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.