



Assembly Committee on Public Safety  
Hon. Reginald Byron Jones-Sawyer, Sr., Chair

## Informational Hearing

We See You:  
**Law Enforcement Surveillance  
and Investigative Technologies**

Tuesday, August 9, 2022  
9:00a.m. – 12:00p.m.  
State Capitol, Room 126  
Sacramento, CA



## **ASSEMBLY COMMITTEE ON PUBLIC SAFETY**

### ***We See You: Law Enforcement Surveillance and Investigative Technologies***

#### **AGENDA**

Tuesday, August 9, 2022

9:00 a.m. to 12:00 p.m.

State Capitol, Room 126

**I. Introduction and Opening Remarks: 9:00 a.m. – 9:30 a.m.**

Reginald Byron Jones-Sawyer Sr., Chair, Assembly Committee on Public Safety

**II. Automatic License Plate Readers: 9:30 a.m. – 10:00 a.m.**

Ángel Díaz, Visiting Assistant Professor, USC Gould School of Law

John Lewis, Principal Auditor, California State Auditor

City of Vallejo Council Member Pippin Dew, Public Safety Policy Committee Chair,  
League of California Cities

Assistant Chief Mike Alvarez, Special Representative to the Legislature, California  
Highway Patrol

**III. ShotSpotter: 10:00 a.m. – 10:30 a.m.**

Tom Chittum, Vice President, Analytics and Forensic Services, ShotSpotter

Steven Oliveira, Deputy Chief, Sacramento Police Department

Brian Hofer, Chair and Executive Director, Secure Justice

Beryl Lipton, Investigative Researcher, Electronic Frontier Foundation

**IV. Geofences and Geofence Warrants: 10:30 a.m. – 11:00 a.m.**

Brett Diehl, Trial Attorney, Federal Defenders of San Diego, Inc.

Katelyn Ringrose, Global Lead for Law Enforcement and Government Access,  
Google

Jennifer Lynch, Surveillance Litigation Director, Electronic Frontier Foundation

Jacob Snow, Technology and Civil Liberties Attorney, American Civil Liberties Union

**V. Facial Recognition Technology: 11:00 a.m. – 11:30 a.m.**

Skylor Hearn, Director of Government Affairs, Clearview AI

Derek Sabatini, Lieutenant, Los Angeles County Sheriff's Department

Jennifer Jones, Staff Attorney, American Civil Liberties Union

**VI. Public Comment: 11:30 a.m. – 12:00 p.m.**

## ASSEMBLY COMMITTEE ON PUBLIC SAFETY

### *We See You: Law Enforcement Surveillance and Investigative Technologies*

#### SPEAKER BIOGRAPHIES

##### **Panel 1: Automatic License Plate Readers**

**Ángel Díaz**, *Visiting Assistant Professor at USC Gould School of Law*

Ángel Díaz is a Visiting Assistant Professor at USC Gould School of Law. His scholarship and teaching focus on the intersection of emerging technology and racial discrimination. He has written on a range of topics, including police surveillance, the regulation of social media companies, and the deployment of automated decision systems.

Ángel has authored or coauthored numerous reports and resources, including *Double Standards in Social Media Content Moderation* (2021), *Law Enforcement Access to Smart Devices* (2020), *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use* (2020), and *New York City Police Department Surveillance Technology* (2019) among others. His work and commentary have been featured in outlets such as the Associated Press, NPR, The Washington Post, NBC News, Just Security, Brookings Tech Stream, and Univision.

Prior to joining USC, Ángel was a Lecturer in Law at UCLA School of Law. He was previously Counsel in the Liberty & National Security Program at the Brennan Center for Justice and an Adjunct Professor of Clinical Law at NYU School of Law.

Ángel received his B.A. and J.D. from the University of California, Berkeley. During law school, he was Book Reviews & Essays Editor of the California Law Review, and Annual Review Editor of the Berkeley Technology Law Journal.

**John Lewis**, *Principal Auditor, California State Auditor*

John Lewis is a principal auditor with the California State Auditor's Office. He has been with the office since 2007 and has worked on a variety of audits, including managing the 2020 audit on automatic license plate readers. He is a certified internal auditor.

**City of Vallejo Council Member Pippin Dew**, *Public Safety Policy Committee Chair, League of California Cities*

Pippin Dew is a Councilmember with the City of Vallejo, elected in 2013. She is deeply involved with the League of California Cities, and has served as President of the North Bay Division, Chair of the Transportation, Communications & Public Works Policy Committee, Chair of the Public Safety Task Force, the Governance Task Force. She currently serves as Chair of the Public Safety Policy Committee, a member of the Governance Committee, and as a member of the Board of Directors for the League of

California Cities. Pippin is a graduate of the Haas School of Business at University of California, Berkeley. She is also a Realtor and a mother of three girls.

**Assistant Chief Mike Alvarez**, *Special Representative to the Legislature, California Highway Patrol*

Assistant Chief Mike Alvarez is California Highway Patrol (CHP) Commissioner Amanda Ray's Special Representative to the Legislature. In this capacity, he serves as CHP's liaison for the Legislature for various public safety issues, including proposed legislation that would impact CHP operations and programs.

## **Panel 2: ShotSpotter**

**Tom Chittum**, *Vice President, Analytics and Forensic Services, ShotSpotter*

After nearly 27 years in federal law enforcement, Tom Chittum joined ShotSpotter to help promote and support the integrated use of the company's vast data holdings and comprehensive public safety solutions. He leads a team of experienced professionals committed to supporting robust and effective application of ShotSpotter's products in investigations, forensics, and litigation.

Tom is a licensed attorney. He retired from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as a member of the Senior Executive Service (SES). He spent his last year as Chief Operating Officer (COO). Over the course of his career, he enforced a wide range of federal criminal laws, especially related to firearms and violent crime. He worked undercover extensively and frequently testified in federal court as both an expert witness and a fact witness. He played an integral role in promoting the U.S. Department of Justice's adoption and use of Crime Gun Intelligence tools and tactics.

He has a B.A. in Criminal Justice from Marshall University in Huntington, West Virginia; an M.S. in Criminal Justice from Eastern Kentucky University in Richmond, Kentucky; and a J.D. from the University of Nevada-Las Vegas.

Tom is dedicated to helping make this a safer world.

**Brian Hofer**, *Chair and Executive Director, Secure Justice*

Chair, City of Oakland Privacy Advisory Commission (2016-Present)

Chair, Domain Awareness Center Ad Hoc Privacy Committee (2014-2015)

In January 2014, Brian Hofer became aware that an Orwellian sounding \$11 million-dollar city-wide surveillance system called the Domain Awareness Center was being planned for Oakland. Intended to aggregate data inputs from facial recognition software, 700 cameras, automated license plate readers, and ShotSpotter, a little sidebar to the Eastbay Express cover story about the project mentioned that a newly formed Oakland Privacy Working

Group had formed to oppose the plans, and would meet the very next day. Brian showed up to see if he could help. Three months later on March 4, 2014, and in response to overwhelming community opposition to the planned project spearheaded by Oakland Privacy, the Oakland City Council voted to dramatically scale back the project, removed the surveillance equipment from the remaining portion, and created an ad hoc committee of citizens to start drafting privacy policies for the city. Brian was appointed to and eventually chaired this committee.

In the few years since the Domain Awareness Center discussion, Brian successfully fought for a permanent committee tasked with oversight of surveillance equipment; successfully introduced ordinances throughout the greater Bay Area at both the county and city level to implement significant surveillance equipment reforms, advised on and advocated for state legislation impacting the right to privacy and surveillance oversight, and coordinated with and advised groups around the country on how to implement reforms through legislation and policy writing. Brian is presently consulting with various cities across the country regarding citizen oversight and participation pertaining to surveillance equipment and data sharing, Smart City regulations, and various “sanctuary” supporting legislative projects.

**Beryl Lipton**, *Investigative Researcher, Electronic Frontier Foundation*

Beryl has extensive experience using freedom of information (FOI) laws and large-scale public records campaigns in her research and journalism, and she regularly speaks on and teaches future journalists, academics, and activists about issues of FOI law and government surveillance.

As an investigative researcher in Electronic Frontier Foundation’s (EFF) Threat Lab, Beryl’s work focuses on government transparency, law enforcement surveillance technology and other uses of technology by government actors. At EFF, Beryl supports the Atlas of Surveillance, The Foibles and The Catalog of Carceral Surveillance, among other projects. She enjoys teaching others about the strengths and limitations of public records laws and discussing the potential and real harms of the surveillance state.

Prior to her work with EFF in 2020, she served as Projects Editor for the nonprofit MuckRock, where she focused on prison privatization and other public-private partnerships. She was a co-editor of the “...*Under Surveillance*” series from MIT Press, which features excerpts of the FBI files kept on writers, scientists and activists. She holds an undergraduate degree from Harvard College, where she concentrated in the History and Literature of America and was an active editor of The Harvard Crimson.

**Steven Oliveira**, *Deputy Chief, Sacramento Police Department*

Deputy Chief Steve Oliveira has been with the Sacramento Police Department for 28 years and oversees the Office of Operations, which consists of the department’s area commands, Patrol Division, and the Communications Center. Steve was previously Captain where he led the operations for the North Command. As a Lieutenant, he had assignments as Patrol Watch Commander, managing the Internal Affairs Division and Professional Standards

Unit, and running the Training, Research and Development Division. Earlier in his tenure was a Sergeant and supervised patrol officers and the canine unit and was a detective in the Robbery/Burglary and Homicide Units. Deputy Chief Oliveira holds a bachelor's degree from Sacramento State University in Criminal Justice and is a graduate of the Police Executive Research Forum's (PERF) Senior Management Institute for Police.

### **Panel 3: Geofences and Geofence Warrants**

**Brett Diehl**, *Trial Attorney, Federal Defenders of San Diego, Inc.*

Brett Diehl is a Trial Attorney with the Federal Defenders of San Diego. He holds a J.D. from Stanford Law School, an M.Phil. in Economic and Social History from the University of Oxford, and an A.B. in History from Princeton University. He recently co-authored a note on geofences in the Stanford Law Review and has been involved with various public defender offices' challenges to geofence warrants.

**Katelyn Ringrose**, *Global Lead for Law Enforcement and Government Access, Google*

As Google's Lead for Global Law Enforcement and Government Access, within the Government Affairs and Public Policy Branch, Katelyn works on any and all issues tied to data governance. Prior to her current position, Katelyn served as the Future of Privacy Forum's Christopher Wolf Diversity Fellow— working on data privacy and security. Through the International Association of Privacy Professionals, Katelyn holds CIPM, CIPP-EU, and CIPP-U certifications and is a 2021 Fellow of Information Privacy.

Katelyn serves as a board member for Women in Security and Privacy (WISP) in Washington, DC— and writes about issues ties to state/federal privacy legislation; sensitive personal data; and appropriate safeguards for cross-border transfers. Find Katelyn's law reviews and articles in Berkeley Tech Law Journal, Berkeley Law Review, Denver Law Review, Notre Dame Journal of Emerging Technology, Notre Dame Law Review, on IAPP, FPF's websites, and more.

**Jennifer Lynch**, *Surveillance Litigation Director, Electronic Frontier Foundation*

As Surveillance Litigation Director, Jennifer Lynch leads Electronic Frontier Foundation's (EFF) legal work challenging government abuse of search and seizure technologies through the courts by filing lawsuits and amicus briefs in state and federal courts, including the U.S. Supreme Court, on important issues at the intersection of technology and privacy.

Jennifer founded EFF's Street Level Surveillance Project, which informs advocates, defense attorneys, and decision makers about new police tools. In 2017, the First Amendment Coalition awarded her its Free Speech and Open Government Award for her years-long litigation against the Los Angeles Police and Sheriff's Departments seeking access to Automated License Plate Reader (ALPR) records and for setting new precedent in California's public records law. In 2019, the Daily Journal named her to its annual list of Top 100 Lawyers in California, and in 2021, the Daily Journal further named her to its list of lawyers who "Defined the Decade" for her work "guarding privacy in an over-

policed world.”

Jennifer has written influential white papers on biometric data collection in immigrant communities and law enforcement use of face recognition. She has also published on forensic genetic genealogy searches with the National Association of Criminal Defense Lawyers (NACDL) and on suspicionless police searches of consumer data as part of the Hoover Institution’s Aegis Paper Series. She speaks frequently at legal and technical conferences as well as to the general public on technologies like location tracking, biometrics, algorithmic decision-making, and AI, and has testified on facial recognition before committees in the Senate and House of Representatives. She is regularly consulted as an expert on these subjects and others by major and technical news media.

**Jacob Snow**, *Technology and Civil Liberties Attorney, American Civil Liberties Union*

Jacob Snow is a Technology and Civil Liberties attorney at the ACLU of Northern California, where he works on a variety of issues, including consumer privacy, surveillance, and the preservation of free speech online.

Before joining the ACLU of Northern California, Jacob was a Staff Attorney in the San Francisco office of the Federal Trade Commission, where his work covered the full breadth of the FTC’s mission. His consumer-protection work resulted in millions of dollars of judgments for consumers in false-advertising actions. Jacob’s health-care antitrust work preserved competition between health-care providers in Central and Southern California.

Jacob also litigated intellectual property cases at Orrick, Herrington, & Sutcliffe. While at Orrick, Jacob was a member of the trial team that won a jury verdict invalidating a series of online-backup patents asserted by a non-practicing entity, Oasis Research. The Oasis Research case and trial were featured on the radio program This American Life in two episodes titled When Patents Attack.

Jacob also served as a law clerk to Ronald M. Whyte, U.S. District Judge for the Northern District of California. He holds a B.A. in Physics from the University of California, Berkeley and a J.D. from Georgetown Law.

#### **Panel 4: Facial Recognition Technology**

**Skylor Hearn**, *Director of Government Affairs, Clearview AI*

Skylor has more than 27 years of progressive law enforcement experience including as former Texas Ranger Captain and DPS Deputy Director. Throughout his career, Skylor provided leadership and direction to patrol, investigations, and support operations across large geographic regions. Additionally he led highly specialized investigative units and programs including Texas Ranger Company “G” and “D”, criminal justice data collection and analysis, the forensic crime laboratory system, biometric data systems, and law enforcement and civilian training.

Skylor retired from law enforcement in 2020, where he joined K&L Gates as a Government Affairs Advisor, leveraging network and relationships in local, state, and federal government to assist clients with their mission and operational objectives.

In 2022, Skylor began working for Clearview AI where he utilizes his law enforcement expertise and legislative experience to help policy makers and law enforcement executives craft model use policies and laws nationally for the utilization of facial recognition technology and public online content by law enforcement.

Skylor remains commissioned as a Special Texas Ranger by DPS and has been recognized with the DPS Director's Citation for Criminal Interdiction as well as received the FBI Director's Award for Rescue of a Kidnapped Child.

Skylor received his Masters of Science, Criminal Justice from Lamar University, Beaumont, Texas, is an Adjunct Professor, Department of Criminal Justice at Austin Community College and lives near Austin, Texas with his family.

**Derek Sabatini**, *Lieutenant, Los Angeles County Sheriff's Department*

Derek Sabatini is a twenty-seven year law enforcement veteran. He currently holds the rank of Lieutenant with the Los Angeles County Sheriff's Department. During his career he has worked at specialized positions such as the Board of Supervisor's Liaison, Emergency Operations, and Counter Terrorism Unit. He is currently the Cal-ID Manager for Los Angeles County. As the Cal-ID Manager it is his job to manage the countywide network of biometric identification systems. He is responsible for providing over 50 law enforcement agencies in Los Angeles County with systems to book, identify and provide investigative tools for those biometrics captured at booking.

Lieutenant Sabatini has been awarded two Exemplary Service Awards and a Distinguished Service Award. In 2008 he was awarded the Los Angeles County Board of Supervisor's Annual Productivity and Quality Award. In 2017 he continued his reputation for productivity when his Cal-ID project team won the Los Angeles Digital Government Summit's Outstanding IT Project Award.

**Jennifer Jones**, *Staff Attorney, American Civil Liberties Union of Northern California*

Jennifer Jones is a Staff Attorney for the Technology and Civil Liberties program at the ACLU of Northern California, where she defends and promotes civil rights and civil liberties in the digital age, with a focus on work at the intersection of government surveillance, immigrants' rights, and racial justice.

Jennifer is a graduate of the UCLA School of Law, where she specialized in critical race studies and completed the David J. Epstein Program in Public Interest Law and Policy. In law school she served as co-chair of the Womyn of Color Collective, associate editor for the UCLA Law Review, and substantive editor for the National Black Law Journal. A UC Human Rights Fellow, she was also recognized as the winner of the Law School Admission Council's Diversity Writing Competition in 2017. Her article *Bakke at 40: Remedying Black Health Disparities Through Affirmative Action in Medical School Admissions* was

nominated by UCLA Law Review for the Scribes Law Review Award, which is presented annually to the best student-written article in a law review nationwide. Jennifer holds a bachelor's degree in sociology from UCLA and a master's of social work from the University of Southern California.

Prior to joining the ACLU, Jennifer focused on racial justice, human rights, and government misconduct litigation as an Ella Baker Intern at the Center for Constitutional Rights and as a summer intern with Advancement Project DC. Before that Jennifer worked as an advocate for youth involved with L.A. County's foster care and juvenile justice systems.









## ***Automated License Plate Readers***

To Better Protect Individuals' Privacy, Law  
Enforcement Must Increase Its Safeguards  
for the Data It Collects

*February 2020*

**REPORT 2019-118**





**CALIFORNIA STATE AUDITOR**

621 Capitol Mall, Suite 1200 | Sacramento | CA | 95814



**916.445.0255** | TTY **916.445.0033**



For complaints of state employee misconduct,  
contact us through the **Whistleblower Hotline:**  
**1.800.952.5665**

*Don't want to miss any of our reports? Subscribe to our email list at*

[auditor.ca.gov](https://auditor.ca.gov)





February 13, 2020  
2019-118

The Governor of California  
President pro Tempore of the Senate  
Speaker of the Assembly  
State Capitol  
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As directed by the Joint Legislative Audit Committee, my office conducted an audit of local law enforcement agencies' use of automated license plate readers (ALPR); the following report details the audit's findings and conclusions. In general, we determined that the law enforcement agencies we reviewed must better protect individuals' privacy through ensuring that their policies reflect state law. In addition, we found that these agencies must improve their ALPR data security, make more informed decisions about sharing their ALPR data, and expand their oversight of ALPR users.

We reviewed four agencies in detail that operate ALPR systems—Fresno Police Department, Los Angeles Police Department, Marin County Sheriff's Office, and Sacramento County Sheriff's Office. An ALPR system collects and stores license plate images of vehicles passing in its view and enables law enforcement to track a vehicle's movements over time; such a system raises privacy concerns. State law helps address these concerns by requiring agencies to have policies and safeguards in place to protect their ALPR systems from misuse. However, the agencies we reviewed either did not have ALPR policies or their policies were deficient, and they had not implemented sufficient safeguards. For example, none had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate. Furthermore, three of the four agencies have shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images. The statewide survey of law enforcement agencies we conducted found that 70 percent operate or plan to operate an ALPR system, and this raises concerns that these agencies may share the deficiencies we identified at the four agencies we reviewed. Because many of the issues we identified link to the agencies' deficient ALPR policies we recommend that the Legislature direct the California Department of Justice to develop a policy template that local law enforcement agencies can use as a model for their ALPR policies.

Our statewide survey also showed that the period of time law enforcement agencies retain ALPR images varies widely. However, among the four agencies we reviewed none had considered the usefulness of the ALPR images to investigators over time when determining their retention periods. We recommend that the Legislature amend state law to specify a maximum retention period for ALPR images.

Respectfully submitted,

A handwritten signature in black ink that reads "Elaine M. Howle".

ELAINE M. HOWLE, CPA  
California State Auditor

## Selected Abbreviations Used in This Report

ACLU	American Civil Liberties Union
ALPR	Automated license plate reader
CHP	California Highway Patrol
CJIS	Criminal Justice Information Services Division
CLETS	California Law Enforcement Telecommunications System
FBI	Federal Bureau of Investigation
GPS	Global positioning system
ICE	U.S. Immigration and Customs Enforcement
IT	Information technology
OECD	Organization for Economic Cooperation and Development

# Contents

Summary	1
Introduction	7
<b>Audit Results</b>	
The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy	15
The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk	18
The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts	32
Other Areas We Reviewed	39
Recommendations	40
<b>Appendix A</b>	
Summary of ALPR Survey Responses	45
<b>Appendix B</b>	
Scope and Methodology	49
<b>Responses to the Audit</b>	
Department of Justice	53
Fresno Police Department	55
Los Angeles Police Department	59
California State Auditor's Comments on the Response From the Los Angeles Police Department	61
Marin County Sheriff's Office	63
California State Auditor's Comments on the Response From the Marin County Sheriff's Office	67
Sacramento County Department of Human Assistance	71
Sacramento County Sheriff's Office	73
California State Auditor's Comments on the Response From the Sacramento County Sheriff's Office	77

Blank page inserted for reproduction purposes only.

# Summary

## Results in Brief

To better protect the privacy of residents, local law enforcement agencies must improve their policies, procedures, and monitoring for the use and retention of license plate images and corresponding data. The majority of California law enforcement agencies (agencies) collect and use images captured by automated license plate reader (ALPR) cameras. The ALPR system is both a real-time tool for these agencies and an archive of historical images. Fixed cameras mounted to stationary objects, such as light poles, and mobile cameras mounted to law enforcement vehicles, capture ALPR images. Software extracts the license plate number from the image and stores it, with the date, time, and location of the scan and sometimes a partial image of the vehicle, in a searchable database. The software also automatically compares the plate number to stored lists of vehicles of interest, called *hot lists* then issues alerts, called *hits* if the plate number matches an entry on the hot list. Agencies compile these hot lists based on vehicles sought in crime investigations and vehicles connected to people of interest—for example, a list of stolen vehicles or of missing persons. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists.

Because an ALPR system stores the plate number and image in a database even if the plate number does not match one on a hot list, the American Civil Liberties Union (ACLU) raised concerns in a 2013 report about law enforcement collecting and storing ALPR images related to individuals not suspected of crimes. The ACLU noted that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates—actions that do not respect individuals’ privacy. Although ALPR supporters contend that the images are collected in public places where there is no reasonable expectation of privacy, state law has made privacy a consideration when operating or using an ALPR system. Nonetheless, we found that the handling and retention of ALPR images and associated data did not always follow practices that adequately consider an individual’s privacy.

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The four local law enforcement agencies we reviewed—Fresno Police Department (Fresno), Los Angeles Police Department (Los Angeles), Marin County Sheriff’s Office (Marin), and Sacramento County Sheriff’s Office (Sacramento)—have accumulated a large number of images in their ALPR systems, yet most of these images are unrelated to their criminal investigations.

## Audit Highlights . . .

*Our audit of the use of automated license plate readers (ALPR) at four local law enforcement agencies highlighted the following:*

- » *Local law enforcement agencies did not always follow practices that adequately consider the individual’s privacy in handling and retaining the ALPR images and associated data.*
- » *All four agencies have accumulated a large number of images in their ALPR systems, yet most of the images do not relate to their criminal investigations—99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a hot list when the image was made.*
  - *None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated—since 2016—requirements.*
  - *Three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data, and the remaining agency has not developed a policy at all.*
  - *Two of the agencies add and store names, addresses, dates of birth, and criminal charges to their systems—some of these data may be categorized as criminal justice information and may originate from a system maintained and protected by the Department of Justice.*

*continued on next page . . .*

- *Three agencies use a cloud storage vendor to hold their many images and associated data, yet the agencies lack contract guarantees that the cloud vendor will appropriately protect the data.*
- *Three agencies share their images with hundreds of entities across the U.S. but could not provide evidence that they had determined whether those entities have a right or a need to access the images.*
- » *Agencies may be retaining the images longer than necessary and thus increasing the risk to individuals' privacy.*
- » *The agencies have few safeguards for creating ALPR user accounts and have not audited the use of their systems.*

For example, at Los Angeles only 400,000 of the 320 million images it has accumulated over several years and stores in its database generated an immediate match against its hot lists. In other words, 99.9 percent of the ALPR images Los Angeles stores are for vehicles that were not on a hot list at the time the image was made. Nevertheless, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to determine the vehicles present at particular locations and to track vehicles' movements at particular times in order to gather or resolve leads in investigations.

Technology gives governments the ability to accumulate volumes of information about people, raising a reasonable question: How is an individual's privacy to be preserved? Effective in 2016 the California Legislature addressed privacy with respect to ALPR systems through Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34) by establishing requirements for these systems, including requiring detailed usage and privacy policies that describe the system's purpose, who may use it, how the agency will share data, how the agency will protect and monitor the system, and how long the agency will keep the data. Yet the agencies we reviewed have not implemented all of the requirements in that law.

