative agencies, drafting amicus briefs, and litigation. Funding and resources would permit MFIA to take on more cases and policy projects that focus on privacy and algorithmic justice. We have asked for support for the project's director and two clinical fellows, each of whom will be experienced lawyers capable of working with and mentoring Yale Law students, who are some of the most talented in the world. In addition to influencing emerging policy, the clinic also encourages and inspires Yale Law students to take an interest in these questions. In this way we hope to create an ever increasing pool of brilliant lawyers who will continue to work to protect privacy rights throughout their careers.

The ISP offers its lawyers and researchers at least two years of funding. The Clinical Directors have a longer tenure but we try to ensure that their time is directed towards their valuable work instead of fundraising by ensuring that all grants offer at least two years of support. We have offered options in the budget (attached) for funding different combinations of people and work at the ISP, depending on the funds allocated to us.

9. Explain why the organization is approaching the issue and/or opportunity in this way.

The ISP is located within Yale Law School and draws on the strengths of its academic community as well as the law school's outstanding student body. Yale Law students' interests are shaped by the issues they work on while they are in New Haven. Our academic fellowship immerses promising young scholars in the community of information scholars that the ISP has been growing for a quarter century, and in the wider network of scholars that Yale University offers. Scholars like James Grimmelmann and Margot Kaminski were nurtured by the ISP at the start of their careers. The ISP community also includes stalwarts of privacy theory like Daniel Solove, Daniel Citron and Neil Richards.



Information Society Project
Yale Law School

10. Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.

The total amount requested is $2,639,646 for two ISP research fellows, the Clinical Director of the Tech Accountability Project and one clinical fellow, along with the expected costs of litigation and the administrative costs of hosting this project. Our request is for four years of funding.

We have broken this down into funds for the Clinical Director and the clinic's work ($1,292,703), funds for one or two clinical fellows ($596,521 each for four years) and one or two research fellows ($502,745 each for four years). The figures include institutional costs for hosting and supporting the fellows.

11. Will the money be used to continue an existing project or create a new project?

It will ensure that our tried-and-tested projects have the resources to focus on privacy.

12. What target population will your organization's project benefit?

In the long term, it will benefit the public through its new ideas about privacy and its litigation, and influence of law and regulation. Additionally, the law students and scholars who are a part of this project will continue have a generative effect through their future work.

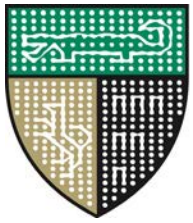
Evaluation

13. Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?

Yes

14. Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.

We will report publications, events, litigation and policy engagement made possible by this project. Our events are made accessible to others through zoom. Our greatest strength is our long term impact. Our scholars remain a part of the community and continue to enhance and promote privacy through their brilliant careers.



Information Society Project
Yale Law School

15. Does your organization intend to use the results of the project in any publications, conference papers, and presentations?

Yes