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.