Law enforcement agencies must first create policies that set clear guidelines for how they will use ALPR data. Setting certain expectations in writing through an ALPR usage and privacy policy helps ensure that agencies operate their ALPR programs in a manner that better protects individuals' privacy. However, none of the four agencies have an ALPR policy that contains all of the required information. In fact, Los Angeles has not developed an ALPR policy at all. The other three agencies did not completely or clearly specify who has system access, who has system oversight, or how to destroy ALPR data. Their poorly developed and incomplete policies contributed to the agencies' failure to implement ALPR programs that reflect the privacy principles in SB 34.

ALPR systems may contain data beyond license plate images. For example, we found that Sacramento and Los Angeles are adding names, addresses, dates of birth, and criminal charges to their ALPR systems, which are then stored in those systems. Some of these data may be categorized as criminal justice information; in addition, the data may originate from the California Law Enforcement Telecommunications System (CLETS), which the California Department of Justice (Justice) maintains. These various types of data require different levels of protection under the law. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. In addition, we believe that policy from the Criminal Justice Information Services

Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI) models reasonable security measures for law enforcement agencies' ALPR data. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of the areas specified in state law.

Fresno, Marin, and Sacramento use a cloud storage solution to hold their many ALPR images and associated data. Although the three agencies told us their systems comply with CJIS policy, none of them could demonstrate the vetting they performed to confirm that their cloud storage vendor did, in fact, meet the CJIS policy standards. Moreover, none of the contracts these three agencies have with their cloud storage vendors include all necessary data security safeguards. Thus, the agencies lack guarantees that the cloud vendor will provide appropriate protection of their data.

Law enforcement agencies of all types may benefit from guidance to improve their policies and data security practices. We surveyed 391 police and sheriff departments statewide, and of those using an ALPR system, 96 percent stated that they have ALPR policies, and nearly all reported that their ALPR data storage solution complies with CJIS policy. However, it is likely that many of the survey respondents have the same problems we identified at the four agencies we visited. Justice has experience guiding law enforcement agencies to help them adhere to state law and to improve their administrative practices. By developing guidance for local agencies on needed ALPR policy elements, Justice could help them improve the quality and completeness of their policies.

State law allows law enforcement agencies to share ALPR images only with public agencies, and it requires such sharing to be consistent with respect for individuals' privacy. Three of the reviewed agencies share their ALPR images widely using features in the ALPR systems that enable convenient sharing of images with minimal effort. Fresno and Marin have each arranged to share their ALPR images with hundreds of entities and Sacramento with over a thousand entities across the United States. However, we did not find evidence that the agencies had always determined whether an entity receiving shared images had a right and a need to access the images or even that the entity was a public agency. We are concerned that unless an agency conducts verifying research, it will not know who is actually using the ALPR images and for what purpose.

In addition, the agencies have not based their decisions regarding how long to retain their ALPR images on the documented usefulness of those images to investigators, and they may be retaining the images longer than necessary, increasing the risk to individuals' privacy. Fresno's policy is to retain ALPR images for

one year; Sacramento's and Marin's policies specify two years. Los Angeles does not have an ALPR policy, and the lieutenant who administers the ALPR program stated that its protocol is to retain the images for at least five years. However, when we reviewed the agencies' ALPR searches over a six-month period in 2019, we found that personnel for three of the four agencies typically searched for images zero to six months old. Nonetheless, the agencies keep the images far longer.

The agencies we reviewed have few safeguards for the creation of ALPR user accounts and have also failed to audit the use of their ALPR systems. Instead of ensuring that only authorized users access ALPR data for appropriate purposes, the agencies have left their systems open to abuse by neglecting to institute sufficient oversight. Over the years, the media has reported that some individuals within law enforcement used or could use data systems—and sometimes ALPR systems—to obtain information about individuals for their personal use, including to locate places they regularly visit, to determine their acquaintances, and to blackmail them based on this information. ALPR systems should be accessible only to employees who need the data, and accounts should be promptly disabled otherwise. However, the agencies often neglected to limit ALPR system access and have allowed accounts that should be disabled to remain active longer than is prudent. To further ensure that individuals with access do not misuse the ALPR systems, the agencies should be auditing the license plate searches that users perform, along with conducting other monitoring activities. Instead, the agencies have conducted little to no auditing and monitoring and thus have no assurance that misuse has not occurred.

## **Recommendations**

### ***Legislature***

To better protect individuals' privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:

- Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.

- Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
- Establish a maximum data retention period for ALPR images.
- Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.

### ***Law Enforcement Agencies***

To address the shortcomings this audit identified, Fresno, Los Angeles, Marin, and Sacramento should do the following:

- Improve their ALPR policies.
- Implement needed ALPR data security.
- Update vendor contracts with necessary data safeguards.
- Ensure that sharing of ALPR images is done appropriately.
- Evaluate and reestablish data retention periods.
- Develop and implement procedures for granting and managing user accounts.
- Develop and implement ALPR system oversight.

### **Agency Comments**

The four law enforcement agencies we reviewed responded to the draft audit report. Fresno responded that it will use the audit to work to achieve its goal of building trust in its community. Los Angeles responded that it respects individuals' privacy and believes it has policies in place to safeguard information. Nonetheless, it is working on an ALPR policy as required by state law and will perform periodic audits of users' searches. Marin stated it is committed to improvement and will consider the recommendations we made, although it disagreed with several of them. Sacramento stated that it had already begun implementing many of the recommendations, but that it did not agree with how we characterized some of the findings. Justice and the Sacramento County Department of Human Assistance also responded by acknowledging the draft report, although we did not have recommendations directed to either entity.

Blank page inserted for reproduction purposes only.

# Introduction

## Background

An automated license plate reader (ALPR) is a camera that captures color images of license plates within its field of view. Fixed cameras are mounted on stationary objects, such as light poles, while mobile cameras are mounted on moving objects, such as patrol cars. Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database. An *ALPR* system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data. Although the primary focus of each image is the license plate, the image may also show part of the vehicle itself, including individuals within the vehicle, depending on the camera's position. ALPR technology has existed since the 1970s, yet widespread adoption by U.S. law enforcement agencies began only in the mid-2000s. Law enforcement agencies generally view ALPR technology as a valuable tool in achieving their missions.

We conducted a statewide survey of 391 police and sheriff departments, and the survey confirmed that ALPR use is widespread in California: 230 police and sheriff departments currently use an ALPR system, and 36 plan to use one. Table 1 provides an overview of the ALPR systems of the four law enforcement agencies we reviewed as part of this audit.

**Table 1**  
**ALPR Systems of Four Audited Law Enforcement Agencies**

LAW ENFORCEMENT AGENCY	NUMBER OF AGENCY PERSONNEL WITH ACCESS TO ALPR DATA	NUMBER OF CAMERA SYSTEMS		CURRENT ALPR VENDOR	DATE AGENCY BEGAN USING CURRENT ALPR VENDOR
		FIXED	MOBILE		
<b>Fresno</b>	231	0	8	Vigilant Solutions, LLC	2016
<b>Los Angeles</b>	13,000	3	393	PIPS Technology*	2007
<b>Marin</b>	38	0	3	Vigilant Solutions, LLC	2010
<b>Sacramento</b>	539	33	27	Vigilant Solutions, LLC	2012

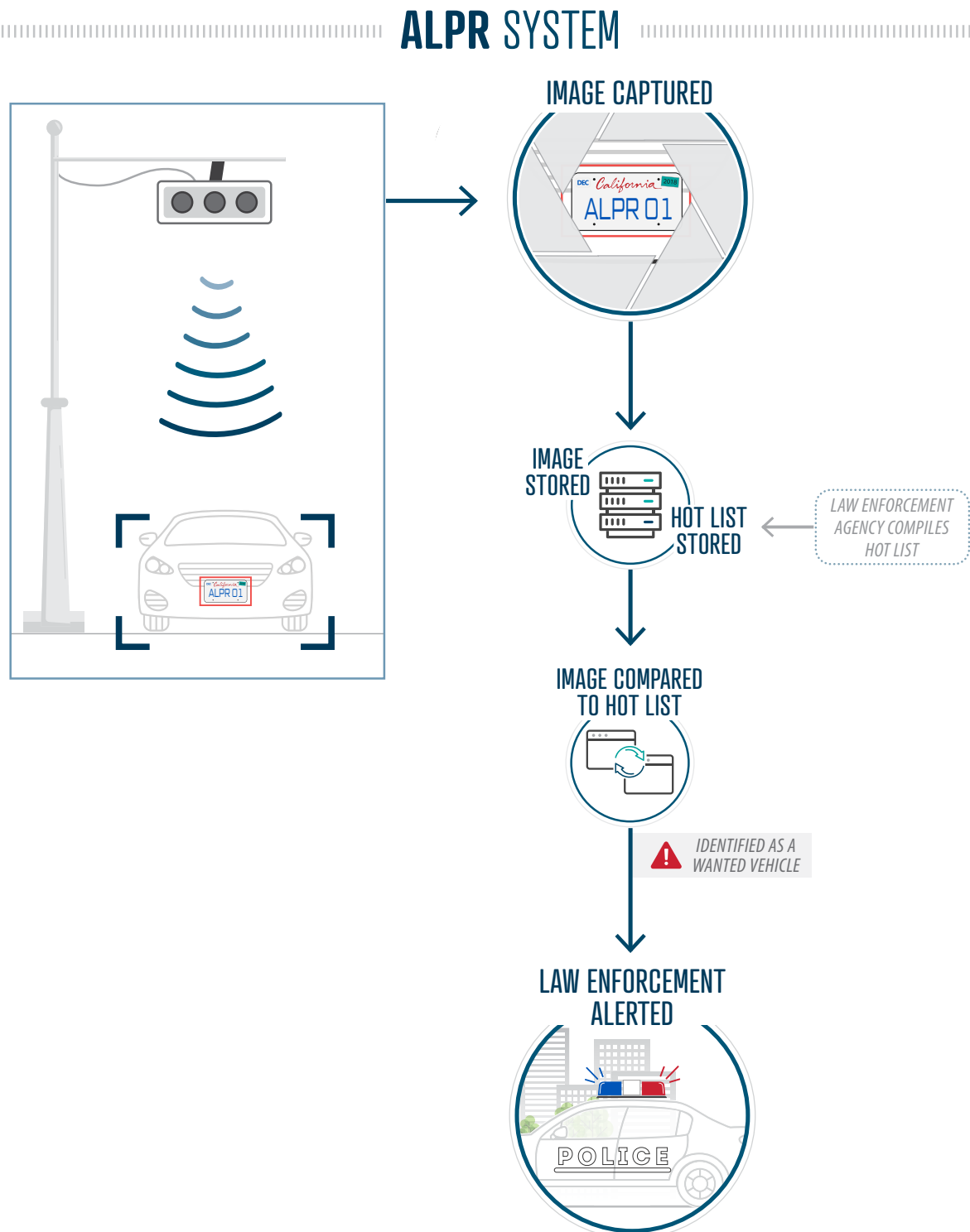
Source: Analysis of reports on ALPR systems as of 2019 and the agencies' survey responses.

\* Los Angeles uses PIPS Technology cameras and a user interface from Palantir Technologies, Inc.

An ALPR system is both a real-time tool for law enforcement agencies and an archive of historical information. After the ALPR system identifies a license plate number in an image, it compares the plate number to stored lists of license plate numbers from vehicles of interest, called *hot lists*. Figure 1 shows how an ALPR system uses hot lists to search stored images. Local law enforcement agencies create their own hot lists and also obtain hot lists from state and federal agencies. For example, the California Department of Justice (Justice) provides hot lists to local agencies that include license plate numbers associated with missing persons, gang members, and suspected terrorists. We use the term *ALPR data* to describe all the information stored in an ALPR system, including license plate images and hot lists. Regardless of whether a license plate number matches a plate on a hot list (a *hit*), an ALPR system stores the plate image in a database, creating a searchable archive. Officers may search the database in various ways. For example, they may search for a full license plate number to locate a specific vehicle, search for a partial license plate number to locate a group of vehicles, or search for all vehicles recorded at a particular location at specific times.

Law enforcement agencies can share ALPR data with other public agencies. In the ALPR systems we observed, the agency could choose to share ALPR images only, to share hot lists only, or to share both. Accessing ALPR images shared from other jurisdictions enables agencies to search a broader area, such as across county and state lines. In addition, even if an agency does not operate ALPR cameras itself, it can, through sharing agreements, access ALPR images other agencies collect. Our statewide survey showed that among agencies that operate ALPR systems, roughly 84 percent share their images. Sharing hot lists also enables broader search coverage. For example, an agency could share a hot list that provides license plates linked to wanted individuals with other entities in the region. These entities would then receive hit alerts if their cameras detected those plates.

**Figure 1**  
How ALPR Systems Work



Source: Analysis of David J. Roberts and Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, Washington, D.C., 2012.

### ALPR Vendors Most Commonly Used in California

Law enforcement agencies typically contract with a third-party vendor for an ALPR system. In our statewide survey, most—70 percent—of those that have an ALPR system reported using a company called Vigilant Solutions, LLC (Vigilant). Figure A.1 in Appendix A summarizes these responses. Three of the agencies we reviewed—the Fresno Police Department (Fresno), Marin County Sheriff’s Office (Marin), and Sacramento County Sheriff’s Office (Sacramento)—contract with Vigilant. The Vigilant ALPR system provides a user interface to search license plates and the option to share ALPR images and hot lists with other agencies through the Vigilant system. Fresno, Marin, and Sacramento all store their ALPR images on Vigilant’s server, which is a cloud service, and share their images with other agencies that subscribe to Vigilant’s services. Roughly 22 percent of the survey respondents that have ALPR systems use a company called PIPS Technology. One of the agencies we audited in depth, the Los Angeles Police Department (Los Angeles), purchased its cameras from PIPS Technology, but it stores the images on its own server. Los Angeles uses a software platform called Palantir for the user interface that allows for searches of its ALPR images, and it shares its ALPR images with other agencies in the region that use the Palantir user interface.

#### Key Elements Law Enforcement Agencies Must Include in Their ALPR Usage and Privacy Policy

- The authorized purpose for using the ALPR system and collecting, accessing, or using ALPR data.
- A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR data.
- The training requirements for those employees and independent contractors authorized to use or access the ALPR system, or to collect ALPR data.
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- The purposes of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time ALPR data will be retained, and the process for determining if and when to destroy retained ALPR data.

Source: Analysis of state law.

#### State Laws Governing ALPR Systems and Data Sharing

With few exceptions, California law requires public agencies that operate and use ALPR systems to implement a usage and privacy policy. The Legislature passed Senate Bill 34 (Statutes of 2015, Chapter 532) (SB 34), effective January 1, 2016, to establish requirements regarding the operation and use of ALPR systems. This law generally requires public agencies, including law enforcement agencies, that operate or use an ALPR system to maintain reasonable security procedures and practices to protect ALPR data, to implement a usage and privacy policy, to make that policy available to the public, and to post that policy on its website should the agency have one, among other provisions. The text box describes required elements of an agency’s ALPR usage and privacy policy.

SB 34 does not specify retention periods for ALPR data, although another state law limits the California Highway Patrol (CHP) to retaining its ALPR images for no more than 60 days, unless those images are being used for felony investigations or as evidence. Agencies implementing ALPR programs after January 1, 2016, must also provide an opportunity for public comment before implementing the program.

In 2018 another state law took effect that limits the information law enforcement agencies can share for immigration enforcement purposes and requires Justice to issue guidance to state and local law enforcement agencies regarding these limitations as they apply to law enforcement databases. In October 2018 Justice issued this guidance, which can also serve as best practices for law enforcement agencies on how to lawfully share ALPR images. The guidance encourages law enforcement agencies that maintain databases to inquire about the purpose for which the other law enforcement agency intends to use the information contained in the database. If a law enforcement agency intends to use the information for immigration enforcement purposes, Justice states that law enforcement agencies should require, as a condition of accessing the database, an agreement that stipulates that access will be made only in cases involving individuals with criminal histories, or for information regarding the immigration or citizenship status of an individual. Beyond this guidance and the hot lists Justice provides to local law enforcement agencies, as we describe earlier, Justice plays no other role in ALPR programs.

State law requires law enforcement agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, destruction, use, modification, or disclosure. These requirements mean that ALPR data are sensitive. For comparison purposes, the California Department of Technology Office of Information Security defines *sensitive data* for state agencies as information that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. In addition to ALPR images and hot lists, a law enforcement agency can enter other information into its ALPR system, such as personal information and criminal justice information. *Personal information* is information that identifies or describes an individual, including name or physical description. SB 34—whose purpose was, in part, to institute reasonable privacy standards for the operation of ALPR systems—requires that ALPR data be protected with reasonable operational, administrative, technical, and physical safeguards to ensure their confidentiality. Thus, personal information in an ALPR system also requires appropriate and reasonable safeguards. *Criminal justice information*, as defined by the Criminal Justice Information Services Division (CJIS) of the U.S. Federal Bureau of Investigation (FBI), refers to data necessary

for law enforcement and civil agencies to perform their missions. This includes information about vehicles associated with crimes, when accompanied by personal information.

When CJIS provides criminal justice information to law enforcement agencies, it requires those agencies to comply with a minimum set of information technology (IT) security requirements to protect the information, and these requirements can serve as best practices for agencies to follow. Because an agency can enter personal information and criminal justice information into its ALPR system, either as part of a hot list or as a comment added as part of a license plate search, all ALPR data are sensitive and require appropriate safeguards.

### **Privacy Concerns Related to ALPR Systems**

Although law enforcement agencies collect ALPR images in public view, and there is no reasonable expectation of privacy regarding a license plate, the use and retention of those images raises privacy concerns. The agencies we reviewed accumulate a large number of images in their ALPR systems. For example, Sacramento recorded 1.7 million images in one week, and Los Angeles currently has more than 320 million images in its ALPR database that it has accumulated over several years. The majority of these images do not generate hit alerts. For example, data from the Los Angeles system show that at the time of our review only 400,000 (0.1 percent) of the 320 million images Los Angeles has stored generated an immediate match against its hot lists for vehicles associated with car thefts, felonies, or warrants. However, the stored images provide value beyond immediate hit alerts, as law enforcement personnel can search the accumulated images to target the whereabouts of vehicles at particular times or locations. This storage, retention, and searching of the images, although valuable to law enforcement, has the potential to infringe on individuals' privacy.

Organizations such as the American Civil Liberties Union (ACLU) have criticized law enforcement agencies' collection of ALPR images because of the risks it poses to privacy. The ACLU stated that increasing numbers of cameras, long data retention periods, and sharing of ALPR images among law enforcement agencies allow agencies to track individuals' movements in detail, and it has voiced concerns that such constant monitoring can inhibit the exercise of free speech and association. The ACLU has also raised concerns that law enforcement officers could inappropriately monitor the movements of individuals such as ex-spouses, neighbors, and other associates. There have been occurrences of officers misusing law enforcement databases like those that contain ALPR images. In 2016 the Associated Press conducted a review that found more than

325 instances between 2013 and 2015 in which law enforcement officers who misused databases were fired, suspended, or resigned, and more than 250 instances of reprimands or lesser discipline related to such misuse. For example, the Associated Press reported on a police sergeant in Ohio who pleaded guilty to stalking his ex-girlfriend after he searched law enforcement databases for personal information about her and also the woman's mother, her close male friends, and students from a course she taught.

Law enforcement has recognized the privacy concerns posed by the operation of ALPR systems, yet it has also pointed to the usefulness of the systems. For example, the Police Executive Research Forum (police research forum) and the Mesa Police Department (Mesa) in Arizona conducted a study of the effectiveness of ALPR systems for Mesa's auto theft unit in 2011. They found that officers got nearly three times as many stolen vehicle hits and made about twice as many vehicle recoveries when using an ALPR system, compared to officers performing manual license plate checks. Law enforcement has also found ALPR systems useful for investigations. For example, the assistant chief of the Minneapolis Police Department told the police research forum in 2012 that the department located a vehicle associated with a domestic kidnapping case by searching ALPR images. With regard to the retention of ALPR images, the International Association of Chiefs of Police (chiefs' association) acknowledged the tension between long retention periods and privacy. The chiefs' association noted that a reluctance to destroy records may stem from investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings further details to light. However, the chiefs' association also recognized the privacy risks of ALPR images. In a 2009 report, it stated that mobile ALPR cameras could record license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, and staging areas for political protests. The chiefs' association argued that establishing policies regulating ALPR programs could mitigate privacy concerns, and it produced a report in 2012 offering guidance on developing such policies.

### **Federal Guidance on Privacy Protection**

As far back as 1973, the federal government acknowledged that individuals' privacy needs to be protected from arbitrary and abusive record-keeping practices. The U.S. Department of Health, Education, and Welfare, as it was then known, identified principles for the fair collection, use, storage, and dissemination of personal information by electronic information systems. Over time the principles were adapted into information practices. According to the U.S. Government Accountability Office, a revised version of the information practices was published in 1980 by

the Organization for Economic Cooperation and Development (OECD)—an international organization that works with governments, policymakers, and citizens on social, economic, and environmental challenges—and with some variation, these practices form the basis of privacy laws in the United States and around the world. The OECD updated its eight information practices in 2013, and California’s lawmakers included many of these information practices in SB 34. For example, the OECD’s information practices describe the importance of an organization specifying the purposes for which it is collecting and using data; keeping data reasonably safe from the risk of unauthorized access, destruction, use, modification, and disclosure; being open about policies involving data; and being accountable for complying with the information practices.

The U.S. Supreme Court (court) has not directly decided a case that we could find addressing ALPR images, although it has decided cases involving other electronic surveillance. Because license plates are in plain view, the collection of license plate images by law enforcement is not a per se violation of the Fourth Amendment’s prohibition against unreasonable searches and seizures. However, the court has found that certain electronic data that reveal individuals’ movements over an extended period of time, if gathered, do at some point impinge on privacy. The court has specifically addressed these issues with respect to the use of global positioning system (GPS) data and cell-site location information, which is location information linked to cellphone use. Cell-site location information—similar to ALPR images—provides data on an individual’s continuous movements over a potentially unlimited period of time. In a 2018 case involving cell-site location information, the court stated that “[a] person does not surrender all [privacy] protections by venturing into the public sphere.” The court continued, “With access to [cell-site location information], the Government can now travel back in time to retrace a person’s whereabouts,” and noted that the information was collected on everyone, not only “persons who might happen to come under investigation.” Thus, even though case law on electronic data that enable tracking of individuals’ movements over an extended period of time is still evolving, the court has recognized that privacy implications exist for such data, which can include ALPR images.

## Audit Results

### **The Four Law Enforcement Agencies We Reviewed Have Not Consistently Fulfilled Requirements Designed to Protect Individuals' Privacy**

California's lawmakers drafted current ALPR law to institute reasonable privacy standards for the operation of ALPR systems. As we discuss in the Introduction, technology gives governments the ability to accumulate significant amounts of information about people, raising the question of how individuals' privacy is to be preserved, and the federal and state governments and courts have issued laws and guidance—including, in the case of California, SB 34—related to the use of such information.

Yet local law enforcement agencies—specifically the four agencies we reviewed—have not done all they could to respect individuals' privacy by incorporating the requirements and concepts in SB 34 into their operations. With few exceptions, SB 34 requires a public agency that operates or uses an ALPR system to implement a usage and privacy policy that describes how the system will be used and monitored to ensure the security of the ALPR data accessed or used. The agencies we reviewed have mature ALPR programs—they have been using their current ALPR vendors since as far back as 2007. However, as we discuss later, we found that the agencies have risked individuals' privacy by not making informed decisions about sharing ALPR images with other entities, by not considering how they are using ALPR data when determining how long to keep it, by following poor practices for granting their staff access to the ALPR systems, and by failing to audit system use.

State law requires law enforcement agencies to administer ALPR programs in ways that respect individual's privacy and protect ALPR data. The law also requires the agencies to have a written usage and privacy policy that sets forth how they will operate and use their ALPR systems. These usage and privacy policies must include the following elements:

- Authorized purposes for using the ALPR system and collecting the data.
- A description of the job title or other designation of individuals who are authorized to use or access the ALPR system.
- Training requirements for the authorized individuals who will use or access the ALPR system.
- A description of how the agency will monitor the ALPR system to ensure the security of the data and compliance with privacy laws.

- The purpose of, process for, and restrictions on the sale, sharing, or transfer of ALPR data.
- The length of time the ALPR data will be retained and the process used to determine if and when to destroy retained ALPR data.

Agencies may expand on these required elements as needed to ensure that their collection, use, maintenance, sharing, and dissemination of ALPR data are consistent with respect for individuals' privacy.

