EXHIBIT A

This is a report from the American Civil Liberties Union Foundation (ACLU) on the work of the ACLU and ACLU of Northern California to enhance Americans' privacy and security with cy pres funds received through settlement of *In re Google LLC Street View Electronic Communications Litigation* (10-md-02184-CRB). This report covers work carried out between 1/1/23 and the present.

PROGRAMMATIC UPDATES

DIGITAL PRIVACY AND SECURITY

- In May the ACLU published an updated white paper, *Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data*. The white paper identifies features of electronically stored data that pose novel problems for our Fourth Amendment rights, and highlights how current search-warrant practice falls short. Drawing on amicus briefs the ACLU has filed in state and federal courts across the country, the paper then sets forth legal arguments in support of robust rules for obtaining and executing warrants in the digital age. Defense attorneys, magistrates, and prosecutors seeking to protect privacy while permitting legitimate investigations can benefit from this paper, as well as the accompanying briefing and court opinions.
- In April we and the Electronic Privacy Information Center submitted comments to the National Institute of Standards and Technology (NIST) on its draft Digital Identity Guidelines for Enrollment and Identity Proofing. We urged NIST to modify the draft guidelines to 1) depreciate repeat, remote collections of biometric information, 2) remove the social security number as a valid attribute for identity verification and invest in alternatives, 3) evaluate W3C Verifiable Credentials as a technical standard to improve remote identity verification, 4) target fraud prevention controls towards large-scale attacks and de-prioritize fraud prevention that creates barriers to claiming benefits, and 5) to further strengthen steps to address equity concerns by requiring agencies to provide multiple options for identity verification and other measures.
- The ACLU of Northern California updated its business primer *Privacy & Free Speech: It's Good for Business*—the most comprehensive repository of historical case studies (150+) and guidance to educate businesses and help them integrate best practices for protecting consumer privacy and build proper protections into their new products and business models right from the start. The updates include four new internet privacy case studies, including one focused on disclosure of location data, as well as six content pages on privacy issues related to data collection, retention, use, disclosure and security, as well as an additional updated content section on the current internet privacy legal landscape.

ARTIFICIAL INTELLIGENCE (AI) AND PRIVACY

- In April we posted an exploration of how ChatGPT and other large language models could be used to supercharge everyday surveillance. Our concerns were cited in a *Forbes* article.
- In March the *Washington Post* revealed "how closely FBI and Defense officials worked with academic researchers to refine artificial-intelligence techniques that could help in the identification or tracking of Americans without their awareness or consent." The exposé is based on thousands of pages of documents we and the ACLU of Massachusetts obtained through an ongoing FOIA lawsuit and provided to the *Post*.

SOCIAL MEDIA SURVEILLANCE

- We continued our FOIA litigation seeking records from seven federal agencies that conduct surveillance of social media users and speech: the Departments of Homeland Security, Justice, and State; the Federal Bureau of Investigation; U.S. Customs & Border Protection; U.S. Citizenship & Immigration Services; and U.S. Immigration & Customs Enforcement. We had filed the lawsuits in 2019 after the agencies failed to produce any responsive documents. In April we published a blog post, *Is the Government Tracking Your Social Media Activity?*, based on documents that we have since secured, and seeking reports of visa holders and immigrants impacted by these programs.
- In late 2022 and early 2023, the ACLU of Northern California worked on a follow-up investigation into how the Los Angeles Police Department was using social media surveillance on people in Los Angeles and how surveillance vendors may be accessing this information and potentially violating corporate privacy policies that we had successfully advocated for previously at Facebook/Meta. It coordinated a series of meetings with Facebook/Meta privacy leadership to address these issues.

DIGITAL CURRENCIES AND PAYMENTS

- In March the ACLU published a white paper on central bank digital currencies. ACLU experts were also quoted on the topic in numerous media outlets, including *The Hill* and *Fortune*. A major focus of our concern is how to preserve privacy and anonymity—not just as a matter of policy, but technologically.
- Building on its earlier work to highlight internet privacy and security issues related to QR codes and the increasing requirements of digital payments during the COVID era, the ACLU of California worked with a team of Berkeley information school and law students for the 2022-2023 school year to identify the proliferation of these no-cash policies in local stores and highlight the internet privacy and security issues and economic justice impact. In April 2023 it shared its findings with local lawmakers, who are exploring actions to address these issues as a result of our investigation.