None of the four agencies we reviewed have an ALPR policy that contains all of the required information, thereby contributing to the agencies' failure to implement programs that reflect the privacy principles in SB 34. Los Angeles has not developed an ALPR policy, and the policies of the other three agencies are deficient in various ways, as Figure 2 shows. For example, all have failed to fully address how they will monitor system use to ensure compliance with applicable privacy laws, which likely contributed to their failure to institute regular audits of user searches. The agencies could have avoided concerns such as those shown in Figure 2, which we describe later in this report if they had developed more thorough policies. Clear policies that define the purposes and procedures for monitoring ALPR systems help agencies meet their goals.

**Figure 2**

The Agencies' ALPR Policies Are Missing Required Key Elements for Respecting Individuals' Privacy



Source: State law and the agencies' ALPR policies as well as interviews with the agencies' management.

As a result of our audit, each of the four agencies is making or considering changes to its policies. The ALPR administrators at Fresno, Marin, and Sacramento agreed that their policies did not contain one or more elements required by state law. They also explained that they did not include certain policy requirements they believed did not apply to their use of ALPR data. For example, Sacramento's ALPR policy does not describe ALPR data-selling restrictions because, according to the ALPR administrator, Sacramento does not currently sell ALPR data. However, because their policies are incomplete and do not specify what personnel cannot do when interacting with their ALPR systems, these three agencies left out critical guidance to staff and increased the risk that staff would use the ALPR system inappropriately. The program administrators at Fresno, Marin, and Sacramento told us that they will consider changes to their policies subsequent to our audit. Although the lieutenant who serves as Los Angeles' program administrator initially believed that the agency's many IT policies covered the ALPR program, when we brought the deficiencies in oversight to his attention, he acknowledged the need for Los Angeles to have an ALPR policy and began drafting one in October 2019.

We are concerned that the policy deficiencies we found are not limited to the agencies we reviewed, and thus law enforcement agencies of all types may benefit from guidance to improve their policies. We surveyed 391 police and sheriff departments statewide about their ALPR programs, and many stated that they have ALPR policies and that these policies are publicly available. Because state law requires each agency that operates or uses an ALPR system to implement a usage and privacy policy, and to make the policy available to the public in writing and post it conspicuously on the agency's website, we inquired about how agencies throughout the State were adhering to these requirements. Of the law enforcement agencies using an ALPR system, 96 percent responded that they have ALPR policies. Of this group, at least 70 percent stated that they have posted their policy to their website. A breakdown of the law enforcement agencies' responses to our survey can be found at <http://auditor.ca.gov/reports/2019-118/supplemental.html>. However, we believe it is likely that many of the survey respondents will have the same problems with the quality and completeness of their policies as the four agencies we visited. As we discuss in the Introduction, Justice has issued guidance to law enforcement agencies to help them understand how to adhere to state law regarding the sharing of information for immigration enforcement purposes. Given Justice's experience and broad reach in the law enforcement community, developing guidance for local law enforcement agencies on needed policy elements could improve the quality and completeness of their policies.

***Fresno, Marin, and Sacramento have incomplete ALPR policies, which increases the risk that staff will use the ALPR systems inappropriately.***

### **The Law Enforcement Agencies Have Often Placed Their ALPR Data at Risk**

Administering ALPR programs in ways that respect individuals' privacy requires a thoughtful and considered approach to data management that the agencies we reviewed have not always taken. Specifically, three of the agencies have agreed to share their images widely with little knowledge of the receiving entities and their need for the images. Moreover, the agencies have not based their decisions regarding retention of images on their actual usefulness to investigators and may be retaining the images longer than necessary, increasing the risk to individuals' privacy.

### ***The Agencies May Not Be Adequately Protecting Their Sensitive ALPR Data***

Law enforcement agency personnel can upload or enter sensitive information into their ALPR systems, which may require specific safeguards. As we discuss in the Introduction, this sensitive information could include personal information and criminal justice information. In addition, these data may originate from the California Law Enforcement Telecommunications System (CLETS)—a system that allows law enforcement agencies to obtain information from federal and state databases, such as arrests and fingerprint records from Justice. In reviewing multiple agencies' ALPR policies, we found several that stated that their ALPR systems may contain information obtained through CLETS. Additionally, in a security and compliance memorandum, Vigilant acknowledged that law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.

*Law enforcement users can upload personal information and criminal justice information into the Vigilant system through hot lists and open text fields.*

For example, in addition to license plate images, Sacramento and Los Angeles add data to their systems such as criminal charges and warrant information, in combination with personal information such as names, addresses, dates of birth, and physical descriptions. The added data can be in the form of hot lists that agencies use to search for license plates of interest, as shown in Figure 1 in the Introduction, or they can be data that are entered into open text fields. By running an automated function each day, Sacramento extracts information from several databases and uploads the information as hot lists to its ALPR system. Los Angeles does not create its own hot lists, but it regularly downloads hot lists from Justice and the Los Angeles County Sheriff's Department, then uploads the hot lists to its ALPR system. Another way that information in addition to license plate images gets into an ALPR system is by users adding it to open text fields. Data entered into open text fields are generally associated with license plate searches.

When conducting a search, staff are prompted to enter a case number and the purpose of the search, and they may do so by typing in text. The ALPR systems store this open text in their audit logs, which detail user activity and the reasons for the activity.

In contrast to Sacramento and Los Angeles, Marin and Fresno occasionally upload hot lists into their ALPR systems. With regard to open text fields, we reviewed the audit logs for Marin and Fresno and did not find personal information in combination with other sensitive information in the six months of search records we studied. However, the possibility exists that law enforcement personnel could enter sensitive information into open text fields during ALPR searches.

When an IT system lacks sufficient security, the system is at risk of misuse and data breaches. Systems containing personal information and criminal justice information must have adequate protections to assure individuals' privacy. However, as discussed in the Introduction, ALPR data can originate from different sources, and the source of the information may drive some of the required IT security protocols. On one hand, CJIS developed a policy that dictates the minimum standards that law enforcement agencies must follow to protect criminal justice information they obtain from the FBI (CJIS policy). On the other hand, users of Justice's CLETS system must follow the protections outlined in the CLETS *Policies, Practices and Procedures* document, which describes formal security measures law enforcement agencies must follow to access and protect CLETS information in addition to the CJIS policy requirements.

Further, it can be difficult to know what protections to apply to data from different sources. For example, an individual's address obtained by searching the Department of Motor Vehicles database through CLETS would be subject to Justice's data security requirements, but the same information obtained from a local law enforcement agency database would not. Moreover, the personal information Los Angeles and Sacramento have entered into their ALPR search records does not include its origin, making the required level of protection unclear.

Given these issues and the need to identify a standard that can be uniformly applied to ALPR data regardless of their source, we believe that CJIS policy provides reasonable security measures for law enforcement agencies to protect all of their ALPR data. State law requires these agencies to maintain reasonable security procedures and practices to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure. CJIS policy specifies operational, administrative, technical, and physical safeguards for each of these areas. For example, CJIS policy

***When an IT system lacks sufficient security, the system is at risk of misuse and data breaches.***

*We are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards.*

requires agencies to ensure that their sensitive data are encrypted, and it limits physical access to specific personnel authorized to access the data. Nearly all of the 230 agencies that reported using ALPR systems in response to our statewide survey—including Fresno, Los Angeles, Marin, and Sacramento—reported that their ALPR data storage solution complies with CJIS policy.

Nevertheless, we are concerned that the agencies using Vigilant may not be protecting their ALPR data in conformity with CJIS policy standards. Fresno, Marin, and Sacramento store their ALPR data in Vigilant's cloud database, and CJIS policy requires agencies to ensure that the cloud vendors that store and process their criminal justice information comply with its security requirements. Such requirements include controlling physical access to sensitive data, encrypting the data, and conducting background checks and training for employees with access to criminal justice information. In addition, before providing sensitive data to a vendor, CJIS requires law enforcement agencies to identify necessary authentication and monitoring controls, such as two-factor authentication and activity logging. Because the Vigilant software is by default accessible via the Internet, an officer may be able to access it using his or her personal device. The ability to access ALPR data in this manner bypasses the agencies' network security safeguards and violates CJIS policy requiring agencies to monitor and control access to the data.

One way to prevent users from signing in to the Vigilant system using personal devices would be to implement authentication controls, such as two-factor authentication. Two-factor authentication involves a second level of verification, such as a passcode sent to a specific device, and allows agencies to require that the passcode be sent only to department-issued devices. Although Vigilant offers two-factor authentication, Marin, Fresno, and Sacramento do not use it. CJIS policy requires two-factor authentication only for systems that directly access federal systems. However, this requirement recognizes that two-factor authentication is more secure than a basic username and password login for systems like Vigilant that are accessible over the Internet. Thus, two-factor authentication could serve as a best practice for agencies to prevent inappropriate access to their ALPR systems.

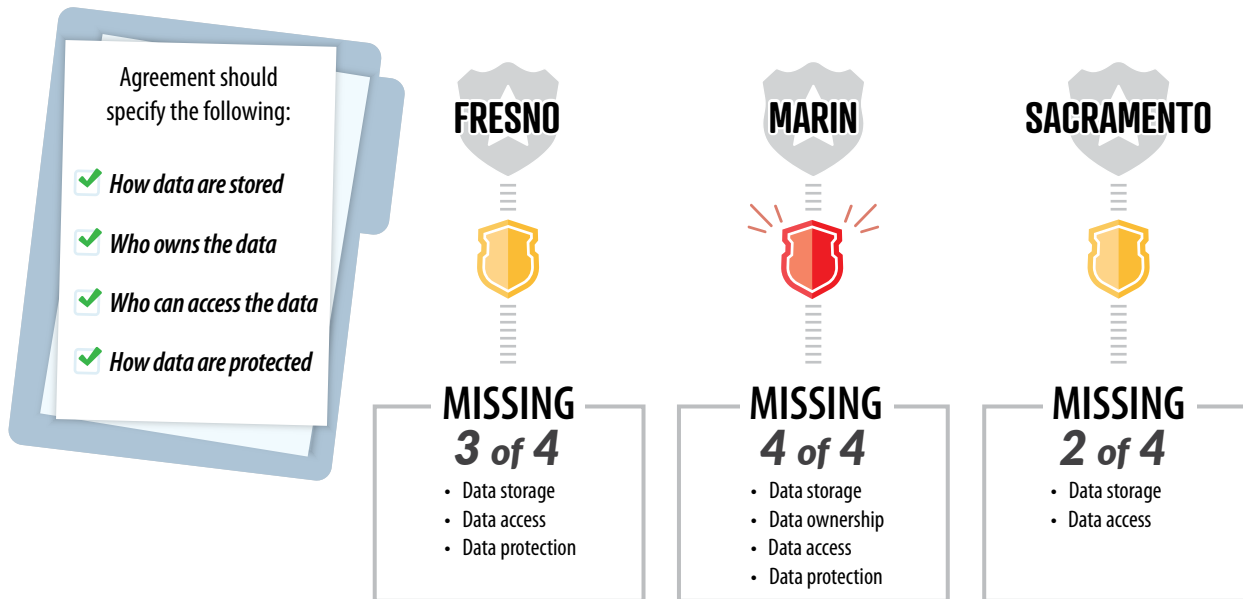
In addition, monitoring the activity logs can alert program administrators to unauthorized access of their ALPR systems. CJIS policy requires agencies to monitor access to systems that contain criminal justice information. Vigilant provides its clients with logs of network addresses that have accessed their ALPR systems, and although Marin's ALPR program administrator stated that he reviews these logs, administrators from Sacramento and Fresno confirmed that they do not. Reviewing the logs of system access

could help the agencies monitor access to their ALPR systems and detect whether someone accesses the ALPR system from an unrecognized network address.

When law enforcement agencies provide sensitive information to ALPR vendors, their contracts should provide assurance that the vendor will adequately protect that information. CJIS policy recommends several provisions that law enforcement agencies should consider including in their contracts to ensure that cloud vendors adequately protect criminal justice information. For example, a contract that protects a law enforcement agency's data would make clear that the agency owns the data it uploads into the ALPR system, that the agency's data will not be stored outside of the United States or Canada, and that employees at the cloud vendor who have access to unencrypted criminal justice information will undergo training and background checks. Without these contract provisions, agencies lack guarantees that the cloud vendor will implement appropriate protections of their data.

We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts. As Figure 3 shows, none of the agencies' contracts with Vigilant meet all of the CJIS data security requirements. For example, the agencies' contracts do not state that Vigilant will store their data in the United States or Canada. Marin's contract does not make clear that Marin owns the data it adds to the ALPR system. It is important to note that Vigilant claims to implement data security measures that comply with CJIS policy. In a security and compliance memorandum, Vigilant lists steps it takes to encrypt data that may contain criminal justice information, as well as physical and network security safeguards it has in place to prevent unauthorized access to its ALPR cloud. We have no basis to dispute Vigilant's claims, but without strong contract provisions requiring CJIS safeguards, the three agencies have no guarantee that Vigilant will protect their data. As CJIS policy states, ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

***We found that the three agencies storing ALPR data in Vigilant's cloud—Fresno, Marin, and Sacramento—do not have sufficient data security safeguards in their contracts.***

**Figure 3****The Agencies' Existing Agreements With Vigilant Do Not Contain Adequate Data Security Measures**

Source: Agencies' agreements with Vigilant and CJS policy requirements.

A lack of IT department involvement and outdated contracts likely contributed to the data security weaknesses we observed. Fresno, Marin, and Sacramento have IT units that administer their systems and ensure compliance with Justice's data security requirements. However, at Fresno and Marin, the IT units are responsible for network security and have little oversight of the ALPR systems' data security. According to Fresno's IT manager, Fresno's main IT unit does not manage user accounts or monitor access to the ALPR system. Fresno has an IT analyst separate from the main IT unit who currently helps administer user accounts and provides technical support for the ALPR system; however, his background is not in network security. A deputy in Marin's auto theft unit manages Marin's entire ALPR system—including user accounts and training. This arrangement is not ideal, since individuals outside of an agency's IT department may lack the expertise necessary to implement adequate data security safeguards. According to Sacramento's ALPR administrator, Sacramento's IT unit recently assumed responsibility for the ALPR system, but before about April 2019, an officer outside of the IT unit administered the ALPR system.

In addition, with the exception of Sacramento, the agencies have not updated their contract terms with Vigilant for several years. The agencies' contracts renew each year when the agencies pay a service fee to Vigilant. As a result, Fresno has not updated its contract for three years, and Marin for nine years. Sacramento updated

its contract terms with Vigilant in September 2019, after using its previous agreement for seven years. Agreements that are not kept current may reflect outdated practices or omit needed assurances, increasing the risk that data are not protected.

Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access. Los Angeles stores its ALPR data in a city-controlled data center rather than in a vendor cloud like the agencies that use Vigilant. Nevertheless, Los Angeles contracts with Palantir for IT support, and the FBI's 2017 audit of Los Angeles' data security practices identified Palantir as an entity with access to criminal justice information; thus we expected Los Angeles' agreement with Palantir to meet CJIS policy requirements. CJIS policy requires agencies to enter into agreements with vendors that access their criminal justice information. The agreements are to include an FBI-drafted security addendum that outlines specific safeguards a vendor agrees to put in place to comply with CJIS policy and an acknowledgment by the vendor of the great harm that may arise from misusing sensitive data. However, in response to our request for its agreement with Palantir, Los Angeles produced two expired contracts and a 2018 commodities agreement extending its licensing and support for Palantir software. None of these documents contained the FBI-drafted security addendum. Thus Los Angeles was not able to demonstrate that its agreement with Palantir contains appropriate data protections to ensure that Palantir employees with access to Los Angeles' ALPR data will not use the data for unauthorized purposes.

*Los Angeles was not able to demonstrate that it has an agreement in place to protect its ALPR data from inappropriate access.*

### ***The Agencies Have Not Made Informed ALPR Image-Sharing Decisions***

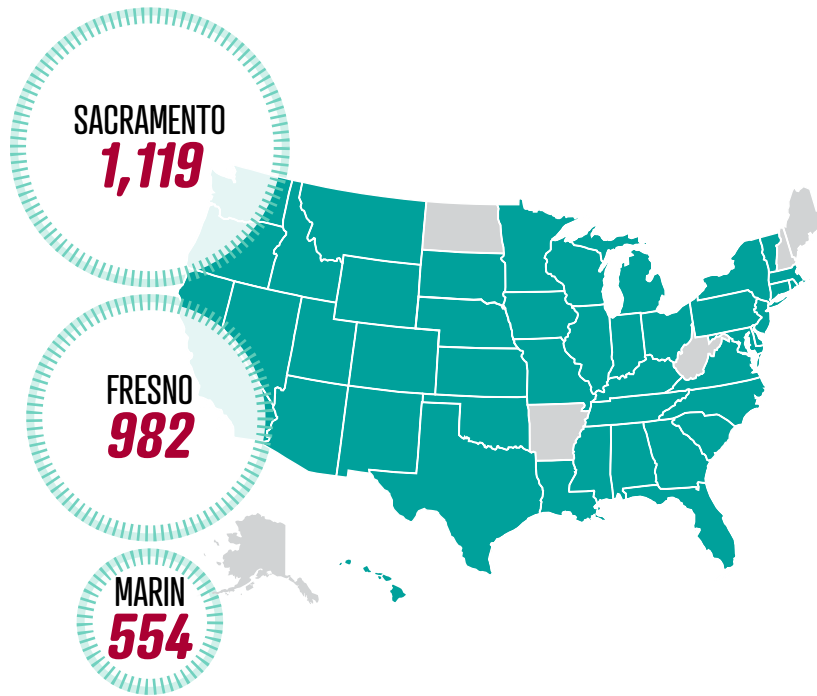
A significant feature of ALPR systems is their ability to share information with users across other organizations. A variety of requirements and guidance exist regarding how law enforcement agencies should share ALPR data, including images. ALPR images contain the date, time, and location of the scanned license plate and largely relate to vehicles that are not linked to crimes. The risk that the images will be misused rises as the images are more widely distributed, and there are numerous examples of law enforcement officers misusing their access to various databases. For example, an Associated Press article from 2016 reported a case from the state of Georgia in which an officer accepted a bribe to search for a woman's license plate number to see whether she was an undercover officer. Although such an example of misconduct is not representative of all law enforcement personnel, it illustrates the need for appropriate safeguards over law enforcement tools. Once a license plate is tied to an individual's identity, which is easy for a law enforcement officer to do, ALPR images may make it possible to track that individual's movements.

State law allows local law enforcement agencies to share ALPR images only with public agencies and requires sharing to be consistent with respect for individuals' privacy. Further, guidance that Justice issued in October 2018 addresses the agencies' governance of databases in relation to immigration enforcement, and this guidance provides a best practice for sharing in general. In the guidance, Justice encourages law enforcement agencies to inquire regarding the purpose for which an agency seeking access to their database intends to use the information and then, as a condition for accessing the database, to require agreements ensuring appropriate use of the data if its purpose includes immigration enforcement. The chiefs' association also recommends that law enforcement agencies maintain ALPR image-sharing records that include information on how the requester intends to use the images. The four agencies we reviewed asserted that they share ALPR images with others on the principle that these entities have a right and need to know the information. Because following state law necessitates establishing an agency's identity, i.e., the right to know, and Justice's guidance suggests establishing the purpose, i.e., the need to know, for which an agency intends to use the images, the agencies' position seems consistent with state law and Justice's guidance.

*We could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency.*

However, we had difficulty determining whether the reviewed agencies have actually made informed decisions about sharing their ALPR images. Fresno and Marin have each approved sharing their ALPR images with hundreds of entities, and Sacramento with over a thousand. Many of these entities are within California, but they also span most of the other 49 states. Figure 4 shows the entities' locations, illustrating how widely distributed access to these ALPR images is. In addition, we could not always ascertain how the agencies determined whether an entity receiving access to images had a right and need to access them or even whether the entity was a public agency. We reviewed the lists of entities and found one that appeared to be a non-public entity and others that were unidentifiable because they were listed only by initials. For example, Fresno, Marin, and Sacramento all approved an entity listed as the Missouri Police Chiefs Association (Missouri Association); however, this is not a public agency but rather a professional organization that provides training opportunities and advocates for pro-law enforcement legislation. However, none of the agencies could demonstrate that they had evaluated the Missouri Association before sharing images, nor could they tell us why the Missouri Association had a right to those images. When we inquired with Vigilant, an official explained that despite the name, it is the Missouri State Highway Patrol—a law enforcement agency—that uses the account. The lists contain many other entities whose identities and law enforcement purposes are not immediately evident. Unless a law enforcement agency verifies each entity's identity and its right to view the ALPR images, the agency cannot know who is actually using them. Although the three agencies reviewed their sharing arrangements to varying degrees during our audit, none could demonstrate that they perform this kind of verification before sharing their ALPR images.

**Figure 4**  
Three Agencies Have Authorized Sharing With Entities Located in States Across the Nation



Source: Analysis of data-sharing reports from the Vigilant system.

Similarly, even when an entity is a verified public agency, it is not always evident that agencies are making informed decisions by establishing the entity's need for the ALPR images. Fresno, Marin, and Sacramento all authorized sharing with the Honolulu Police Department, but given the distance between California and Hawaii and the limited instances of cars traveling between the two states, it is uncertain whether the Honolulu Police Department has a persuasive need for these ALPR images. Fresno's ALPR administrator agreed that not a great deal of thought went into its decision to share with the Honolulu Police Department, and he believes that it probably authorized the share because the entity was a law enforcement agency. In contrast, Marin's ALPR administrator believes that sharing ALPR images widely is important because the more information available to law enforcement, the more successful it can be in its mission. However, sharing decisions should also consider the importance of protecting individuals' privacy. Each authorized share exposes the ALPR images to greater risk of misuse; therefore, the agencies should approach each sharing request individually based on the requester's actual need for the images.

The three agencies have also relied on features in Vigilant's software rather than establishing their own practices for sharing their ALPR images. A sound approach to sharing would include establishing each requesting entity's need to know and right to know and keeping records of the assessment and resulting decision. However, none of these agencies maintain records outside of the Vigilant user interface of when or why they agreed to share with particular entities, and neither Marin nor Sacramento includes a process for approving sharing requests in their ALPR policies as state law requires. Fresno has outlined procedures that incorporate these elements, but it has not followed them. Fresno's ALPR administrator explained that its procedures require more information than an entity requesting a share provides in the Vigilant user interface, and there has been frequent turnover in the position responsible for approving sharing requests.

Current administrators at the three agencies have difficulty understanding when and how sharing occurred because the information the Vigilant user interface displays has changed over time. The status of a sharing relationship in the Vigilant system depends on whether the involved entities' accounts are *active* or *inactive*. Active entities have a current account with Vigilant while inactive entities do not. An agency may agree to share with an active entity that later becomes inactive. Images cannot be shared between active and inactive entities. However, unless an agency deliberately removes a sharing relationship with an inactive entity, that sharing relationship remains and would become operational if an inactive entity decided to renew its account with Vigilant and become active once more. Previously, Vigilant had structured its user interface so that inactive entities did not appear in the sharing report that shows a list of entities with whom an agency had agreed to share. Recently, Vigilant changed its interface to make inactive entities visible. Whether an entity is active is not apparent from the sharing report alone.

***A change in the vendor's user interface and not keeping records of authorized shares made it difficult for ALPR administrators to track current sharing relationships.***

This change in the user interface and the fact that agencies kept no records of the shares they have authorized made it difficult for ALPR administrators at the agencies to know the status of current sharing relationships. For example, in 2014 a prior ALPR administrator for Marin had agreed to share images with three U.S. Immigration and Customs Enforcement (ICE) agencies. In December 2018, Marin's current ALPR administrator used the Vigilant user interface to review the sharing report and noted that the report included no ICE agencies. However, when he reviewed the report again in August 2019—at our request—three ICE agencies appeared on the list. We discussed this discrepancy with Vigilant, which explained that the three ICE agencies were currently inactive. When Marin's ALPR administrator reviewed the sharing report in December 2018, inactive agencies did not appear on the report, but Vigilant subsequently changed its user interface so that inactive

agencies did appear. Although the ICE agencies could not access Marin's ALPR images because they were inactive, to effectively end the share, Marin needed to remove the authorization for sharing with the ICE agencies, which Marin has since done.

According to Marin's ALPR administrator, it is now the department's position that it will not share images with ICE, but if it had remained unaware that the sharing relationships existed and the ICE agencies had become active again, it would have been sharing its ALPR images with them without knowing it was doing so. Had Marin kept its own records of the sharing to which it had agreed, it would have been aware that it had agreed to share with ICE in the past, and it would have been able to remove those shares promptly. Sacramento had also authorized sharing to ICE agencies in the past. When the current ALPR administrator reviewed the list of entities with which it shared images with in response to our audit, he removed those shares as well. In contrast, Fresno had never authorized any sharing relationship with an ICE agency.

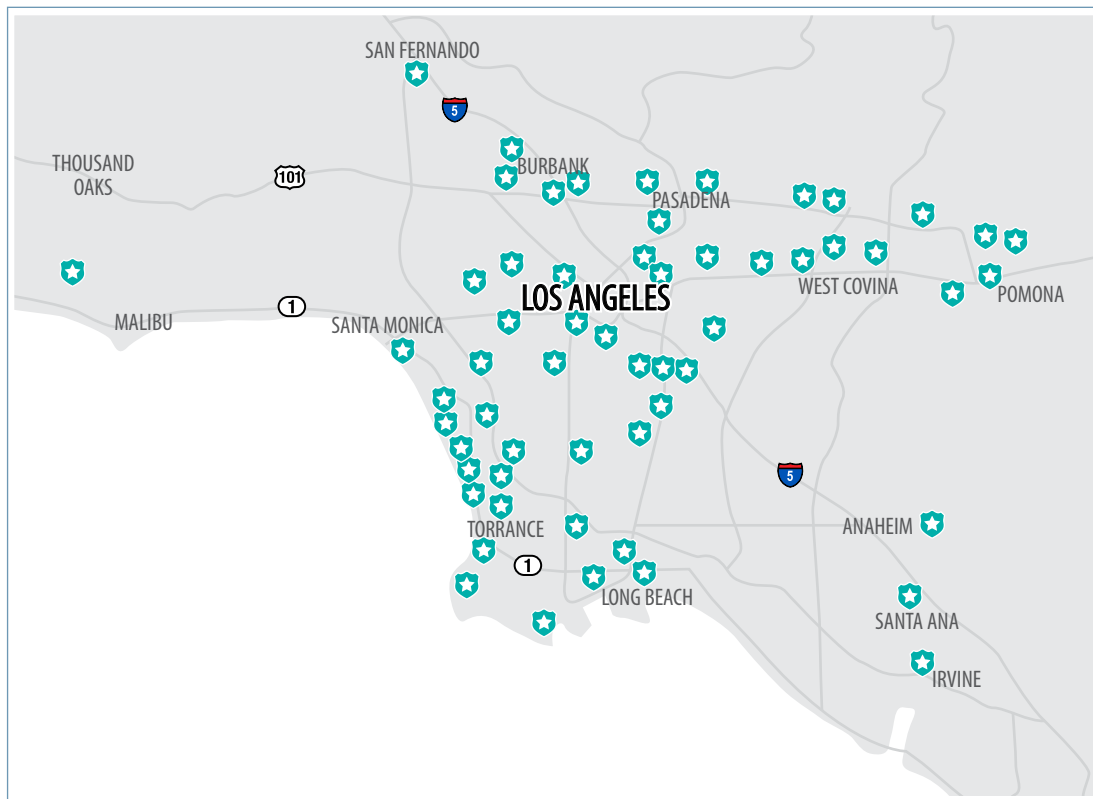
Although none of the agencies using Vigilant currently share with ICE agencies, all three had authorized shares with entities with border patrol duties. Despite not having implemented any agreements related to this sharing since Justice issued its guidance in October 2018, the three agencies were all sharing with the San Diego Sector Border Patrol of U.S. Customs and Border Protection at the start of our audit. During our audit, Sacramento removed the share to this agency. Marin and Sacramento had also authorized sharing with an agency listed as "California Border Patrol," and although Sacramento removed this share at the same time it removed the shares to ICE, Marin continues to share with this entity. Fresno continues to share with the Customs and Border Protection National Targeting Center. Although Sacramento had also authorized a share to this entity, it removed this share during our audit. All of these entities' duties could potentially intersect with immigration enforcement. Justice's guidelines for sharing data are particularly relevant in these cases, yet the agencies were either unaware of these guidelines or had not implemented them for their ALPR systems.

Of the four agencies we reviewed, only Fresno and Sacramento share hot lists they create, and they do so through a more controlled process than for sharing ALPR images. Vigilant's user interface enables hot-list sharing in addition to sharing ALPR images. In contrast to its wide sharing of ALPR images, Fresno shares the hot lists it occasionally uploads with only three law enforcement agencies in the nearby region. Sacramento has agreed to share six hot lists with eight law enforcement agencies in California. With each agency, Sacramento took the additional step of developing a memorandum of understanding providing guidelines for sharing the hot lists and the signature of the chief official at each agency.

*Justice's guidelines for sharing data are particularly relevant, yet Fresno, Marin, and Sacramento were either unaware of these guidelines or had not implemented them for their ALPR systems.*

In contrast with the other reviewed agencies, Los Angeles has limited its sharing of ALPR images to entities within a regional structure established for its ALPR program through a federal grant that helped fund its ALPR program. As Figure 5 shows, Los Angeles shares ALPR images with 58 other law enforcement agencies in the region. It does not have agreements to share its ALPR images with any federal agencies, including ICE. According to the lieutenant who administers the ALPR program, Los Angeles decided to share images only with entities using the same software so that it could maintain greater control over its ALPR images. It has a formal agreement with each agency, which provides a record of its sharing decisions.

**Figure 5**  
Los Angeles Shares Images With 58 Law Enforcement Agencies



Source: Analysis of data-sharing memorandums of agreement.

### ***The Agencies' Image Retention Decisions Are Unrelated to How They Use the Images***

The four agencies we reviewed retain ALPR images for varying periods of time. Our review determined that with the exception of CHP, state law does not mandate a specific retention period for ALPR images collected, accessed, or used by public agencies, nor does state law delineate the factors public agencies should use in determining those periods. Instead, state law requires that public agencies other than CHP that use or operate ALPR systems specify, in the agency's usage and privacy policy, the length of time ALPR data will be retained and the process that the agency will use to determine if and when to destroy retained ALPR data. Fresno's policy is to retain ALPR images for a minimum of one year, Sacramento's policy is to retain ALPR images for a minimum of two years, and Marin's policy is to retain images for two years. Although the agencies' policies describe their retention periods as minimums, in practice the agencies have configured their ALPR systems to delete images older than their specified retention periods. Fresno and Sacramento each download and retain images for longer than their prescribed retention policies if the images are relevant to investigations. Los Angeles does not have an ALPR policy, but the lieutenant who administers the ALPR program stated that it adheres to the city's Administrative Code, which requires data to be retained for a minimum of five years.

None of the agencies considered the images' utility over time when establishing their retention periods. Fresno based its ALPR image retention period on state law, which allows some cities to destroy certain video monitoring records after one year. Marin did not cite state law in its policy; its former ALPR administrator stated that when setting a two-year retention period, he considered other agencies' retention periods and the retention requirements for litigation related to investigations. Both Marin's and Fresno's ALPR administrators stated that they were not aware of any studies of how useful older images in their ALPR systems were to their personnel. In its ALPR policy, Sacramento cited a general state law that prohibits some cities from destroying records less than two years old. The lieutenant who oversees Sacramento's ALPR program acknowledged that the agency has not conducted any statistical analysis to determine how long it needs to retain ALPR images. However, he stated that, although he was not involved in drafting the original policy, two years made sense considering federal regulations, which permit retention of criminal intelligence information for no longer than five years. The lieutenant cited those federal regulations as a best practice for retaining sensitive data, connecting the ALPR images to a tenet of federal regulations that law enforcement agencies should keep criminal intelligence information as long as it is useful, even though ALPR data are not criminal intelligence.

***None of the agencies considered the images' utility over time when establishing their retention periods.***

To develop a retention policy that better protects individuals' privacy, an agency might begin by considering the time period during which ALPR data are most useful to law enforcement. To assess the usefulness of these images over time, we reviewed the four agencies' ALPR searches over a six-month period—between late January and September 2019, depending on when we visited the agencies—and found that personnel at three of the four agencies typically searched for ALPR images zero to six months old. When searching ALPR systems, investigators can enter search dates to target specific periods of interest. For example, on March 29, 2019, a Sacramento investigator searched for ALPR images from six days earlier—March 23—indicating that images less than one week old were relevant to that search. As Table 2 shows, we found that the searches agency personnel at the three agencies performed infrequently included older images. In fact, when investigators at Fresno, Marin, and Sacramento specified date ranges, most searches were of ALPR images that were less than six months old. In contrast, Los Angeles had a relatively even distribution of searches between those less than one year and those more than one year old. The Vigilant system defaults to showing the 50 most recent records when investigators do not specify a search date range. We analyzed 46,000 records for searches that did not specify a date range and found that investigators for Marin, Fresno, and Sacramento frequently did not seek further than the 50 default records, indicating that they generally were not interested in older ALPR images.

**Table 2**  
The Agencies Usually Search for ALPR Images That Are Six Months Old or Less

	RETENTION PERIOD	TOTAL SEARCHES OVER 6-MONTH PERIOD ANALYZED	PERCENTAGE OF SEARCHES FOR IMAGES OF A SPECIFIED AGE			
			0 TO 6 MONTHS	6+ MONTHS TO 1 YEAR	1+ TO 2 YEARS	MORE THAN 2 YEARS
<b>Fresno*</b>	1 year	850	92%	6%	1%	1%
<b>Los Angeles</b>	5 years	28,874	42	8	29	21
<b>Marin*</b>	2 years	26	88	8	0	4
<b>Sacramento*</b>	2 years	4,262	84	4	11	1

Source: Analysis of search records from the agencies' ALPR systems between late January and September 2019, depending on when we visited the agency.

\* The percentage of searches listed in this table beyond an agency's retention period are likely from their personnel searching data belonging to other agencies with longer retention periods.

Other states have established retention periods that are generally shorter than the lengths of time California's local law enforcement agencies are retaining ALPR images. The National Conference of State Legislatures identified at least 13 states that mandate maximum ALPR image retention periods. As the text box shows, these vary widely, from three minutes in New Hampshire to three years in Florida. Nevertheless, the majority of these states have retention periods that do not exceed six months.

In contrast, 230 California agencies responding to our survey reported that they use ALPR systems, and nearly 80 percent of these—180 agencies—stated that they retain their ALPR images for more than six months. About 20 of those agencies indicated that they retain ALPR images for more than five years. Figure A.2 in Appendix A summarizes these responses.

The length of time law enforcement agencies need to retain ALPR images will vary depending on how they use the images. Narrow use—for one purpose only, such as locating stolen cars—could dictate a short retention window. Personnel we interviewed at each of the four agencies stated that investigators rely primarily on recent images to investigate some types of crimes, such as auto theft. In contrast, using ALPR images to solve complex crimes could necessitate a longer retention window. For example, first-degree murder can be prosecuted at any time; therefore, a homicide investigator may be able to use ALPR images of any age to help solve a case. The four agencies we reviewed have access to information they can use to evaluate whether their ALPR retention periods are reasonable. Their systems record each time personnel search ALPR images, and these search records show the date of the search and the parameters used to narrow the search, such as location, date, and time. Agency administrators can analyze these activity logs to understand the images personnel are searching for and their relative ages.

Marin and Sacramento have allowed expired hot lists to remain in their ALPR systems for far longer than their specified retention periods. Unlike ALPR images, hot lists cannot be automatically deleted by the Vigilant system. Instead, the agencies define a period after which the hot list becomes inactive—meaning the ALPR system no longer generates alerts from the list—but the list remains stored in Vigilant’s servers until the agency deletes it. We found that Marin and Sacramento are retaining hot lists longer than necessary because their administrators were unaware of the need to manually delete them. They assumed that their Vigilant system would automatically delete inactive hot lists according to the designated purge schedule, as it does ALPR images. For example, Marin retained an inactive hot list of sex offenders for five years—three years longer than its two-year retention period for ALPR images. Sacramento has retained multiple hot lists for as long as six years—four years longer than its retention period for ALPR images. The types of lists ranged from a hot list of Sacramento County sex offenders to a warrants hot list. When we brought the inactive hot lists to the agencies’ attention,

#### ALPR Image Retention Periods for 13 States

New Hampshire	<b>3 minutes</b>
Maine	21 days
Minnesota	60 days
Montana	90 days
North Carolina	90 days
Tennessee	90 days
Arkansas	150 days
Nebraska	180 days
<b>----- LONGER THAN SIX MONTHS -----</b>	
Utah	270 days
Colorado	365 days
Vermont	540 days
Georgia	900 days
Florida	<b>3 years</b>

Source: National Conference of State Legislatures, *Automated License Plate Readers: State Statutes*, March 15, 2019, and review of the listed states’ ALPR laws and guidelines.

Note: These states allow retention for longer periods for specific reasons, such as data used in investigations.

the administrators at Marin and Sacramento acknowledged that the age of the hot lists exceeded the agency's retention period, and they were willing to delete the hot lists.

Law enforcement agencies should consider both the usefulness of the ALPR images and individuals' privacy when deciding how long to retain the images. Cost, however, is not a factor. According to the lieutenant who oversees Los Angeles' ALPR program, the images are useful to investigators and the cost of storing ALPR images is not a significant factor in determining how long to store them. Nevertheless, two studies by a consultant to the National Institute of Justice and the chiefs' association concluded that law enforcement agencies must consider the trade-offs between privacy concerns and the utility of retaining the ALPR images they capture and store.

### **The Law Enforcement Agencies Have Failed to Monitor Use of Their ALPR Systems and Have Few Safeguards for Creating ALPR User Accounts**

Instead of ensuring that only authorized users access their ALPR data for appropriate purposes, the agencies we reviewed have made abuse possible by neglecting to institute sufficient monitoring. ALPR systems should be accessible only to employees who need the data and who have been trained in using the system. However, the agencies often neglected to limit ALPR system access, to provide appropriate training to individuals with access, or to monitor accounts. Similarly, to ensure that individuals with access do not misuse the system, the agencies should audit the license plate searches users perform. Instead, the agencies conduct little to no auditing and thus have no assurance that misuse has not occurred.

#### **Best Practice Safeguards for Establishing and Managing User Accounts**

##### **Account Setup**

- Supervisor approval is a prerequisite for account access.
- ALPR training is a prerequisite for account access.

##### **Account Maintenance**

- Accounts defined as *inactive* are suspended.
- ALPR training is required for users linked to inactive accounts to regain active status.
- Accounts are deleted when employees separate from the agency.

Source: CJIS policy and the *State Administrative Manual*.

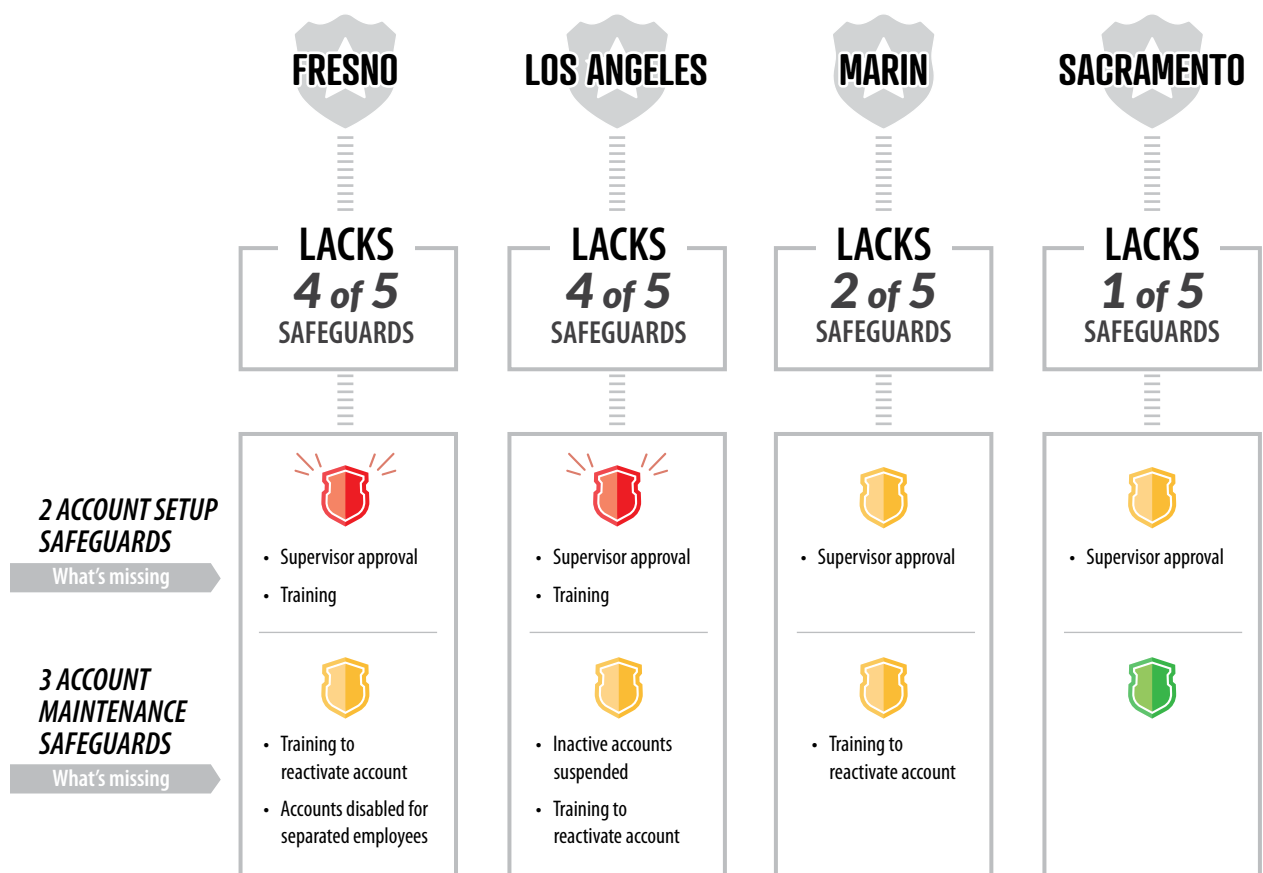
#### ***The Agencies Need Stronger User-Access Safeguards***

The four agencies we reviewed all failed to follow one or more best practices related to user access. State law requires agencies to maintain reasonable security procedures and practices to protect ALPR data from unauthorized access, and the text box lists five best practices for user access, from initiating an account to disabling it when an employee separates from the agency. Figure 6 shows the four agencies' status in implementing these best practices. Each ALPR administrator stressed the concept of "need to know, right to know" as a key for data security; however, no agency followed all of the best practices that would help establish the need to know and right to know. For example, no agency had a requirement

that supervisors approve staff requests for creating ALPR user accounts. Such a step would provide assurance that the staff member receiving the account had both a need and a right to access the information in the ALPR system. Los Angeles is particularly lax in this area because the protocol of its IT division is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system nevertheless have access to the system. In contrast, Sacramento follows all but one of the best practices listed in the text box. In doing so, it requires staff to prove their initial and continued need for ALPR data, among other access requirements.

**Figure 6**

**The Agencies Lack Many Best Practice Safeguards for Establishing and Managing User Accounts**



Source: Agencies' policies, applicable procedures and protocols, and interviews with the agencies' management.

Agencies could reduce instances of unnecessary access by ensuring that only those staff whose current work assignments require access to ALPR data have that access. The ALPR administrators at Marin and Los Angeles believe that supervisory approval is unnecessary

*Limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.*

because ALPR users are already privy to data they consider more confidential than ALPR data, such as criminal justice information. However, these views do not consider that ALPR systems capture images indiscriminately, irrespective of the criminal history of the individual who is driving the vehicle, and the images allow law enforcement to track individuals. Given that agencies retain these images for several months or years, a user could combine them with personal information from separate data sources to produce a great number of details about someone's life, such as his or her political or religious affiliation. Without proper safeguards, staff could conduct this form of surveillance on any driver. In fact, the chiefs' association acknowledged this possibility and warned that increasing ALPR use and data sharing would enhance the potential for surveillance. Thus, as the chiefs' association concluded, limiting ALPR access to employees with the needs and the rights to access these data is a good step toward protecting the individuals whose privacy would be violated if the data were misused.

Ensuring that ALPR users are properly trained is another weakness among the agencies we reviewed. Three of the agencies do not ensure that all of their ALPR users are properly trained. The chiefs' association called the training of authorized ALPR users "a critical accountability measure." However, as Figure 6 shows, neither Fresno nor Los Angeles requires all ALPR users to complete ALPR training before initially obtaining system access. Although Los Angeles offers ALPR training, the detective who conducts this training confirmed that it is not required before users can access the ALPR system. Fresno's policy encourages such training; however, its ALPR administrator confirmed that the agency does not provide training to all of its users. Further, Marin's ALPR administrator stated that although Marin provides training when staff first receive access to the ALPR system, it does not require staff to renew their training in order to reactivate their accounts following long periods of not using the system. Without sufficient training, there is little assurance that ALPR users know and understand agency ALPR policies, including recent changes, or are aware of the limits on how they may use ALPR data.

Although the Fresno ALPR administrator agrees that the agency's safeguards surrounding user access are currently inadequate and plans to improve them, the ALPR administrators at Los Angeles, Marin, and Sacramento believe their current practices are acceptable. The administrators at Marin and Los Angeles are reluctant to alter their agencies' existing practices because they believe ALPR data are not as sensitive as other law enforcement data. We disagree with these views because, as we mention previously, ALPR data are sensitive and state laws require reasonable security procedures and practices to protect them. A basic protection for data that must be treated as sensitive is to limit who can access them.

In addition, as we mention earlier, the ALPR images law enforcement agencies collect largely involve vehicles that are not associated with crimes, and if the images were analyzed, the data could reveal behavior patterns and preferences that law enforcement could use to conduct surveillance on individuals. For example, according to a 2012 newspaper article, the New York Police Department collected license plate numbers of vehicles parked near a mosque. The department was purportedly trying to identify terrorist activities. Although the department justified this data collection as part of its strategy to identify potential criminal activities, it targeted mosques and collected license plate numbers at times without any leads or proof of terrorist connections. Given the sensitivity of the information collected in this example, access safeguards would ensure that only those staff who have a need and right to access an ALPR system would possess that privilege.

Law enforcement agencies could further improve safeguards by disabling employees' accounts once they separate or after long periods of nonuse. We reviewed Marin's and Sacramento's processes for disabling accounts of separated employees. Both agencies follow a similar approach, relying on one part of the organization providing information to another. Sacramento produces a personnel transfer and separation list every two weeks, and the IT security group uses it to identify accounts to close. Although the IT security group generally disabled accounts promptly after receiving the list, we found that the contents of the list were not always current. For example, in one instance, a separated employee did not appear on the list until 46 days after his separation date in June 2019. According to a human resources specialist, employees submit their resignation paperwork late at times, which causes human resources to not process this paperwork until after an employee has left the department. Marin's ALPR administrator said that he removes ALPR accounts once he receives a department-wide email notifying him of an employee's resignation or termination. He also stated that he checks ALPR accounts every few months to verify that active accounts match active employees. However, for one employee, the administrator did not disable his ALPR access until two months after he resigned in October 2019. In fact, the administrator did not disable this employee's access until our office pointed out that the account was still active. The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.

With regard to Los Angeles and Fresno, Los Angeles' network manager described an automated process for deleting accounts linked to overall network access, which reasonably aligned with best practices. Conversely, Fresno's ALPR administrator said that

*The fact that Marin and Sacramento did not disable some accounts as necessary is problematic because the former employees could log into their accounts and access ALPR data from the web-based version of the ALPR systems on any Internet-capable device, not just office devices.*

he periodically reviews the names of employees with user accounts but started doing so only in September 2019 when he learned of our audit. We did not test deleted accounts at either agency. Deleting accounts prevents separated employees from continuing to access ALPR data and is thus critical to protecting ALPR data and individuals' privacy.

***The Agencies Have Failed to Audit ALPR Users' Searches to Ensure That Individuals' Privacy Is Protected***

State law requires law enforcement agencies that operate, access, or use ALPR systems to protect their ALPR data—including ALPR images—from unauthorized access, destruction, use, modification, or disclosure. The law specifically requires them to describe and implement a policy detailing how they will monitor their ALPR systems. According to state law, agencies that access or use ALPR systems must also conduct periodic system audits. In its reports on managing ALPR systems, the chiefs' association stated that conducting audits aids in discouraging unnecessary or inappropriate use of the data; in addition, when agency policies include a strong auditing requirement, this reassures the public that their privacy interests are recognized and respected.

***Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, they should also conduct audits as required by state law.***

A primary form of auditing to prevent misuse is reviewing the searches users conduct in the ALPR systems. Users conduct searches for specific license plates. Even though law enforcement agencies that use or access ALPR systems can monitor searches simply by reviewing search records for red flags, such as an unknown user account, they should also conduct audits as required by state law. An audit entails a more rigorous approach, including evaluating risk and randomly selecting test items for review. Developing an audit of license plate searches, for example, would involve determining how many searches to review, how to select test items, and how frequently to conduct the audit. Law enforcement agencies have often found evidence of misuse of their databases, showing the need for auditing. For example, a news article reported that CHP investigated 11 cases of database misuse in 2018, including three involving officers improperly looking up information on license plates through CLETS without a need to know the information. The large datasets of ALPR images, dating back at least one year, that the four reviewed agencies maintain can be analyzed to reveal the daily patterns of vehicles that can be linked to individuals and their activities—most of whom have not engaged in criminal activity. A member of law enforcement could misuse ALPR images to stalk an individual or observe vehicles at particular locations and events, such as doctors' offices or clinics and political rallies. Despite these risks, the agencies we reviewed conduct little to no auditing of users' searches.

We asked key officials at the three agencies using the Vigilant system why they had not audited the searches users performed and found that either they were unaware of the auditing requirement in state law or the auditing they did conduct did not include user searches. Fresno's policy states that it should conduct audits on a regular basis, but the ALPR administrator told us he believed audits are the responsibility of the Audits and Inspections Division within the department. However, the sergeant responsible for audits and inspections—who took charge in January 2018—responded that he was not aware of the requirement until our audit. Similarly, the Marin ALPR administrator was unaware of the state law requiring audits of ALPR systems until our audit and thus had not been conducting them. At Sacramento, the policy states that the ALPR administrator will conduct periodic audits of user searches. Even though Sacramento administrators had been monitoring some system functions, they had not audited searches of the older ALPR images. The officer administering the ALPR program until April 2019 said that she did not conduct these audits because her predecessor had not informed her that it was necessary. The ALPR program transferred to a new division in April, and according to the current ALPR administrator, limited staff resources have prevented him from instituting these audits.

Although the agencies have not been conducting audits, we considered the possibility that an agency employee or member of the public may have reported instances of ALPR misuse. We searched each agency's records of internal affairs investigations from January 1, 2016, to the present for cases involving ALPR misuse and did not find any such cases. However, we do not consider this proof that no instances of ALPR misuse occurred. Given that the agencies were not regularly auditing their systems, ALPR misuse may have occurred and gone unnoticed and unreported.

To engage in meaningful auditing of their system users, all four agencies need to address the quality of the information users enter into the system as part of their searches. Before allowing users to conduct searches, Fresno, Los Angeles, and Marin require users to enter case numbers and reasons for the search; however, this is not happening consistently. We reviewed six months of user queries at the three agencies and found that users entered a wide variety of information in the case number field. For example, users at Los Angeles simply entered "investigation" into this field as well as descriptions of vehicles and actual case numbers. In contrast, Sacramento does not require users to enter either case numbers or reasons. Our review showed that in 66 percent of searches, Sacramento's users left both fields blank. When users fail to enter any information or fail to include appropriate detail, identifying misuse through audits becomes nearly impossible.

***All four agencies must address the quality of information they will need to audit user searches. In Sacramento, for 66 percent of searches, users left case number and search reason fields blank.***

***Fresno, Marin, and Sacramento do not have adequate policies or processes in place for conducting meaningful audits.***

Los Angeles faces additional hurdles in performing meaningful auditing because its ALPR administrators do not have immediate access to data on user searches. Instead, according to the chief data officer, administrators need to request that a software engineer from Los Angeles' ALPR software contractor build and run a query in the system to obtain these data. In 2015 Los Angeles recognized a need to fix this software limitation to enable administrators to audit user searches. The chief data officer for Los Angeles stated that, although an initial upgrade provided an audit dashboard tool for administrators, subsequent software upgrades made this tool unusable, and the company that provides the software is developing a new one. He said that it is Los Angeles' goal to have a new audit dashboard tool by the end of the first quarter of 2020, at which point he will work with the appropriate division within the department to develop an audit plan. Although we agree that an audit tool will facilitate audits, we believe it was entirely possible for Los Angeles to obtain the data on user searches, and thus it could have implemented a process for periodic system audits as state law requires, despite the difficulties.

The other three agencies also do not have an adequate policy or process in place for conducting meaningful audits. For example, Fresno's ALPR policy states that it should conduct periodic audits, but its policy does not specify how frequently it will audit its ALPR system, who will perform those audits, who will review and approve the audit results, and how long it will retain the audit documents. Specifics such as these provide a clear road map for planning, conducting, documenting, and resolving audits. When followed, the agencies will have records demonstrating their necessary oversight. Marin's latest policy—dated July 2019—also fails to cover these necessary details. Fresno and Marin began reviewing user queries subsequent to the beginning of our audit, but in the absence of an adequate policy or formal plan, their methodologies are lacking. For example, although Fresno began conducting audits that included a random sample of user searches, staff have not developed a formal plan and provided us only with handwritten notes on their methodology. Marin's ALPR administrator has not instituted audits and is simply monitoring license plate searches by looking for instances in which the user did not enter a reason for the search or entered a reason that does not make sense, such as an investigation that does not exist. In addition, at both Fresno and Marin, the individual conducting the audits or monitoring is also a system user, creating a conflict when acting as a system monitor or auditor. Without sound methodologies, the agencies cannot be confident that they have sufficient protocols in place to detect misuse.

## **Other Areas We Reviewed**

To address all the audit objectives approved by the Joint Legislative Audit Committee (Audit Committee), we reviewed two additional subject areas: whether the agencies offered opportunities for the public to comment on their ALPR programs and whether the Sacramento County Department of Human Assistance (Human Assistance) continues to operate an ALPR program.

### ***Three Agencies Provided Information to the Public on Their ALPR Programs***

State law requires that public agencies implementing ALPR programs after January 1, 2016, offer an opportunity for the public to comment about those programs. These opportunities increase public awareness that law enforcement agencies are using electronic means to collect information about vehicles in the community and offer a way for the public to provide feedback about the programs. The four agencies we reviewed began using ALPR before 2016 and consequently were not required to offer an opportunity for public comments. Nonetheless, three of the agencies took some steps to communicate with the public about their ALPR programs. Los Angeles and Sacramento published documents describing their ALPR programs, and at a Fresno City Council meeting, the public had an opportunity to comment on the selected ALPR vendor before the council voted on a new contract. The minutes from that meeting reflect that the public made no comments. This transparency helps foster public trust in law enforcement and government as a whole.

### ***Human Assistance No Longer Operates an ALPR Program***

Our audit scope included reviewing the ALPR program of Human Assistance, which provides Sacramento County residents with employment assistance and supportive services. Human Assistance contracted with Vigilant for three years to access ALPR images. Human Assistance did not operate its own cameras, and it used the ALPR images to investigate welfare fraud. According to the administrator of its ALPR program, Human Assistance ended its program in 2018 after determining that investigative staff rarely searched the images, so the program could not justify the cost. On November 1, 2018, Human Assistance deleted its ALPR user accounts, leaving the administrator's account active for internal review. On May 31, 2019, Human Assistance's ALPR agreement with Vigilant expired, and the administrator no longer has access to the account. Therefore, we did not perform any additional audit work pertaining to Human Assistance.

## Recommendations

### *Legislature*

- To better protect individual's privacy and to help ensure that local law enforcement agencies structure their ALPR programs in a manner that supports accountability for proper database use, the Legislature should amend state law to do the following:
  - Require Justice to draft and make available on its website a policy template that local law enforcement agencies can use as a model for their ALPR policies.
  - Require Justice to develop and issue guidance to help local law enforcement agencies identify and evaluate the types of data they are currently storing in their ALPR systems. The guidance should include the necessary security requirements agencies should follow to protect the data in their ALPR systems.
  - Establish a maximum data retention period for ALPR images. The Legislature should also establish a maximum data retention period for data or lists, such as hot lists, that are used to link persons of interest with license plate images.
  - Require periodic evaluation of a retention period for ALPR images to ensure that the period is as short as practicable.
  - Specify how frequently ALPR system use must be audited and that the audits must include assessing user searches.
  - Specify that those with access to ALPR systems must receive data privacy and data security training. The Legislature should require law enforcement agencies to include training on the appropriateness of including certain data in an ALPR system, such as data from CLETS.

### *Law Enforcement Agencies*

- To ensure that their ALPR policies contain all of the required elements as specified in state law, by August 2020, Fresno, Los Angeles, Marin, and Sacramento should review their policies and draft or revise them as necessary. Also by August 2020 these agencies should post their revised policies on their websites in accordance with state law.

- To protect ALPR data to the appropriate standard, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By August 2020, identify the types of data in their ALPR systems and, as they review or draft their ALPR policies, ensure that they clarify the types of information their officers may upload into their ALPR systems, such as, but not limited to, information obtained through CLETS.
  - By August 2020, perform an assessment of their ALPR systems' data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.
- To ensure that the agreements with their cloud vendor offers the strongest possible data protections, by August 2020, Fresno, Marin, and Sacramento should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy.
- To ensure that ALPR images are being shared appropriately, the specific agencies noted should do the following:
  - By April 2020, Fresno, Marin, and Sacramento should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.
  - As Los Angeles develops its ALPR policy, it should be certain to list the entities with which it will share ALPR images and the process for handling image-sharing requests.
  - By August 2020, Marin and Sacramento should each develop a process for handling ALPR image-sharing requests that includes maintaining records separate from the Vigilant system of when and with whom they share images. The process should verify a requesting agency's law enforcement purpose for obtaining the images and consider the requesting agency's need for the images. The process should be documented in the agency's ALPR policy and/or procedures.
  - By August 2020, Fresno should revise its written procedures for ALPR image-sharing, as necessary, to ensure that it follows those procedures.

- To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By August 2020, review the age of the ALPR images their personnel are searching for and ensure that their retention periods for ALPR images are based on department needs. Each agency should reflect in its ALPR policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.
  - Include in their ALPR policies a retention period for data or lists, such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.
- To ensure that ALPR system access is limited to agency staff who have a need and a right to use ALPR data, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By April 2020, review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.
  - Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.
  - By August 2020, develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that supervisors must approve accounts for users, providing training to users before granting accounts, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously inactive accounts. Each agency should also ensure that it has procedures in place to deactivate an account immediately for an account holder who separates from the agency or who no longer needs a user account.

- To enable auditing of user access and user queries of ALPR images, Fresno, Los Angeles, Marin, and Sacramento should do the following:
  - By April 2020, assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.
  - Ensure that their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. Each agency should have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.
  - By June 2021, implement their audit plans and complete their first audits.

We conducted this performance audit under the authority vested in the California State Auditor by Government Code 8543 et seq. and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Respectfully submitted,



ELAINE M. HOWLE, CPA  
California State Auditor

February 13, 2020

Blank page inserted for reproduction purposes only.

## Appendix A

### Summary of ALPR Survey Responses

The Audit Committee requested that we determine ALPR use among law enforcement agencies statewide. Specifically, the Audit Committee asked us to determine whether agencies use ALPR information, what vendors they use, and whether law enforcement agencies have policies and procedures to govern their use and sharing of ALPR information. We surveyed 391 county sheriffs and municipal police departments statewide. We relied upon information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI to obtain assurance that our list of statewide local law enforcement was reasonably comprehensive.

We received 381 responses (97 percent) to the 391 surveys we sent. Ten agencies we surveyed did not respond. The text box lists those agencies. A breakdown of the law enforcement agencies' responses to our statewide survey can be found at <http://auditor.ca.gov/reports/2019-118/supplemental.html>. The discussion here summarizes the survey results.

#### Agencies That Did Not Respond to Our Survey

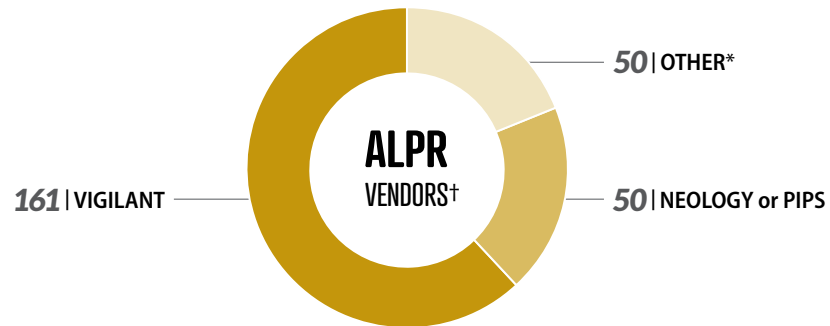
- Anderson Police Department
- Barstow Police Department
- Del Norte County Sheriff's Office
- Lakeport Police Department
- Lodi Police Department
- Mendocino County Sheriff's Office
- Mount Shasta Police Department
- Oceanside Police Department
- San Francisco Sheriff's Department
- Siskiyou County Sheriff's Department

Source: Analysis of survey responses.

### Summary of Results From Agencies That Reported Using ALPR Systems

In responding to our survey, law enforcement agencies indicated whether they use ALPR systems and, if so, what vendors' systems they use to collect and access ALPR information. Of the agencies that responded, 60 percent, or 230 agencies, reported that they currently operate or access information from ALPR systems. Of those agencies, 96 percent said they have an ALPR usage and privacy policy. Vigilant is the most common vendor for the agencies that reported using ALPR systems. Figure A.1 summarizes which vendors the 230 law enforcement agencies reported that they use. Finally, 9 percent, or 36 of the agencies we surveyed, stated that they are implementing or planning to implement ALPR systems.

**Figure A.1**  
Vigilant Is the ALPR Vendor the Majority of Law Enforcement Agencies Use



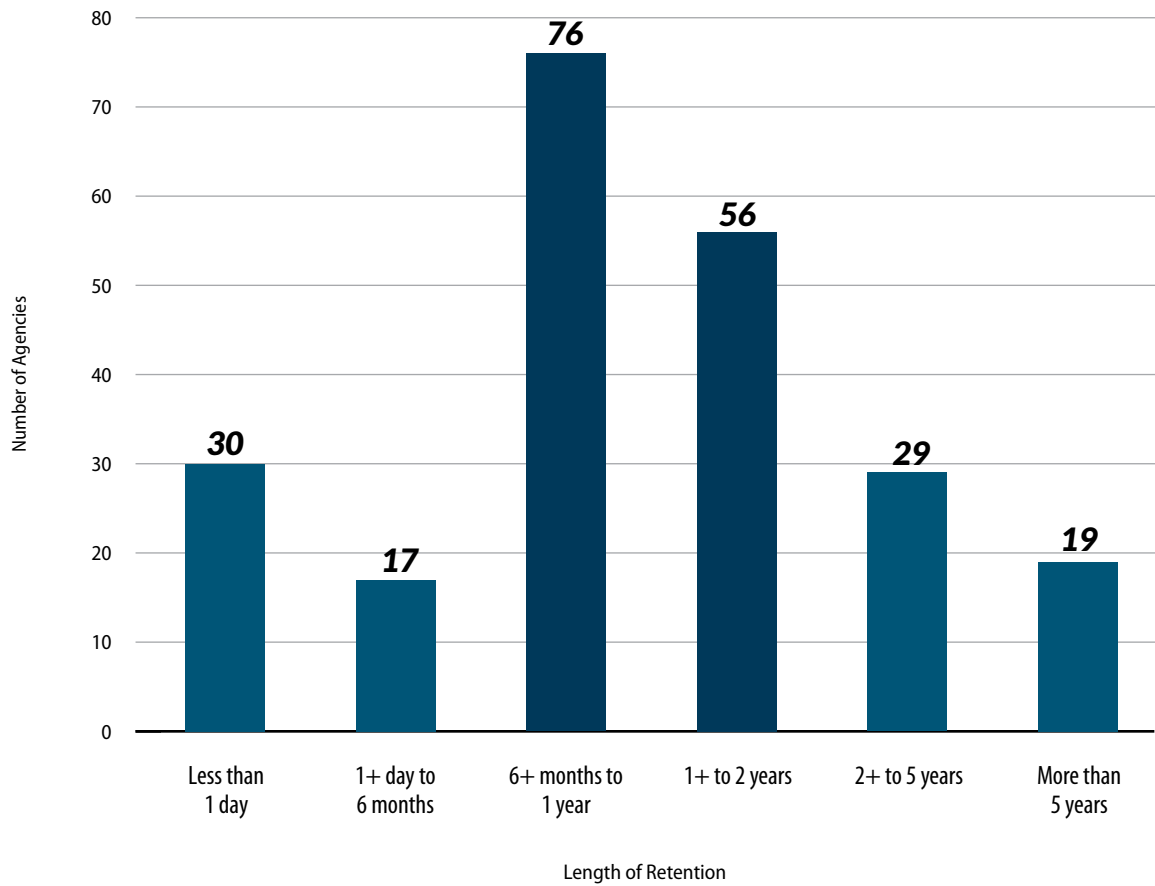
Source: Analysis of survey responses.

\* The *Other* category includes vendors such as Genetec, ELSAG, and All Traffic Solutions.

† The total number of ALPR vendors used is greater than the 230 agencies that said they use ALPR systems because some agencies use more than one vendor.

Law enforcement agencies that reported using ALPR systems also answered questions related to their retention and sharing of ALPR information. We asked how long the agencies retain ALPR information not related to ongoing investigations or litigation. As Figure A.2 shows, the retention periods varied, but the majority of law enforcement agencies reported retention periods between six months and two years. Additionally, we asked agencies that operate ALPR systems if they share or sell the information they collect with other law enforcement or public agencies. Seventy-three percent, or 168 agencies that use ALPR systems, reported that they share ALPR images with other law enforcement agencies; only three of those agencies also reported that they share ALPR images with other public agencies that are not law enforcement. None of the agencies we surveyed reported selling images to other law enforcement or public agencies.

**Figure A.2**  
**A Majority of Agencies Generally Retain ALPR Information for Between Six Months and Two Years**



Source: Analysis of survey responses.

Note: Three responding agencies that use ALPR systems did not indicate a retention period for their information: Bakersfield Police Department, Fountain Valley Police Department, and Pasadena Police Department.

Blank page inserted for reproduction purposes only.

## Appendix B

### Scope and Methodology

The Audit Committee directed the California State Auditor to conduct an audit of the extent to which local law enforcement agencies are complying with existing law regarding the use of ALPR systems. The analysis the Audit Committee approved contained five objectives. We list the objectives and the methods we used to address them in Table B.

**Table B**  
**Audit Objectives and the Methods Used to Address Them**

AUDIT OBJECTIVE	METHOD
1 Review and evaluate the laws, rules, and regulations significant to the audit objectives.	Reviewed relevant state laws, regulations, and other background materials applicable to the use and operation of ALPR systems by local law enforcement.
2 To the extent possible, determine the following for law enforcement agencies statewide: <ul style="list-style-type: none"> <li>a. Whether they use ALPR information and, if so, what vendors they use to access this information.</li> <li>b. Whether they have policies and procedures in place governing the use and sharing of ALPR information.</li> </ul>	<ul style="list-style-type: none"> <li>• Surveyed 391 county sheriff and municipal police departments statewide.</li> <li>• Obtained and verified a list of statewide local law enforcement agencies, using information from the California State Sheriffs' Association, the California Police Chiefs Association, and the FBI.</li> <li>• Questioned agencies regarding their use of ALPR systems, including whether they use or are planning to use an ALPR system; if they share or sell the ALPR information; if their ALPR storage is CJIS-compliant; which system they use to store, share, or access ALPR information; if they have a usage and privacy policy and post the policy on their website; how long they retain ALPR information; how many department personnel have access to the ALPR data; and how many total personnel their department has. Full questions and a breakdown of the responses are on our website at <a href="http://auditor.ca.gov/reports/2019-118/surveys.html">http://auditor.ca.gov/reports/2019-118/surveys.html</a>.</li> <li>• Created an interactive graphic to display responses by county, assembly district, and senate district at <a href="http://auditor.ca.gov/reports/2019-118/supplemental.html">http://auditor.ca.gov/reports/2019-118/supplemental.html</a>.</li> <li>• The survey responses were self-reported, and we did not verify their accuracy.</li> </ul>

*continued on next page...*

AUDIT OBJECTIVE	METHOD
<b>3</b> Examine the use of ALPRs by the Sacramento County Sheriff's Office and Department of Human Assistance, the Los Angeles Police Department, the Fresno Police Department, and the Marin County Sheriff's Office by performing the following:	
a. Determine whether they have policies and procedures in place regarding ALPR systems and whether those policies contain the elements state law requires.	<ul style="list-style-type: none"> <li>• Interviewed the agencies' ALPR administrators.</li> <li>• Obtained and reviewed ALPR policies and procedures and determined whether each agency met state law requirements in this area.</li> </ul>
b. Determine whether they have followed state law regarding all required public notifications related to ALPR systems and information, including required public hearings.	<ul style="list-style-type: none"> <li>• Interviewed the agencies' public information officers.</li> <li>• Obtained evidence of public notifications and public hearings and determined whether each agency met state requirements in this area.</li> </ul>
c. Determine whether they maintain records of access to ALPR information from both within and outside the agency that includes all required documentation and whether they have ensured that ALPR information has only been used for authorized purposes.	<ul style="list-style-type: none"> <li>• Interviewed the agencies' ALPR administrators.</li> <li>• Reviewed access records from the agencies' ALPR systems.</li> <li>• Determined whether the agencies conducted any audits or monitoring by interviewing ALPR administrators, staff of internal audit divisions, and executive staff of any oversight entities. We also reviewed relevant policies and procedures.</li> <li>• Reviewed the agencies' internal affairs files for any cases involving ALPR misuse.</li> <li>• Reviewed Justice's and the FBI's audits of the agencies' IT security and the safeguards those audits identified.</li> </ul>
d. Determine whether they have sold, shared, or transferred ALPR information only to other public agencies, except as otherwise permitted by law, and whether they have properly documented these activities.	<ul style="list-style-type: none"> <li>• Interviewed the agencies' ALPR administrators.</li> <li>• Reviewed reports and records about data sharing from the agencies' ALPR systems.</li> <li>• Reviewed existing memorandums of agreement and understanding for data sharing.</li> <li>• Interviewed executive staff at Vigilant regarding ALPR system functionality and their procedures for verifying the law enforcement purpose of client agencies.</li> </ul>
e. Determine the nature of any contracts with third-party vendors related to ALPR information.	<ul style="list-style-type: none"> <li>• Interviewed Justice staff responsible for protecting criminal justice information.</li> <li>• Evaluated the agencies' contracts with third-party vendors and determined whether the contracts contained adequate protections for information in the agencies' ALPR systems.</li> </ul>
<b>4</b> Evaluate whether current state law governing ALPR programs can be enhanced to further protect the privacy and civil liberties of California residents.	<ul style="list-style-type: none"> <li>• Interviewed agencies' investigators and ALPR program administrators.</li> <li>• Reviewed the information in the agencies' ALPR systems and identified the necessary protections for that information.</li> <li>• Obtained the agencies' justifications for their ALPR data retention periods.</li> <li>• Analyzed six months of the agencies' ALPR search records— between late January and September 2019, depending on when we visited the agencies—to determine how often the agencies' personnel searched for older data in their ALPR systems.</li> <li>• Reviewed other states' ALPR data retention laws based on a report from the National Conference of State Legislatures and identified best practices for data retention.</li> <li>• Analyzed laws pertaining to privacy, personal information, and criminal justice information and determined whether changes to current ALPR law would further protect the privacy and civil liberties of California residents.</li> </ul>
<b>5</b> Review and assess any other issues that are significant to the audit.	Reviewed informational material produced by law enforcement agencies, nonprofit organizations, and other entities to identify concerns surrounding privacy and ALPR systems.

Source: Analysis of state law, policies, information, and documentation identified in the table column titled Method.

### Assessment of Data Reliability

The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, and recommendations. In performing this audit, we relied on electronic data files we obtained from Fresno, Los Angeles, Marin, and Sacramento. These files included reports from the agencies' ALPR systems. Because the agencies relied on remote third-party systems to produce the reports, our analysis of these reports was limited to verifying that we had received the information we requested. We did so by reviewing source materials such as user manuals, interviewing vendor staff, and confirming with the agency staff that the number of records in the files we received were correct. We also used electronic lists from the California Police Chiefs Association and the California State Sheriffs' Association to compile a list of statewide police and sheriff departments for our survey. We verified the nature of the data with the associations' staffs, and we also verified record counts by comparing the provided lists with FBI crime-reporting data. We found the data to be sufficiently reliable for our purposes.

Blank page inserted for reproduction purposes only.