TECH-ENABLED HOME SURVEILLANCE

- Our work building on the historic *Carpenter* decision to establish more robust warrant requirements in the digital age continued. In May 2023 we, the ACLU of Kansas, the ACLU of Colorado, the Brennan Center for Justice, the Center for Democracy & Technology, and the Electronic Privacy Information Center filed an amicus brief in a federal appeals court in *U.S. v. Hay*. This case arises from the government's warrantless use of a sophisticated pole camera aimed at a home to surveil everyone who came and went for nearly ten weeks. During that period, police officers could watch the camera's feed in real time (or later, at their leisure) from the station, and could remotely pan, tilt, and zoom close enough to read license plates or detect what someone was carrying into or out of the house. The district court erred in concluding that this did not amount to a Fourth Amendment search. Our involvement in *Hay*—and in other cases involving warrantless pole camera surveillance—is part of our broader work, post-Carpenter, to update the protections of the Fourth Amendment for the digital age. We are also counsel in another pole camera case, *Moore v. United States*, currently being considered for review by the U.S. Supreme Court.

LOCATION PRIVACY & GEOFENCE WARRANTS

- In February we provided guidance for how communities considering agreements with Flock Safety can better protect their privacy through concrete contractual amendments. Flock Safety has been blanketing American cities with dangerously powerful and unregulated automatic license plate recognition (ALPR) cameras, many networked into a nationwide mass-surveillance system out of its customers' cameras. This advocacy builds on our March 2022 white paper on the company, which had been flying largely under the radar of public awareness.
- In February we highlighted how a new privacy-protective mobile phone service (Pretty Good Phone Privacy) and other technical solutions prove that technology exists to protect the privacy of our location, identity, and data, and could be built into our technology providers' infrastructures if they so choose.
- In January we, the ACLU of Virginia, and 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 unknown numbers of people in a large area without reason to believe they were engaged in criminal conduct.

MOBILE/APPS

- With the passage of anti-abortion and anti-transgender laws in some states around the country, we have engaged in a variety of public education efforts related to the intersections of gender, sexuality and reproductive rights and internet privacy, helping people better protect their sensitive personal information,

and urge companies to strengthen privacy protections to protect people around the country. For example:

- In April we raised the alarm about the dangers of location information being sold by data brokers, and the threat it posed to people seeking reproductive care and others.
- ACLU of Northern California Director of Technology and Liberty Nicky Ozer presented on threats to bodily and intimate privacy at the 11th Annual Berkeley Center for Law and Technology Privacy Law Forum along with Professor Khiara Bridges. The program is currently offered on demand online by Berkeley Center for Law & Technology for California general CLE credit.

OTHER SURVEILLANCE

- In January we and the ACLU of Arizona released more than 200 documents on one of the largest government surveillance programs in recent memory. The records show that the state of Arizona has sent at least 140 overbroad and illegal subpoenas to money transfer companies to compel them to turn over customers' private financial data—of all $500+ money transfers from border states, and to/from Mexico—amassing a huge database and giving virtually unfettered access to thousands of officers from hundreds of law enforcement agencies across the country. The database, run by an organization called the Transaction Record Analysis Center (TRAC), contained 145 million records of people's financial transactions as of 2021 and, as our blog post explained, there is reason to think it continued to amass records.

ORGANIZATIONAL UPDATES

The ACLU's Speech, Privacy, and Technology Project (SPT) has had three notable staff changes since our original application for cy pres funding. First, attorneys Nate Wessler and Esha were both promoted to SPT deputy directors. Mr. Wessler, who successfully argued the landmark privacy case U.S. v. Carpenter before the Supreme Court, focuses on privacy. Ms. Bhandari, who had led several ACLU cases involving the impact of big data and artificial intelligence (AI) on rights and liberties, now coordinates AI work across the ACLU. Finally, in November 2021 Scarlet Kim joined SPT as a senior staff attorney. Prior to joining the ACLU, Ms. Kim worked as a legal officer at Privacy International, an associate legal adviser at the International Criminal Court, and a Gruber Fellow in Global Justice at the New York Civil Liberties Union.

You can find biographies of these and other key SPT staff here.

In January 2023 Nick Hidalgo joined the ACLU of Northern California as a staff attorney with the Technology and Civil Liberties Program, where he works on a variety of issues, including privacy, surveillance, and free speech. Prior to joining the ACLU of Northern California, Nick was a deputy attorney general at the California Department of Justice, where he worked to protect Californians from fraud and financial misconduct through

enforcement of the California False Claims Act. Before that, Nick represented individual and corporate clients at Jones Day. Nick's practice primarily focused on complex civil litigation, but he also advised clients on how to comply with data security and privacy laws such as the California Consumer Privacy Act and European Union General Data Protection Regulation.

You can find biographies of other key Technology and Civil Liberties Program staff here.

EXPENDITURES

SALARIES/BENEFITS:

ACLU nationwide privacy/surveillance attorneys and other staff: $654,016

ACLU of California privacy/surveillance attorneys: $251,646

Total Salaries/Benefits: $905,662

OTHER ACLU AND ACLU OF CALIFORNIA COSTS:

Litigation: $5,000

Office costs (includes phones, equipment, rent, IT): $35,000

Administrative overhead (includes time dedicated to this surveillance work by ACLU development, executive, human resources, and finance department staff): $60,921

Total Other Costs: $100,921

TOTAL EXPENDITURES: $1,006,583