February 2020

**XAVIER BECERRA**  
*Attorney General*

*State of California*  
**DEPARTMENT OF JUSTICE**



1300 I STREET  
SACRAMENTO, CA 95815-4524  
Public: (916) 210-5000  
Fax (916) 227-3079  
Email: [Joe.Dominic@doj.ca.gov](mailto:Joe.Dominic@doj.ca.gov)

January 28, 2020

Elaine Howle  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

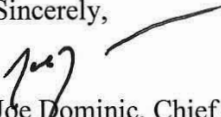
Re: Draft Audit Report - California State Auditor Report 2019-118; Automated License Plate Readers (ALPR)

Dear Ms. Howle:

The Department of Justice (DOJ) appreciates the opportunity to review the above-mentioned draft audit report. DOJ currently has no program in place to provide policy template and guidance to law enforcement agencies for their ALPR programs. Express authority from the Legislature and funding are needed to implement the recommendations.

If you have any questions or concerns regarding this matter, you may contact me at the telephone number listed above.

Sincerely,

  
Joe Dominic, Chief  
California Justice Information Services Division

For **XAVIER BECERRA**  
Attorney General

cc: Sean McCluskie, Chief Deputy to the Attorney General  
Edward Medrano, Chief, Division of Law Enforcement  
Chris Prasad, CPA, Director, Office of Program Oversight and Accountability

Blank page inserted for reproduction purposes only.



Mariposa Mall  
P.O. Box 1271  
Fresno, CA 93715-1271

January 27, 2020

**ANDREW J. HALL**

Chief of Police



Elaine Howle  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

Dear Ms. Howle:

On behalf of the men and women of the Fresno Police Department, allow me the opportunity to thank you and your team for the time and effort in completing the Automated License Plate Reader (ALPR) audit at the request of the Joint Legislative Audit Committee. The Fresno Police Department always strives to ensure we maintain excellence and utilize best practices in all facets of service to the community especially concerning personal privacy. Building trust in the community is paramount to our agency as we continue our on-going efforts to be a model community policing agency. We will utilize this audit to ensure those goals are achieved.

The following are the Fresno Police Department's response to the audit recommendations included in the report.

1. *"To ensure that agency ALPR policies contain all of the required elements as specified in state law, by August 2020 Fresno should review their ALPR policies and draft or revise them as necessary. Also by August 2020 post their revised policies on their websites in accordance with state law:*

The Fresno Police Department has already begun reviewing and updating our ALPR policy. In fact, it is nearly complete and will be completed well in advance of the August 2020 recommended timeline.

2. *"To protect ALPR data to the appropriate standard, Fresno should do the following:"*
  - a. *By August 2020 identify the types of data in their ALPR systems, and as they review or draft their policies, ensure that they clarify the types of information their officers may upload into their ALPR systems such as, but not limited to information obtained through CLETS."*

As the audit showed, the Fresno Police Department has not entered personal data into the ALPR system; however we will continue to review data and incorporate into policy the parameters for types of data which can be entered.

- b. *By April 2020 perform an assessment of their ALPR systems data security features, and make adjustments to their system configurations where necessary to comply with CJIS policy best practices based on that assessment.*

*Safety, Service, Trust*

Fresno Police Department  
ALPR Audit Response  
January 23, 2020  
Page 2

The Fresno Police Department IT Manager will assess the ALPR system and ensure it is in compliance with CJIS Security Policy best practices.

3. *"To ensure that the agreement with their cloud vendor offers the strongest possible data protections, by August 2020 Fresno should enter into new contracts with Vigilant that contain the contract provisions recommended in CJIS policy."*

The Fresno Police Department IT Manager will review the Vigilant contract and ensure the contract is updated and in compliance with CJIS Security policy.

4. *To ensure that ALPR images are being shared appropriately:*
  - a. *By April 2020 Fresno should review the entities with which they currently share images, determine the appropriateness of this sharing, and take all necessary steps to suspend those sharing relationships deemed inappropriate or unnecessary.*

The Fresno Police Department has suspended most sharing and now only shares images with bordering states.

- b. *By August 2020 Fresno should revise its written procedures for ALPR image sharing, as necessary, to ensure that it follows these procedures.*

The Fresno Police Department will incorporate these changes into the updated policy.

5. To minimize the privacy risk of retaining ALPR images for long periods of time, Fresno should do the following:
  - a. *By August 2020 review the age of the ALPR images their personnel are searching for and ensure their retention periods for ALPR images are based on department needs. {REDACTED} reflect in its ALPR policy the updated retention period in its policy the updated retention period and state in its policy that it will reevaluate its retention period at least every two years.*

Based on the results of the audit, the Fresno Police Department will amend our current practice of retaining images for one year to six months which is consistent with the time frame the majority of the searches occur.

- b. *Include in their ALPR policies a retention period for data or lists such as hot lists, used to link persons of interest with license plate images, and create necessary processes to ensure that those data unrelated to ongoing investigations are periodically removed from their ALPR systems.*

The Fresno Police Department will maintain active hot lists for 90 days. If an investigator requires a longer period, approval will be obtained from a commander. This will be incorporated in the revised ALPR policy.

Fresno Police Department  
ALPR Audit Response  
January 23, 2020  
Page 3

6. To enable monitoring of user access and user queries of ALPR images, Fresno should do the following:
  - a. *By April 2020 assess the information their ALPR systems capture when users access them to ensure that the systems' logs are complete and accurate and that they form a reasonable basis for conducting necessary, periodic audits.*

This is already being done and is part of the quarterly audit process.

- b. Ensure their ALPR policies make clear how frequently they will audit their ALPR systems, who will perform those audits, who will review and approve the audit results, and how long they will retain the audit documents. [REDACTED] have in place by February 2021 an audit plan that describes its audit methodology, including, but not limited to, risk areas that will be audited, sampling, documentation, and resolution of findings.*

A quarterly audit process has been put in place. The audit process, methodology and responsibilities will be included in the updated ALPR policy.

- c. By June 2021 implement their audit plans and complete their first audits.*

The audit process is already in place and audits were completed for the last two quarters of 2019.

7. To ensure that ALPR access is limited to agency staff who have a right and a need to use ALPR data, Fresno [REDACTED] should do the following:
  - a. *By April 2020 review all user accounts and deactivate accounts for separated employees, inactive users, and others as necessary.*

This has been completed. Separated employees are removed upon notification of their separation. The ALPR system automatically deactivates accounts for users who have been inactive for 365 days.

- b. Ensure that their ALPR policies specify the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on need to know and right to know.*

This will be incorporated into the revised ALPR Policy. Access will be granted on a need to know and right to know basis for sworn department members and crime specialists who have investigative responsibility.

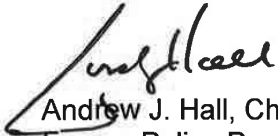
- c. By August 2020 develop and implement procedures for granting and managing user accounts that include, but are not limited to, requiring that a supervisor must approve an account for a user, providing training to users before granting an account, suspending users after defined periods of inactivity, and requiring regular refresher training for active users and training for users before reactivating previously*

Fresno Police Department  
ALPR Audit Response  
January 23, 2020  
Page 4

*inactive accounts. [REDACTED] ensure that it has procedures in place to deactivate accounts immediately for account holders who separate from the agency or who no longer need a user account.*

The Fresno Police Department will incorporate supervisor approval for new accounts and minimum training requirements for new users in the revised policy.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew J. Hall", is written over a horizontal line.

Andrew J. Hall, Chief of Police  
Fresno Police Department

AJH: rb

February 2020

## LOS ANGELES POLICE DEPARTMENT



**MICHEL MOORE**  
Chief of Police

**ERIC GARCETTI**  
Mayor

P. O. Box 30158  
Los Angeles, Calif. 90030  
Telephone: (213) 486-0150  
TDD: (877) 275-5273  
Ref #: 1.1

February 4, 2020

Elaine Howle\*  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

Dear Ms. Howle:

In response to your draft report titled "Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects," I would like to inform you that the Los Angeles Police Department (LAPD) has the utmost respect for individuals' privacy and currently has policies and procedures in place to safeguard personal information stored on the Automated License Plate Reader (ALPR) Systems. Personnel who utilize ALPR data have been through extensive training on accessing and using the data on a right to know and need to know basis. The LAPD continuously reviews all user accounts and deactivates accounts for separated employees, while allowing ALPR access to all active employees who have attended the training. ① ②

Although our dedication to protecting individuals' privacy is covered in our day to day operations and procedures, the Department is currently working on an ALPR policy to ensure that the protection of those rights is also memorialized in our Department Manual. The aforementioned ALPR policy will be completed by April 2020 and posted on the Department website once it is completed, as required by state law. The policy will address the types of information personnel may upload into the ALPR systems, as well as the retention period for the data or lists (i.e., hot lists used to link persons of interest with license plate images). The LAPD will perform an assessment of the systems' data security features and retention periods for ALPR images to evaluate the need for adjustment, prior to publishing of the ALPR policy. Furthermore, the policy will list the entities the Department shares ALPR images with and the process for handling image-sharing requests.

To ensure the ALPR policy is up to date and our ALPR systems are capturing proper information, the Department will perform periodic audits to assess the information the systems capture when accessed by the Department users. Per the recommendations listed in your audit draft report, the Department will have a plan that describes the periodic audits by February 2021 and will complete the first audit by June 2021.

Should you have any questions concerning this matter, please contact Sergeant Monica Tokoro, at (213) 486-0197.

Very truly yours,

  
**MICHEL R. MOORE**  
Chief of Police

**AN EQUAL EMPLOYMENT OPPORTUNITY EMPLOYER**  
[www.LAPDOnline.org](http://www.LAPDOnline.org)  
[www.joinLAPD.com](http://www.joinLAPD.com)

\* California State Auditor's comments appear on page 61.

Blank page inserted for reproduction purposes only.

## Comments

### CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE LOS ANGELES POLICE DEPARTMENT

To provide clarity and perspective, we are commenting on the response to our audit report from the Los Angeles Police Department. The numbers below correspond with the numbers we have placed in the margin of its response.

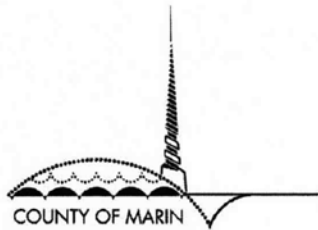
Los Angeles is the only one of four agencies we audited that did not have the ALPR policy state law requires. As we describe on page 15, state law requires law enforcement agencies to have written usage and privacy policies and for the policies to include various elements. As we describe on page 17, the program administrator for Los Angeles initially believed that the agency's many IT policies cover the ALPR program, but we identified deficiencies in the policies he shared with us. When we brought those deficiencies to the administrator's attention, he acknowledged the need for Los Angeles to have an ALPR policy.

①

We stand by our conclusion that Los Angeles does not follow best practices for granting users ALPR system access. As we describe on page 33, of the four agencies we reviewed Los Angeles was the most lax in its approach to authorizing user accounts. The protocol its IT division follows is to include its ALPR software on each computer it assigns to staff, regardless of their position. Thus, staff who do not perform functions related to the ALPR system and possibly have not had training, nevertheless have access to the system. Moreover, on page 34 we state that the detective who conducts ALPR training confirmed that Los Angeles has not required training before users can access the ALPR system.

②

Blank page inserted for reproduction purposes only.



OFFICE OF THE  
COUNTY COUNSEL

Brian E. Washington  
COUNTY COUNSEL

January 28, 2020

Jack F. Gavi  
ASSISTANT COUNTY COUNSEL

Elaine M. Howle, CPA \*  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

Renee Giacomini Brewer  
CHIEF DEPUTY COUNTY COUNSEL

Dear Ms. Howle:

Patrick M. K. Richardson  
Stephen R. Raab  
Steven M. Perl  
Brian C. Case  
Jenna J. Brady  
Valorie R. Boughey  
Kerry L. Gerchow  
Tarisha K. Bal  
Deidre K. Smith  
Brandon W. Halter  
Sarah B. Anker

The Marin County Sheriff's Office appreciates the opportunity to respond to your draft report entitled, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

DEPUTIES

The Marin County Sheriff's Office is pleased to note that although your draft report includes recommendations to the Marin County Sheriff's Office regarding its use of automated license plate reader (ALPR) cameras, your audit team did not find any evidence of abuse or misuse of ALPR data by the Marin County Sheriff's Office.

Colleen McGrath  
ADMINISTRATIVE SERVICES  
OFFICER

Nevertheless, the Marin County Sheriff's Office is and remains committed to the need for further improvement and as stated in your draft report, will consider your report's recommendations. However, based on some of the redactions in the draft report, it is difficult, at times, to determine which findings and conclusions are in reference to the Marin County Sheriff's Office as opposed to the other confidential law enforcement agencies discussed in your draft report.

Marin County Civic Center  
3501 Civic Center Drive  
Suite 275  
San Rafael, CA 94903  
415 473 6117 T  
415 473 3796 F  
415 473 2226 TTY  
[www.marincounty.org/cl](http://www.marincounty.org/cl)

Accordingly, in responding to the issues discussed in your draft report with additional details and/or context, the Marin County Sheriff's Office will address sections which may not apply to it because it is unable to distinguish which law enforcement agency is being implicated.

The following is the Marin County Sheriff's Office response:

**Recommendation No. 1:** Improve their ALPR policies.

**Response to Recommendation No. 1:** While the Marin County Sheriff's Office agrees that its current policy regarding the ALPR system does not specifically describe a "process for periodic system audits," the Marin County Sheriff's Office's policy does state that user/data query audits would be performed. Moreover, although the audit team contends that the ALPR data collected by the

\* California State Auditor's comments begin on page 67.

PG. 2 OF 4

Marin County Sheriff's Office qualifies as personal information, this is not the case. The draft report readily admits that there is no personally identifiable information contained in a license plate capture. Further, the audit team's erroneous belief is based on a free text box in the ALPR system wherein a user *could* enter a person's name in this text box and attach personal information to the images of license plates captured by the ALPR system. However, the Marin County Sheriff's Office does not utilize this free text box and does not enter any other personal information to be associated with the images taken by its ALPR system. In fact, the draft report concedes this fact as it states in regard to the Marin County Sheriff's Office and open text fields, the audit team "did not find personal information in combination with other sensitive information in the six months of search records [it] studied."

**Recommendation No. 2:** Implement needed ALPR data security.

**Response to Recommendation No. 2:** As noted in the draft report, the Marin County Sheriff's Office contracts with a third-party vendor Vigilant Solutions (Vigilant) regarding its ALPR system. While the audit team is critical of Vigilant, all access to Vigilant for the Marin County Sheriff's Office is activity logged and auditable as noted in the draft report, even if the user accesses the system via the internet with a personal device, and those logs are reviewed by the Marin County Sheriff's Office ALPR program administrator; all data on Vigilant is stored on secure servers in the United States as recommended by the audit team; and Vigilant only permits credentialed law enforcement officers with a valid Originating Agency Identifier (ORI) number issued by the Criminal Justice Information System (CJIS) Division of the Federal Bureau of Investigation (FBI). Additionally, as part of its services, Vigilant maintains it is compliant with all relevant requirements set forth in the FBI-CJIS Security Policy as recommended by the audit team.

**Recommendation No. 3:** Update vendor contracts with necessary data safeguards.

**Response to Recommendation No. 3:** As discussed above, while not explicitly stated in the Marin County Sheriff's Office's contract with Vigilant, Vigilant warrants in its services that the data captured by an agency remains the property of the agency; all data is stored on secure servers in the United States; and it conforms with all relevant requirements set forth in the FBI-CJIS Security Policy.

**Recommendation No. 4:** Ensure that sharing of ALPR images is done appropriately.

**Response to Recommendation No. 4:** As discussed above, the Marin County Sheriff's Office has confirmed with Vigilant that it has and continues to verify that it only permits credentialed law enforcement officers with a valid ORI number issued by the CJIS Division of the FBI access to the data on its hosted

PG. 3 OF 4

server. While the audit team was critical of the Marin County Sheriff's Office sharing information with agencies such as the Honolulu Police Department, such cooperation with this particular law enforcement agency was done properly and with consideration as to the multiple matters which have in the past involved both agencies.

⑥

As for ICE access, any prior approval by the Marin County Sheriff's Office with Vigilant was before any of the relevant state law went into effect. As noted in the draft report, Vigilant confirmed that the recent viewing of ICE accounts in question were not active and that these inactive agencies were not previously visible to the Marin County Sheriff's Office.

⑥

**Recommendation No. 5:** Evaluate and reestablish data retention policies.

**Response to Recommendation No. 5:** The Marin County Sheriff's Office's two-year retention policy is based on the statute of limitations for most crimes in the State of California. The audit team states that it would like the Marin County's Sheriff's Office to have a more detailed policy regarding retention based on usefulness of images to investigators and even suggest that the retention of the images should be based on whether the images are for minor crimes versus complex crimes. However, it would be impossible for the Marin County Sheriff's Office to know whether the captured images would be used in a minor criminal case or a major felony case at the time the images were taken or at any time afterwards. Indeed, as noted in the draft report, there is no statute of limitations for the crime of murder.

⑦

**Recommendation No. 6:** Develop and implement procedures for granting and managing user accounts.

**Response to Recommendation No. 6:** The audit team believes that the Marin County Sheriff's Office should require supervisory approval for all users of its ALPR system. As noted above and in the draft report, at this time the Marin County Sheriff's Office does not believe that this particular requirement is appropriate for the following reasons: there is no personal information associated with the images taken by the Marin County Sheriff's Office; as discussed in the draft report, all users of the ALPR system receive training before they are permitted access to the ALPR system; and the Marin County Sheriff's Office regularly audits the use of the ALPR system.

⑧

**Recommendation No. 7:** Develop and implement ALPR system oversight.

**Response to Recommendation No. 7:** In the draft report, the audit team identifies an incident in which it claims it brought to the Marin County Sheriff's Office's attention an active account for a resigned employee. However, this is not accurate. The system administrator was notified about deactivating the account on the same day the audit team informed him about this account. However, the

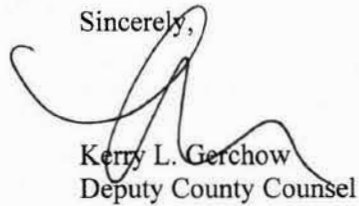
⑨

PG. 4 OF 4

ALPR administrator had deactivated the account *prior* to the audit team discussing this particular account with him. Moreover, the ALPR administrator does not solely rely on a department-wide email notification regarding resigned or terminated employees as discussed in the draft report. In addition to the audits he regularly performs, the ALPR administrator also performs periodic spot checks to verify that active accounts match active employees.

Should you have any questions regarding this response, including any comments and clarifications made herein, please do not hesitate to contact us directly.

Sincerely,

A handwritten signature in black ink, appearing to read "Kerry L. Gerchow", is written over the typed name and title.

Kerry L. Gerchow  
Deputy County Counsel

## Comments

### CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE MARIN COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Marin County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

Marin's response correctly notes that our review of its internal affairs investigations records did not identify evidence of abuse or misuse of ALPR data. However, as we state on page 37, we do not consider this absence as proof that no instances of ALPR misuse occurred. There is the possibility that misuse occurred and went unnoticed and unreported, particularly since Marin does not conduct audits of its ALPR system.

①

During our exit conference, we specifically informed Marin that we would send it only those portions of the draft report that were relevant to it. The text that we redacted pertains to the other entities that were part of the audit and that we are required by law to keep confidential. Further, during its review of the draft report, Marin did not communicate with us to seek clarification regarding the report content we provided, despite our providing multiple opportunities for it to do so.

②

Marin is incorrect in stating that we contend that the license plate images Marin collects qualify as personal information. On page 11, we note that a law enforcement agency can enter additional information, such as personal information, into its ALPR system. However, we do not assert that the ALPR image alone contains personal information.

③

Marin has mischaracterized our finding. In its response, Marin states that we based our conclusion on a free-text box wherein a user could enter an individual's name and attach it to a license plate image. However, as we describe on pages 18 and 19, we based our conclusion on information that users enter into open text fields as part of license plate searches, specifically the fields for case numbers and purpose for the searches. On page 37, we note that Marin requires users to enter both case numbers and reasons for the search before allowing such searches. Although we did not find evidence users had entered personal information in combination with other sensitive information in the six months of search records we studied, the fact that these text fields exist means that users could enter such information during ALPR searches, as we point out on pages 18 and 19. Moreover, Marin's ALPR policy does not prohibit users from entering personal information in combination with other sensitive information in its ALPR system.

④

- ⑤ We disagree with the focus of Marin's response, which implies that the vendor's security controls are a suitable substitute for specific contract safeguards. As we show in Figure 3 on page 22, Marin's contract does not contain any of the safeguards CJIS policy recommends for contracts with cloud vendors. We note on page 21 that CJIS policy states that ambiguous contract terms can lead to controversy over data privacy and ownership rights, whereas a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.
- ⑥ We disagree with Marin's belief that it has managed its image sharing appropriately. Although Marin described in its response the type of information that it could maintain to document its image-sharing decisions, it did not provide such evidence documenting why it made past sharing decisions, and its ALPR policy does not include a process for approving image-sharing requests, as we state on page 26. Moreover, Marin acknowledged in its response the issue we describe on page 26 regarding ICE and the fact that the status of Marin's sharing relationship with ICE was not always visible to Marin. This issue underscores the need for Marin to maintain records regarding sharing decisions.
- ⑦ Marin appears to miss the point of our recommendation. As we state on page 29, we concluded that Marin did not establish its retention period based on when it uses the ALPR images it captures. On page 31, we mention minor and complex crimes as examples of ALPR data being used narrowly, such as for the single purpose of locating stolen vehicles, or broadly, such as for investigation of crimes in addition to stolen vehicles. Our recommendation—based on our analysis of Marin's search activity as referenced on page 30—provides a method for Marin to better align how long it retains ALPR data with whether it actually uses the data as they age.
- ⑧ The reasons Marin cites in its response for not adopting our recommendation are not valid. Requiring a supervisor to approve a user for an ALPR account is a meaningful step in establishing that user's need to access ALPR data and right to know what the data portray in an effort to avoid the ALPR data being misused. In point 4 above, we describe that the existence of text fields in the ALPR system allows for personal information to be linked to license plate images. Further, we note that Marin has no policy prohibiting its users from entering personal information in its ALPR system. In addition, despite Marin's claim of training all users, we state on page 34 that Marin does not require staff to renew their training when reactivating their user accounts following long periods of not using the ALPR system. Finally, we found that contrary to Marin's assertion, it had not regularly audited its system. As we discuss

on page 37, Marin's ALPR administrator was unaware of the state law requiring audits of ALPR systems, so he had not been conducting them. Despite recent efforts to institute some form of monitoring, as we describe on page 38, the limitations in its approach led us to conclude that Marin does not have sufficient protocols in place to detect the misuse of user accounts.

Marin's assertion is incorrect. As we describe on page 35, we reviewed Marin's processes for disabling the accounts of separated employees. Although Marin's ALPR administrator informed us of his approach for deactivating an account when he receives an all-staff email that an employee is separating from the department, we found such an email dated August 6, 2019, after which one separated employee continued to hold an active account as of October 22, 2019. After we informed the administrator of this employee's continued access, the administrator acknowledged that the account was still active, and we directly observed him deactivating the account.

⑨

Blank page inserted for reproduction purposes only.

February 2020

**Human Assistance**

Ann Edwards, Director

**Branches**Customer Service Operations  
Finance and Administration  
Community and Program Support

County Veterans Services Office

**County of Sacramento**

January 27, 2020

Elaine M. Howle  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

SUBJECT: License Plate Readers Audit Response

Dear Ms. Howle:

We are writing in response to the draft findings of your report, titled Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects.

The Department of Human Assistance (DHA) appreciates the work performed by the California State Auditor. No recommendations were issued in the report, and DHA agrees with the results of the audit.

If you have any questions regarding this matter, please contact Lane Ruddick, Program Integrity Chief, by telephone at (916) 875-1275, or by email at [ruddickl@saccounty.net](mailto:ruddickl@saccounty.net).

Sincerely,

A handwritten signature in cursive script that reads "Ann Edwards".

Ann Edwards  
Director

Blank page inserted for reproduction purposes only.



## SACRAMENTO COUNTY SHERIFF'S OFFICE

**Scott R. Jones**  
Sheriff

January 28, 2020

Elaine M. Howle, CPA\*  
California State Auditor  
621 Capitol Mall, Suite 1200  
Sacramento, CA 95814

Dear Ms. Howle:

I am in receipt of the draft report entitled *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards Over the Data It Collects*, which includes recommendations for the Sacramento County Sheriff's Office to revise and improve some of our Automated License Plate Reader program (ALPR) processes.

While I agree with some of your findings, I disagree with some of the characterizations made. As the Sheriff of Sacramento County, I take seriously the protection of our citizens, including their personal privacy. Within our role as guardians of the data we collect, my staff works diligently to develop and consistently apply security protocols that maintain the integrity of our systems. ①

The Summary (Results in Brief) section of the report was clearly written separately or prior to the completion of the main body of the report, because it fails to present your teams' actual conclusions. Let me address each point. ①

### Recommendation #1 – Review and revise policies

Before the Audit began, the Sacramento County Sheriff's Office began reviewing and revising policies governing a wide range of service deliverables. Although the Sacramento County Sheriff's Office existing policy contains the majority of the requirements outlined in California Civil Code section 1798.90.51, it does not list the restriction on selling ALPR data. As expressed during the interviews, my staff did say that the restriction on selling data is not listed in the policy because the Sacramento Sheriff's Office does not sell any data. The lack of specifically addressing this fact in the ALPR policy is an oversight.

Elaine M. Howle, CPA  
January 28, 2020  
Page 2

Recommendation #2 – Identify types of data and perform a security assessment

As you learned during the audit, the Sacramento County Sheriff's Office began reorganizing ALPR related security over two years ago. The initial step of this process was securing funding to hire a fulltime Information Technology Analyst in hopes of increasing program administration because this employee's primary job will be the continuous development of ALPR related security protocols that either meet or exceed these recommendations.

Recommendation #3 – Ensure the vendor offers the strongest possible data protections

The Sacramento County Sheriff's Office completed extensive research in the use of cloud storage systems and CJIS security. I am aware your team received the latest contract between the Sacramento County Sheriff's Office and Vigilant Solutions and the Vigilant CJIS Security Policy Guide. Both the contract and comprehensive policy provide a thorough explanation regarding compliance including agreeing to participate in any Technical Security Compliance Audit performed by the FBI-CJIS Division.

②

Recommendation #4 – Develop a process for handling ALPR image-sharing requests

Although the existing policy does provide language on how sharing data can occur, the Sacramento County Sheriff's Office began developing a ticketing system for handling various technology requests over four years ago. As such, the natural progression was to utilize the same request, approval, and record retention system used by the entire organization.

③

Recommendation #5 – Review the retention periods of ALPR images and data

The Sacramento County Sheriff's Office is continually reviewing data retention practices. Although, a simple review of searches provides a small subset of activity, the success of an ALPR program could only come from tracking and identifying which cases provided leads or convictions of data. During the audit, my understanding is your team was told this very fact. As the agency prepares to transition to a new report writing system, I request our crime analysts to conduct a multi-year study that will provide a realistic view of how long ALPR images provide usefulness in the criminal justice system.

④

Recommendation #6 – Enable monitoring of user access and user queries of ALPR images

Throughout the audit your team requested a substantial number of reports and logs showing when accounts were activated, deactivated, or changes occurred. The ability to provide these reports demonstrated the robust nature of the logging system. Although your team learned the

Elaine M. Howle, CPA  
January 28, 2020  
Page 3

Sacramento County Sheriff's Office has no reported incidents of ALPR misuse, I have directed my program administrator to make certain fields mandatory to ensure proper documentation of usage. With the addition of a dedicated IT Analyst, the expansion of audits already occurring will surely continue.

Recommendation #7 – Ensure that ALPR access is limited to agency staff who have a right and a need to know

Not only is this recommendation listed in the Sacramento County Sheriff's Office policy, it is the way the organization operates with all data systems. As this directly relates to ALPR, only 561 employees, out of a department of 2,170, have access to the system. While I understand your position that a supervisor should approve each account, there were over 5,880 personnel moves during 2019. The Sacramento County Sheriff's Office uses Role Based Access Controls. Rather than rely solely on a supervisor to approve a request, the application of Role Based Access Control is how the Security Operations unit of the Sacramento Sheriff's Office processes access to this and all other law enforcement data systems. Role Based Access Controls are addressed by the National Institute of Standards and Technology as a best practice.

⑤

In Conclusion

In the end, we are not opposed to implementing many of your recommendations and in fact, are already in the process of doing so. Throughout the process, which was long and took many staff hours, we made every effort to cooperate with the auditor's requests for information and tried to anticipate the types of problems they would find while trying to understand the actual uses and practices within the ALPR program.

During interviews and based on some of the requests, we felt concern that there was a bias toward a particular outcome, intended or otherwise. Because this report contains many redacted sections, there is still some concern about what has not been shown to us. Nonetheless, we await your full findings about Sacramento and the other agencies covered in this report.

⑥

⑦

Very truly yours,



SCOTT R. JONES, SHERIFF

Blank page inserted for reproduction purposes only.

## Comments

### CALIFORNIA STATE AUDITOR'S COMMENTS ON THE RESPONSE FROM THE SACRAMENTO COUNTY SHERIFF'S OFFICE

To provide clarity and perspective, we are commenting on the response to our audit report from the Sacramento County Sheriff's Office. The numbers below correspond with the numbers we have placed in the margin of its response.

We stand by the language we use to describe Sacramento's ALPR program. Our report provides appropriate context and sufficient evidence to support our findings. Further, the Results in Brief section of the report serves as a summary of the report as a whole and as such it represents the overall conclusions for this report. The details of our findings and conclusions are included in the Audit Results section of the report.

①

We disagree with Sacramento's contention that the department's current contract is thorough. On pages 22 and 23, we acknowledge that Sacramento updated its contract with Vigilant in September 2019. In reviewing that latest version, we determined that it is missing some of the best practices outlined in CJIS policy, as we show in Figure 3 on page 22. On page 21, we note that CJIS policy states that a contract that clearly establishes data ownership acts as a foundation for trust that the cloud vendor will protect the privacy of the agency's data.

②

Sacramento's response implies that a process for approving image-sharing requests and maintaining records outside of the Vigilant system was already in place. However, although Sacramento states that it began developing a ticketing system for handling technology requests more than four years ago, as we discuss on page 26, Sacramento could not provide any evidence of records outside of the Vigilant user interface demonstrating when or why it agreed to share with particular entities. As we further point out on page 26, Sacramento's ALPR policy currently does not include a process for approving sharing requests.

③

Sacramento's proposed study of ALPR images may benefit its ALPR program. Our analysis of the search records from the agencies we reviewed—summarized on page 30 and in Table 2—presents one method of identifying the age of the data personnel are using. We point out on page 31 that the agencies' existing ALPR systems provide the ability to conduct such an analysis. Nevertheless, our recommendation does not preclude the type of analysis Sacramento describes in its response.

④

- ⑤ We stand by our recommendation that Sacramento should have a policy that clearly states the staff classifications, ranks, or other designations that may hold ALPR system user accounts and that accounts are granted based on a need to know and a right to know. As we state on page 32, each ALPR administrator, including Sacramento's, stressed the concept of "need to know, right to know." Assigning an individual an ALPR account based strictly on his or her classification or role—the practice Sacramento follows—does not ensure that an individual has a need to know because of their specific assigned work.
- ⑥ Sacramento's concern about bias is unfounded. To meet generally accepted government auditing standards, which my office is obligated to comply with, we have and follow policies and procedures for all audits to ensure that we identify and rectify any threats to our independence, including bias. Moreover, we follow quality control procedures on every audit that ensure that we have sufficient and appropriate evidence to support our findings and conclusions.
- ⑦ Sacramento received draft text that was relevant to our findings about it. State law requires us to keep confidential information about an unpublished audit. Consequently, we cannot share with one agency information about another. Sacramento received a draft audit report with redacted information regarding other agencies as necessary to maintain confidentiality. During our exit conference, we stressed that staff should contact us with questions they might have about the draft report during the formal review period; Sacramento did not contact us. We also contacted Sacramento's ALPR administrator during the formal review period to inquire about questions staff may have, and he did not return our call.

## REPORT

# Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use



Spencer Platt/Getty

**SUMMARY:** The proliferation of ALPR technology raises serious civil rights and civil liberties concerns. Courts, lawmakers, and technology vendors must take action.



Ángel Díaz



Rachel Levinson-Waldman

**PUBLISHED:** September 10, 2020

Americans drive. According to one survey, 83 percent of U.S. adults drive a car at least several times a week. <sup>1</sup> In jurisdictions with limited or no public transportation, driving may even rival cell phone use as a modern necessity. Cars connect people with work, love, school, prayer, and protest.

They also leave a data trail. Historically, it would have been virtually impossible for law enforcement to routinely surveil all drivers. However, with the growing use of automatic license plate readers (ALPRs), police can now receive alerts about a car's movements in real time and review past movements at the touch of a button. ALPRs could prove valuable in police investigations and for non-law enforcement uses like helping government agencies to reduce traffic and curb environmental pollution. But legal and policy developments have failed to adequately address the risks posed by this highly invasive technology. <sup>2</sup>

Recent events crystalize ongoing concerns. With Black Lives Matter demonstrations taking place across the United States in the wake of the George Floyd and Breonna Taylor murders, law enforcement agencies large and small are deploying their expansive surveillance arsenals to monitor protesters. For many agencies, those surveillance tools include ALPRs, which have heightened relevance in localities where people must drive to protests, or if protests themselves are occurring by car, as is increasingly happening during the ongoing Covid-19 pandemic. <sup>3</sup>

The pandemic adds an additional dimension for consideration, as states look for creative ways to control the virus's spread. With car travel expected to increase as states begin slowly loosening restrictions, ALPRs may play a larger role in law enforcement. <sup>4</sup> States such as Rhode Island have already directed law enforcement to look for New York license plates in order to identify people who should be directed to self-quarantine. <sup>5</sup> Law enforcement agencies may look to automate this process by using ALPR devices to alert officers any time an out-of-state license crosses into their localities.

This white paper explains how ALPR technology works, focusing on its use by law enforcement agencies. It then analyzes both the legal and policy landscapes, including how courts have ruled on the use of ALPRs, and how they can be expected to rule in the future. Next, it outlines a series of concerns, ranging from high error rates to the impact on civil liberties and civil rights. Finally, it concludes with a set of recommendations for law enforcement, lawmakers, and technology vendors to enhance transparency and accountability and mitigate the impact of this technology on individuals' civil liberties and civil rights.

## How Do Automatic License Plate Readers Work?

Automatic license plate readers use a combination of cameras and computer software to indiscriminately scan the license plates of every car passing by. The readers, which can be mounted on stationary poles, moving police cruisers, and even handheld devices, log the time and date of each scan, the vehicle's GPS coordinates, and pictures of the car. Some versions can also snap pictures of a vehicle's occupants and create unique vehicle IDs.

<sup>6</sup> The devices send the data to ALPR software, which can compare each plate against a designated "hot list." Such lists can include stolen cars and cars associated with AMBER Alerts for abducted children. <sup>7</sup> They can also reference vehicles that are listed in local and federal databases for reasons that may include unpaid parking tickets or inclusion in a gang database. <sup>8</sup> These queries happen automatically, though officers can also query plates manually. <sup>9</sup>

In addition to checking data in real time, many cities and agencies retain plate information for future use, sometimes indefinitely. <sup>10</sup> This data can be used to plot a particular vehicle's various locations or to identify all the cars at a given location, and it can even be analyzed to predict routes and future locations of a vehicle or set of vehicles. <sup>11</sup> These tools may cost little or nothing for police, often because the drivers themselves shoulder the cost of the technology through a fee charged on top of traffic ticket costs. <sup>12</sup> Notably, drivers in some jurisdictions can be jailed for failure to pay the private company's fee. <sup>13</sup>

Law enforcement use of ALPRs is rapidly expanding, with tens of thousands of readers in use throughout the United States; one survey indicates that in 2016 and 2017 alone, 173 law enforcement agencies collectively scanned 2.5 billion license plates. <sup>14</sup> According to the latest available numbers from the Department of Justice's Bureau of Justice Statistics, 93 percent of police departments in cities with populations of 1 million or more use their own ALPR systems, some of which can scan nearly 2,000 license plates per minute. <sup>15</sup> In cities with populations of 100,000 or more, 75 percent of police departments use ALPR systems. <sup>16</sup> In some of the largest U.S. cities, millions of license plates are scanned over the course of a year. <sup>17</sup> According to a 2020 Cali-

fornia state auditor report, the Los Angeles Police Department (LAPD) alone has accumulated more than 320 million license plate scans, and the Sacramento Police Department recorded up to 1.7 million scans in just one week. <sup>18</sup> Despite this expansive data collection effort, many departments have not developed a policy to govern the use of ALPR technology, or provided privacy protections. While states such as California and Nebraska have passed laws requiring their departments to establish ALPR policies, not all departments have complied. <sup>19</sup>

Law enforcement use of ALPR data is not limited to reads captured by departments' own devices; many departments have contracts with vendors that grant them access to private databases containing scans from private ALPRs and from other local and federal law enforcement agencies. For example, Vigilant Solutions (owned by Motorola Solutions), a leading provider of ALPR data to police based in Livermore, California, sells access to its database of more than 5 billion license plate scans collected across the country, including 1.5 billion reads provided by law enforcement agencies. This process creates a revolving door of license plate scans from law enforcement to Vigilant Solutions back to law enforcement agencies. <sup>20</sup>

Moreover, access to ALPR tools and data is not limited to law enforcement. For example, government agencies use license plate readers to automate toll collection and for pollution research; businesses analyze ALPR location data when assessing loan applications to help verify an applicant's listed home address or to detect commercial use of vehicles when analyzing insurance claims; and private individuals and neighborhood associations can buy ALPRs for home and neighborhood security purposes. <sup>21</sup> These private actors can maintain their own hot lists of flagged license plate numbers and can share any data they collect with law enforcement at their discretion. <sup>22</sup> Similarly, public agencies that collect and store ALPR data for non-law enforcement purposes may hold onto a dataset that proves alluring for police departments.

## What Does the Law Say?

The U.S. Constitution's Fourth Amendment protects people from unreasonable searches and seizures. <sup>23</sup> According to the U.S. Supreme Court, the Amendment's purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." <sup>24</sup> Until the late 1960s, the Supreme Court ruled that Fourth Amendment protections only applied to searches and seizures of tangible property. <sup>25</sup> But in 1967, the Court expanded Fourth Amendment protections, holding in *Katz v. U.S.* (1967) that "the Fourth Amendment protects people, not places." <sup>26</sup> Specifically, the government was now prohibited from intruding upon a person's "reasonable expectation of privacy." In other words, if an individual seeks to keep something private, and that expectation of privacy is "one that society is prepared to recognize as reasonable," the Fourth Amendment is triggered, and the government generally must obtain a warrant supported by probable cause before conducting a search. <sup>27</sup> This approach seeks to protect the "privacies of life" from "arbitrary power," and to "place obstacles in the way of a too permeating police surveillance." <sup>28</sup>

By contrast, the Court has not required a warrant or other heightened standard for police officers to take pictures of individual license plates and compare them against a law enforcement database. Its reasoning has been twofold. First, due to "the pervasive regulation of vehicles capable of traveling on the public highways," there is no expectation of privacy in the content of license plates. <sup>29</sup> Second, longstanding precedent holds that drivers on public roads cannot expect their movements to be kept private from the police since they could be observed by any member of the public (though, as discussed below, this presumption is beginning to shift). In keeping with these doctrines, courts have regularly held that law enforcement officers may, at their discretion and without any suspicion of criminal activity, perform at least an initial check of a license plate against a law enforcement database. <sup>30</sup>

Even so, there have long been hints that the tracking of vehicles' movements could, under some circumstances, trigger Fourth Amendment concerns. As far back as 1979, the Supreme Court declared that "an individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regulation." <sup>31</sup> Similarly, when the Court analyzed the use of beeper technology in the 1980s, it distinguished limited monitoring from "twenty-four hour surveillance of any citizen in the country," reserving the question of whether such "dragnet type law enforcement practices" merit the application of different constitutional principles. <sup>32</sup>

More recently, the Court's application of the Fourth Amendment has evolved significantly in response to technological "innovations in surveillance tools." <sup>33</sup> In *Kyllo v. U.S.* (2001), for instance, the Supreme Court held that police need a warrant before they can use a thermal imager to detect heat coming from a garage. By doing so, the Court rejected a return to a "mechanical interpretation" of the Fourth Amendment, under which the Constitution would have protected only against physical intrusions into a person's private space, holding instead that it was necessary to ensure that people were not left "at the mercy of advancing technology." <sup>34</sup> Over time, the Court has ruled that law enforcement must obtain a warrant before searching a suspect's cell phone during an arrest (even though it had previously allowed warrantless searches incident to arrest), before installing a GPS tracker on an automobile for long-term monitoring (despite precedent suggesting that vehicular movements are not private), and before obtaining historical cell-site location information revealing an individual's daily movements (although third-party information can normally be obtained without a warrant). <sup>35</sup>

The reasoning in these cases is instructive. Take *U.S. v. Jones* (2012), in which the Supreme Court held that the police need a warrant in order to install a GPS tracking device on a car and use it for extended surveillance. In her concurrence, Justice Sonia Sotomayor observed that inexpensive location tracking "makes available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track" that it "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" <sup>36</sup> Similar themes run through the Court's decision in *Carpenter v. U.S.* (2018), which holds that police must get a warrant before they can obtain historical information from cell phone providers about the location of individuals' mobile phones (known as cell-site location information, or CSLI). <sup>37</sup> The Court observed that this information could be used to track the minutiae of people's daily lives. It reasoned that the "depth, breadth, and comprehensive reach" of this data, along with "the inescapable and automatic nature of its collection" by virtue of simply carrying a cell phone, necessitate a warrant supported by probable cause. <sup>38</sup>

While the *Carpenter* decision narrowly addresses the use of historical CSLI, it provides an important framework for analyzing reasonable expectations of privacy in the digital age. Location tracking via ALPR databases raises many of the same concerns outlined in *Carpenter*; an application of its framework should lead courts to conclude that police must first obtain a warrant before searching historical location information from ALPR databases.

Specifically, first, *Carpenter* instructs courts to consider the capacity of a technology to enable ongoing surveillance that would have been unimaginable before the digital age. <sup>39</sup> Just as with CSLI, automatic license plate readers enable data collection that is "detailed, encyclopedic, and effortlessly compiled." <sup>40</sup> A person's phone is constantly creating records simply by being powered on and connecting to the network. Similarly, ALPRs automatically collect information about every car that passes within their range. But while a person might turn off their cell phone while they travel, it may be almost impossible to avoid traveling some roads without exposing one's vehicle to ALPRs.

Second, the *Carpenter* Court considered the extent to which data collection is indiscriminate, targeting not only people under investigation but a much broader segment of the population. <sup>41</sup> While ALPR scans provide a different level of pinpoint accuracy than CSLI, they also indiscriminately collect data about every car that passes by a license plate reader, regardless of the driver's connection to criminal activity. In fact, the vast majority of scans capture information about drivers who are not suspected of any wrongdoing. <sup>42</sup> The only limitations on this ongoing surveillance of all cars traveling a public road are the number of ALPRs and the data retention policies maintained by police or third-party vendors.

Third, the Court considered the extent to which the long-term CSLI retention allowed officers to effectively create a time machine of a person's movements. Just as with historical CSLI, the long-term retention of plate data allows the police to retroactively track every location where a particular car was tagged by an ALPR device. <sup>43</sup> To be sure, the current scope of ALPR devices does not match the scope of cell phone towers blanketing the country, which makes a direct comparison difficult. Nonetheless, the current adoption rate of ALPRs suggests that this technology will continue to expand its coverage areas. In fact, the *Carpenter* Court ruled that lower courts "must take account of more sophisticated systems that are already in use or in development." <sup>44</sup> ALPR technology is expanding at a rapid rate, with growing databases containing billions of license plate scans, and with governmental and private ALPR devices capturing larger swaths of cities. Courts should consider this foreseeable future when confronted with nascent uses of ALPR that appear smaller in scale.

Finally, the Court ruled that an interpretation of the Fourth Amendment called the third-party doctrine is inapplicable to historical CSLI. <sup>45</sup> Under the third-party doctrine, individuals do not have a reasonable expectation of privacy in information they are deemed to have voluntarily handed over to third parties. <sup>46</sup> The *Carpenter* Court found that while this doctrine is appropriate for limited disclosures such as bank records or a log of dialed telephone numbers, it should not apply to CSLI data, which can provide a "chronicle of a person's physical presence compiled every day, every moment, over several years." <sup>47</sup> Historical ALPR data similarly chronicles the movements of all vehicles, regardless of the registered owner's connection to a suspected crime.

The *Carpenter* Court also reasoned that individuals do not truly voluntarily share their location data with wireless carriers; instead, the data is automatically collected simply by possessing a cell phone — a device the Court described as "indispensable to participation in modern society" — and by connecting to a mobile network. <sup>48</sup> Similarly, a majority of Americans rely on driving in order to fully participate in society, and their movements are logged by ALPRs by virtue of simply driving and parking on public roads. Just as the only way to avoid generating CSLI would be to turn off a mobile device, the only way to avoid ALPR data collection would be to give up driving altogether or to keep a vehicle away from the range of a license plate reader — an impossible task in many places. <sup>49</sup> *Carpenter* thus suggests that the third-party doctrine is equally inapplicable to historical location data collected by ALPR devices.

Although the Supreme Court has not yet addressed whether police access to historical ALPR data requires a warrant, appeals courts have begun hearing challenges to warrantless ALPR database searches. However, courts appear reluctant to embrace a bright-line rule that extends *Carpenter* to ALPR searches. The result has been a series of one-off decisions that seek to avoid direct engagement with the foreseeable proliferation of ALPR data.

For example, in *U.S. v. Yang* (2020), the Ninth Circuit ruled that the defendant did not have standing to challenge government queries of a private ALPR database for records of his rental car travels when he kept the vehicle past the contract due date in violation of company policy. <sup>50</sup> This ruling now compels defendants in the Ninth Circuit to prove that they had a sufficiently close relationship with the property that was searched before the court will address their Fourth Amendment rights.

And in *Commonwealth v. McCarthy* (2020), the Massachusetts Supreme Judicial Court ruled that while widespread use of ALPR devices *can* implicate a person's Fourth Amendment privacy interest in the whole of their movements, the limited surveillance undertaken in that case did not violate the defendant's reasonable expectation of privacy. <sup>51</sup> The case involved police officers' use of ALPR hot list notifications to track the defendant's movements as he traveled across two bridges over the course of two months. <sup>52</sup> The court applied what is commonly referred to as the "mosaic theory," where the long-term surveillance of a person's public movements triggers a privacy interest that could be absent with only limited or isolated monitoring. <sup>53</sup> The court acknowledged that "with enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and constitute a search for constitutional purposes." <sup>54</sup> Four ALPR devices on two bridges did not, however, rise to this level, according to the ruling. <sup>55</sup> Lower courts will continue to face the dilemma of how to rule on the specific use of ALPRs in a given case while taking into account the Supreme Court's admonition that courts must consider the logical evolution of these systems of surveillance. <sup>56</sup>

Separate from Fourth Amendment considerations, courts have also considered how ALPR technology may violate privacy protections under state law. For example, the Virginia Supreme Court is currently hearing an appeal seeking to reopen the substantive issue of whether the Fairfax County Police Department's use of an ALPR system to passively track the movements of cars that were not on a hot list violates the state's Government Data Collection and Dissemination Practices Act. <sup>57</sup> This act requires, among other things, that information not be collected unless the need for it has been clearly established ahead of its collection — a standard that indiscriminate collection of ALPR data cannot meet. <sup>58</sup> If the trial court's ruling is upheld, the Fairfax County Police will be required to purge ALPR data that is not linked to a criminal investigation and to stop using ALPRs to passively collect data on people who are not suspected of criminal activity. <sup>59</sup>

ALPRs are relevant to more than privacy. Courts have also considered whether an ALPR hit provides sufficient justification for a police officer to stop a car. In *Kansas v. Glover* (2020), the Supreme Court ruled that a license plate search indicating that a car's registered owner has had his or her license revoked gives police reasonable suspicion to perform a traffic stop in the absence of information suggesting that someone other than the owner is driving the vehicle. <sup>60</sup> Several state courts reached the same conclusion. <sup>61</sup>

An ALPR hit is not always a sufficient basis for a stop, however. <sup>62</sup> In 2014, the U.S. Court of Appeals for the Ninth Circuit considered an erroneous ALPR alert that led to a traffic stop in which a woman was detained and held at gunpoint. <sup>63</sup> Unlike in *Glover*, where an officer manually searched a license plate number and confirmed that the truck he observed matched the vehicle in the database, in *Green v. City and County of San Francisco* (2014), an ALPR device mounted on an officer's cruiser malfunctioned and returned a hit for a different vehicle and license plate number than the plaintiff's car. <sup>64</sup> An officer radioed in a description of the plaintiff's vehicle, along with the incorrect license plate number picked up by the ALPR device. <sup>65</sup> A second officer identified the plaintiff's car, but did not attempt to confirm whether the radioed license plate number matched the plates on the plaintiff's car. The Ninth Circuit ruled that the case could proceed on the question of whether the second officer should have taken additional steps to independently confirm whether the ALPR device had identified the right car and license plate number before initiating a traffic stop. <sup>66</sup> The *Green* decision, which analyzed an ALPR system that "frequently" makes mistakes, may suggest that there are situations in which reliance on an ALPR hit remains insufficient to justify a traffic stop.

## Policy Concerns

In light of the wide saturation of license plate readers, it is critical that the use of these devices be accurate, bias-free, and protective of established legal values and constitutional rights. Unfortunately, publicly available information suggests that this is not the case. This may explain why at least 16 states have passed laws regulating the use of ALPRs or the use of data collected by the devices. <sup>67</sup> Some prohibit the use of ALPRs except for limited public safety purposes, whereas others establish controls governing their use, including mandatory privacy policies, limits on data retention, express limits on the types of investigations in which they can be used, and mandatory audits. <sup>68</sup> These regulations highlight many of the concerns around ALPRs listed below and predict many of the recommendations that follow.

- **High error rates:** Errors can arise in at least two ways — inaccurate hot lists and inaccurate reads. If hot lists are not updated, an individual may be pulled over when, for instance, the system incorrectly indicates that a license is suspended when it has actually been reinstated. Inaccurate reads are surprisingly common as well: one randomized control trial in Vallejo, California, found that 37 percent of all ALPR “hits” from fixed readers (such as those attached to a street light) and 35 percent from mobile ALPRs were misreads — an astonishingly high error rate. <sup>69</sup> In several high-profile incidents, drivers have been pulled over because a reader read the numbers on their license plates wrong and erroneously tagged the vehicles as stolen. <sup>70</sup> In one instance, a Colorado woman and several children were detained and handcuffed facedown on the ground after an ALPR mistook their SUV for a stolen motorcycle from a different state. <sup>71</sup> In another, the chair of Oakland’s Privacy Advisory Commission was mistakenly stopped and detained at gunpoint after his rental car’s license plate triggered an out-of-date hit signaling to police officers that the car had been stolen. <sup>72</sup> Even in cases where a vehicle *is* accurately flagged, it may not convey accurate information about an individual. A car can be shared among family members, among friends, or as part of a carshare; this reality may place low-income individuals, who are more likely to share cars, at greater risk of misidentification.

To be sure, license plate readers have had some high-profile successes: a man accused of stabbing several people after breaking into a rabbi’s home during a Hanukkah celebration was found in part due to an alert from an ALPR device; a Tennessee girl abducted by her noncustodial father was recovered when a license plate camera spotted his car; and police were able to use information from a license plate reader to help halt a string of random shootings on highways in Kansas City, Missouri. <sup>73</sup> Despite these anecdotal successes, there has not been a thorough assessment of the tool’s value. Any such assessment would require consideration of the ALPR’s additional costs and benefits described here.

- **Privacy and data security concerns:** An extremely small percentage of cars scanned by ALPRs — generally far below 1 percent — are connected to any crime or wrongdoing. <sup>74</sup> For example, an audit found that 99.9 percent of the ALPR images stored by the LAPD are for vehicles not on a hot list at the time a license plate was scanned. <sup>75</sup> Nevertheless, many jurisdictions keep the scans “just in case,” storing the data for anywhere from 90 days to two years or even indefinitely. <sup>76</sup> These scans, over time, can reveal individuals’ movements and help create detailed pictures of their private lives. <sup>77</sup>

In addition to information generated by ALPRs, police officers can also add to and store sensitive information in the databases housing license plate scans through open text fields and hot lists available in the user interface. For example, the California state auditor found that law enforcement can input information including personal information such as names, addresses, dates of birth, and physical descriptions, and they can also store criminal justice information such as criminal charges and warrant information. <sup>78</sup> License plate readers have also been known to capture private information, such as shots of children exiting a car in the driveway of a home or activity inside an open garage — information that surely should not be retained. <sup>79</sup> This is information that goes far beyond the legitimate need to find stolen cars or vehicles linked to AMBER Alerts. The ongoing storage of this wide array

of sensitive information also raises security concerns, as this information can be vulnerable to data breaches and hacking. The data security applied to ALPR data may not be commensurate with the sensitivity of the data being held.

- **Data sharing concerns:** Many vendors allow their law enforcement clients to share and receive ALPR data from other law enforcement agencies. For example, through Vigilant Solutions' Law Enforcement Archival Reporting Network (LEARN), police departments can elect to automatically share their collection of license plate reads with outside law enforcement partners that are also part of the network. These data sharing arrangements are not always made public or adequately tracked by police departments, which can result in impermissible or unaccountable sharing. An ACLU investigation found that more than 80 local police departments had set up their LEARN settings to share ALPR data with U.S. Immigrations and Customs Enforcement (ICE), even though the practice may violate local privacy laws or sanctuary policies. <sup>80</sup> Local laws and policies will have limited effect if they do not address automated data sharing or if law enforcement cannot effectively control data flows in and out of their departments. In one instance, the California state auditor found that despite efforts to limit data sharing with ICE, confusing vendor settings had left three different ICE agencies with access to ALPR data from Marin County Sheriff's Office, frustrating compliance with a California law that places controls on local police cooperation with immigration authorities. <sup>81</sup> Customs and Border Protection also receives ALPR data from commercial vendors, including information from across the United States, "outside of the border zone in which CBP activities take place." <sup>82</sup>

With public agencies seeking to collect ALPR data for uses such as toll collection or environmental analysis, there are concerns that the information being collected may be intentionally or unintentionally shared with law enforcement agencies. Without policies governing the type of data that is collected, stored, and shared, these government data sets may create a frictionless data sharing opportunity that frustrates attempts to limit law enforcement access to ALPR data. For example, in San Diego, law enforcement officers regularly access smart streetlight footage — in some cases, to surveil Black Lives Matter protests — even though the streetlights project was originally intended to assist city planners and app developers. <sup>83</sup>

As more companies sell ALPRs to homeowners, additional data sharing concerns emerge. For example, this trend allows police officers to expand the reach of their surveillance systems by providing them with access to private device feeds that may be outside the scope of law enforcement policies governing their own equipment (if any exist at all). When police officers solicit data from private ALPR systems, the decision to share information is up to the individual homeowner or the private company providing the service. While companies may maintain privacy policies that explain the situations in which they share information with law enforcement, the policy only covers the company and the person who purchased the devices. <sup>84</sup> The registered owners of vehicles tracked and logged by these private devices will not receive notice or an opportunity to object to data sharing arrangements between police and private individuals.

- **Layering ALPR data with other surveillance systems:** License plate readers can be used alongside other kinds of technologies to facilitate even more widespread surveillance. The New York City Police Department (NYPD) Domain Awareness System, for instance, can track the movements of cars and people using its 20,000 security cameras and license plate readers (along with face and object detection technology). <sup>85</sup> Several police departments, including those in Chicago, Detroit, and Memphis, incorporate ALPR technology into Real Time Crime Centers (RTCCs) that combine license plate data with surveillance footage from thousands of police, school, and traffic cameras, gunshot detection systems, and social media monitoring. <sup>86</sup> The expansive and ongoing monitoring that is facilitated through these integrated systems may be incompatible with

constitutional freedoms, including the right to free assembly and the right to privacy. These burdens hinder the collective organizing necessary to hold the government accountable to the will of the people.

- **Lack of transparency and access controls:** While ALPRs are increasingly ubiquitous, many police departments do not actively maintain use policies, and there are insufficient controls to protect against misuse. <sup>87</sup> A 2016 investigation by the Associated Press found that police officers across the country abuse confidential databases to spy on love interests, journalists, business associates, and others. <sup>88</sup> For example, the investigation reported officers stalking ex-girlfriends, looking up the addresses of crushes, and in one case, running searches on a journalist who wrote a series of stories critical of the department. ALPR databases could easily be put to similar use. <sup>89</sup> Police departments exacerbate this problem when they fail to implement access and monitoring safeguards to ensure that ALPR data is only accessed on a “need to know” basis, and that access is appropriately logged and monitored to protect against misuse. Instead, some departments automatically install ALPR software on every computer assigned to staff, even when their position does not require access to this kind of information. <sup>90</sup> There is a further lack of transparency in many jurisdictions where vendor contracts prohibit police departments from disclosing their use of surveillance systems to the public. <sup>91</sup>
- **Disparate impact concerns:** ALPRs can also be deployed to target communities of color or other vulnerable populations. The NYPD has used license plate readers as part of its widespread surveillance of Muslim communities in the New York and New Jersey area. <sup>92</sup> And an investigation of license plate readers in Oakland, California, found that they were located predominantly in Black and Latino neighborhoods, despite the fact that automobile crimes and offenses predominantly occurred elsewhere. <sup>93</sup> Even the placement of ALPRs in “high crime” neighborhoods will likely reflect a history of biased and selective enforcement that has already led to the over-policing of communities of color. The guise of neutral surveillance will only reinforce these practices and maintain the attendant potential for deadly police encounters.

Some police departments also incorporate ALPR data into gang databases, which allows officers to track vehicles associated with suspected gang members. <sup>94</sup> These gang databases are notoriously unreliable, as they rely on vague and often contradictory criteria for inclusion. <sup>95</sup> Gang databases, which contain tens of thousands of names, are almost overwhelmingly comprised of individuals of color, and people frequently have no opportunity to challenge their inclusion. <sup>96</sup> The LAPD suspended use of California’s statewide gang database after announcing audits and investigations in response to allegations that police falsified records and listed innocent people as gang members. <sup>97</sup> Meanwhile, an audit by Chicago’s Office of Inspector General found that the city’s gang database contained incomplete and conflicting data, with some entries raising serious concerns about how officers “perceive and treat the people with whom they interact.” <sup>98</sup>

In the wake of nationwide protests that followed the police killings of George Floyd and Breonna Taylor, public attention has increasingly focused on the ongoing instances of police brutality and racial bias in policing. However, there is a risk that police departments and legislators may incorrectly propose surveillance as a neutral alternative. Surveillance that disproportionately targets communities of color carries a distinct and cognizable equal protection harm: branding them with a badge of inferiority. As one appellate court wrote, “Our nation’s history teaches the uncomfortable lesson that those not on discrimination’s receiving end can all too easily gloss over the ‘badge of inferiority’ inflicted by unequal treatment itself. Closing our eyes to the real and ascertainable harms of discrimination inevitably leads to morning-after regret.” <sup>99</sup>

- **Impact on protected First Amendment rights:** Law enforcement agencies have a history of misusing license plate surveillance to monitor First Amendment–protected activity. During the 2008 presidential election, the

Virginia State Police recorded the license plate numbers of attendees at political rallies for Barack Obama and Sarah Palin — and subsequently at President Obama's inauguration — and kept the data for more than three years until it was purged following an opinion from the Virginia Attorney General warning that ongoing retention would violate the state's Government Data Collection and Dissemination Practices Act. <sup>100</sup> Similarly, police in Denver spied on anti-logging activists and shared license plate information with the FBI's Joint Terrorism Task Force when the activists held a training on nonviolence. <sup>101</sup>

Such surveillance — whether it involves the locations of multiple cars that appear together in the same place, or of a single car at places like a mosque, synagogue, or rally — has a chilling effect on Americans' First Amendment rights to freedoms of association, religion, and speech. <sup>102</sup> An investigation into an NYPD program that monitored mosque visitors' license plates found that this surveillance “chilled constitutionally protected rights — curtailing religious practice, censoring speech and stunting political organizing.” <sup>103</sup> The International Association of Chiefs of Police has noted that ALPRs can cause people to “become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance.” <sup>104</sup> And there is always the specter of more flagrant abuse, such as putting a political opponent's license plate on a hot list and using it to keep track of that person's whereabouts. <sup>105</sup>

## Recommendations

In light of these concerns, the need for a multifaceted response to the proliferation of ALPR use is overdue. This section contains a number of recommendations for policymakers, law enforcement agencies, and technology vendors. These are intended as starting points, as the circumstances and implementation of ALPR use reforms will vary by jurisdiction.

- **Adopt retention limits and require warrants for searching historical data:** Plates that are scanned and do not match a hot list alert should be promptly discarded. Using ALPRs to record the movements of all vehicles in a municipality goes far beyond the limited information that is revealed by an isolated capture of license plate data. It also goes beyond what an ordinary person could observe on a public road. Alternatively, if plates are retained, the retention period should be as brief as possible — on the scale of days, not months. These limits could be imposed both by departmental policies and by state law. If municipalities elect to permit retention of license plate data to enable historical searches, such searches should require a warrant supported by probable cause absent emergency situations. ALPR databases collect expansive and sensitive accounts of people's movements regardless of whether they are suspected of criminal activity in a manner that is not available through traditional surveillance. Aside from ceasing to drive altogether, it is exceedingly difficult to avoid this type of surveillance — a condition that is likely to become more pronounced as ALPR technology continues to expand.
- **Institute a two-step scanning process:** When it comes to officers individually running plates, police departments should tailor their scanning processes so that the first pass through a database will not yield protected personal information, instead revealing only registration information and presence on a hot list. Only if that first inquiry reveals a “basis for further police action” should the officer be permitted to proceed to a second step, which would “allow access to the ‘personal information’ of the registered owner, including name, address, social security number, and if available, criminal record.” <sup>106</sup> This simple process can help deter police use of these systems for purposes other than law enforcement.

- **Require verification of hot list data:** Law enforcement agencies should enact policies that require both independent verification of the information yielded from a hot list and real-time updating of hot list data. These steps would help prevent erroneous and potentially dangerous stops based on incorrect or outdated information.
- **Require transparency and invite community input into ALPR use and policies:** The public should have an opportunity to offer input into whether and how ALPRs are deployed. Given that a very small percentage of license plates scanned will actually be connected to a crime, communities may decide that money spent on ALPRs is better spent on other public safety needs, or that the privacy trade-offs are not worthwhile. If ALPRs are purchased, mechanisms must be in place to solicit feedback from interested community members on the policies governing their use. This public consultation process should also inform the types of crimes that merit inclusion on an ALPR hot list. Draft and final policies should be easily available to the public and must include the results of ongoing audits to detect and deter misuse of the system. ALPRs should not be deployed absent clear and enforceable use policies. Except in emergency circumstances, historical ALPR searches should not be conducted absent a warrant supported by probable cause.
- **Maintain audit logs:** Law enforcement use of ALPR data should be logged and stored in a format that permits auditing. First, a log should maintain details about automated ALPR alerts, including the reason for the alert, whether any information was automatically shared with other agencies, and the outcome of the alert. Second, logs should track every time an officer seeks to access historical ALPR data as part of an investigation. This log should specify the officer and the crime being investigated and require evidence that a warrant has been obtained or specification of the exigent circumstances that mandate quicker access. If this functionality is not available through vendor platforms, law enforcement should establish internal access controls to ensure the same outcome.

Separately, each police department should establish a log that tracks and catalogs all the ways they receive, store, and share ALPR data. This includes the license plate reads collected by their own devices, as well as those provided by other law enforcement agencies, by private vendors, and voluntarily by businesses and individuals. Many vendor platforms provide automated methods for tracking and updating authorized data flows, but each department should appoint an appropriate office to lead their efforts to track and maintain this log. When a department elects to share ALPR data with another law enforcement agency, the parties should enter into data sharing arrangements ensuring that policies regarding access control and retention are at least as strict as those of the originating agency. The receiving agency should also commit to entering into similar data sharing agreements for any downstream data sharing. Without adequate steps to protect downstream data sharing, even the most rigid policies will be insufficient once data is shared with a department that does not maintain the same level of protection.

- **Conduct audits for disparate impact:** Law enforcement use of ALPRs should be periodically audited in order to protect against disparate impact on historically marginalized communities and constitutionally protected activities. These audits should evaluate the times and locations where ALPRs are used to ensure that they are not being used to disproportionately target particular communities or constitutionally protected activities such as protests. To facilitate this process, law enforcement agencies must keep records that detail the locations where ALPRs are deployed and the areas where historical searches are being run. Audits should also assess the types of investigations that merit a vehicle's inclusion on a hot list to ensure that low-level offenses are not effectively being used to target vulnerable communities. Audits should evaluate the extent to which ALPR data is used with other surveillance technologies — such as predictive policing algorithms or inclusion in gang data-

bases — in a manner that could disproportionately harm historically marginalized groups or constitutionally protected activity.

- **Conduct audits to ensure effective safeguards:** Every ALPR policy should include regular audits to evaluate safeguard effectiveness. These audits should ensure that ALPR data is only available to employees with a need to access the data, that their access is promptly terminated when no longer necessary, and that ALPR searches are appropriately limited to specific law enforcement investigations. Ongoing oversight of the use of ALPR data within law enforcement agencies is an essential safeguard to detect and prevent officers' misuse of the system.

---

## Endnotes

<sup>1</sup> See Megan Brennan, "83% of U.S. Adults Drive Frequently; Fewer Enjoy It a Lot," *Gallup*, July 9, 2018, <https://news.gallup.com/poll/236813/adults-drive-frequently-fewer-enjoy-lot.aspx>.

<sup>2</sup> The focus of this report is law enforcement use of ALPR. Although there is an important discussion and analysis to be had regarding non-law enforcement applications, such as ALPR use to help institute congestion pricing or to automate toll collection, they are outside the scope of this report.

<sup>3</sup> See, e.g., Katie Schoolov, "As Protests over the Killing of George Floyd Continue, Here's How Police Use Powerful Surveillance Tech to Track Them," *CNBC*, June 18, 2020, <https://www.cnn.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protest-ors.html>; Benjamin Wofford, "The Genius of Protesting in Car Caravans," *Washingtonian*, June 1, 2020, <https://www.washingtonian.com/2020/06/01/the-genius-of-protesting-in-car-caravans/>; Caroline Haskins and Ryan Mac, "Here Are the Minneapolis Police's Tools to Identify Protesters," *BuzzFeed News*, May 29, 2020, <https://www.buzzfeednews.com/article/carolinehaskins1/george-floyd-protests-surveillance-technology>; and Catherine E. Shoichet, "They Can't March in the Streets. So They're Protesting in Their Cars Instead," *CNN*, April 14, 2020, <https://www.cnn.com/2020/04/14/us/coronavirus-car-protests/index.html>.

<sup>4</sup> See Haixia Wang, "41 Percent of Americans Say First Trip Will Be by Car within 100 Miles: Skift Research Travel Tracker," *Skift*, May 1, 2020, <https://skift.com/2020/05/01/41-percent-of-americans-say-first-trip-will-be-by-car-within-100-miles-skift-research-travel-tracker>.

<sup>5</sup> Prashant Gopal and Brian K. Sullivan, "Rhode Island Police to Hunt Down New Yorkers Seeking Refuge," *Bloomberg*, March 27, 2020, <https://www.bloomberg.com/news/articles/2020-03-27/rhode-island-police-to-hunt-down-new-yorkers-seeking-refuge>.

<sup>6</sup> Catherine Crump, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, American Civil Liberties Union, New York, NY, July 2013, 4, <https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf>; see also Dustin Slaughter, "Philly Police Admit They Disguised a Spy Truck as a Google Streetview Car," *Vice*, May 12, 2016, [https://www.vice.com/en\\_us/article/kb77dm/philly-police-admit-they-disguised-a-spy-truck-as-a-google-streetview-car](https://www.vice.com/en_us/article/kb77dm/philly-police-admit-they-disguised-a-spy-truck-as-a-google-streetview-car); Sam Biddle, "Hacked Border Surveillance Firm Wants to Profile Drivers, Passengers, and Their 'Likely Trip Purpose' in New York City," *Intercept*, July 9, 2019, <https://theintercept.com/2019/07/09/surveillance-perceptics-new-york-city-drivers>; and Lily Hay Newman, "New Traffic-Enforcement Tech Peers into Your Car and Counts Passengers," *Slate*, April 28, 2015, [http://www.slate.com/blogs/future\\_tense/2015/04/28/automated\\_vehicle\\_occupancy\\_detection\\_looks\\_in\\_cars\\_counts\\_passengers\\_records.html](http://www.slate.com/blogs/future_tense/2015/04/28/automated_vehicle_occupancy_detection_looks_in_cars_counts_passengers_records.html).

<sup>7</sup> See, e.g., Crump, *You Are Being Tracked*, 5; International Association of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, Alexandria, VA, September 2009, 2, 24–26, <https://web.archive.org/web/20131024095529/http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87>; and *New York v. Davila*, 901 N.Y.S.2d 787, 789 (2010) (describing use of a hot list).

<sup>8</sup> See, e.g., "National Crime Information Center (NCIC)," Federal Bureau of Investigation, Washington, DC, accessed August 26, 2020, <https://www.fbi.gov/services/cjis/ncic> (showing that NCIC database includes 21 files, including a Gang File and an Immigration Violator File); see also David J. Roberts and Meghann Casanova, *Automated License Plate Recognition (ALRP) Systems: Policy and Operational Guidance for Law Enforcement*, International Association of Chiefs of Police, Alexandria, VA, September 2012, 6, 22, <https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf>.

<sup>9</sup> Roberts and Casanova, *Automated License Plate Recognition Systems*, 10.

<sup>10</sup> Roberts and Casanova, *Automated License Plate Recognition Systems*, 8–9.

**11** Crump, *You Are Being Tracked*, 5–6; Dave Maass and Beryl Lipton, “Data Driven: What Is ALPR?” Electronic Frontier Foundation, San Francisco, CA, November 15, 2018, <https://www.eff.org/pages/what-alpr>.

**12** Eric Markowitz, “Pay This Fee, or Go to Jail: How License Plate Scanner Vigilant Solutions Makes [sic] Money in Texas,” *International Business Times*, February 3, 2016, <http://www.ibtimes.com/pay-fee-or-go-jail-how-license-plate-scanner-vigilant-solutions-makes-money-texas-2290835>.

**13** Markowitz, “Pay This Fee, or Go to Jail.”

**14** See Tanvi Misra, “Who’s Tracking Your License Plate?” Bloomberg CityLab, December 6, 2018, <https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904>.

**15** Brian A. Reeves, *Local Police Departments, 2013: Equipment and Technology*, Bureau of Justice Statistics, U.S. Department of Justice, Washington, DC, July 2015, 4, <https://www.bjs.gov/content/pub/pdf/lpd13et.pdf>.

**16** Reeves, *Local Police Departments*, 4.

**17** See, e.g., Dave Maass and Beryl Lipton, “Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers,” Electronic Frontier Foundation, San Francisco, CA, November 15, 2018, <https://www.eff.org/pages/automated-license-plate-reader-dataset> (finding that between 2016 and 2017, the Los Angeles County Sheriff’s Department scanned 234.36 million license plates with a 0.22 percent hit rate, the San Bernardino County Sheriff’s Department scanned 162.69 million license plates with a 0.06 percent hit rate, and the Sacramento Police Department scanned 116.23 million license plates with a 0.1 percent hit rate).

**18** Auditor of the State of California, *Automated License Plate Readers: To Better Protect Individuals’ Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects*, Sacramento, CA, February 2020, 12, <http://auditor.ca.gov/pdfs/reports/2019-118.pdf>.

**19** See Cal. Civ. Code § 1798.29; Neb. Rev. Stat. § 60–3206; Auditor of the State of California, *Automated License Plate Readers*, 2 (finding that the LAPD “has not developed an ALPR policy at all”).

**20** See Vasudha Talla, “Documents Reveal ICE Using Driver Location Data from Local Police for Deportations,” American Civil Liberties Union, New York, NY, March 13, 2019, <https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data>.

**21** See “Electronic Toll Collections: Easy System Integration for Vehicle Recognition,” Perceptics, Farragut, TN, accessed August 26, 2020, <https://www.perceptics.com/markets/electronic-toll-collection/>; Alexis Rivas, “Automatic License Plate Scanners Get Green Light for Pollution Research in San Diego,” NBC San Diego, November 22, 2019, <https://www.nbcsandiego.com/news/local/automatic-license-plate-scanners-approved-for-pollution-emissions-research-san-diego-barrio-logan-national-city/2178630/>; “Solutions,” Digital Recognition Network, Fort Worth, TX, accessed August 26, 2020, <https://drndata.com/solutions>; and Sam Dean, “Neighbors Are Using These Smart Cameras to Track Strangers’ Cars — and Yours,” *Los Angeles Times*, September 13, 2019, <https://www.latimes.com/business/story/2019-09-12/flock-safety-license-plate-readers-los-angeles>.

**22** Dean, “Neighbors Are Using These Smart Cameras to Track Strangers’ Cars.”

**23** State law may provide additional protections that go further than the guarantees of the Fourth Amendment. See, e.g., Electronic Communications Privacy Act, Cal. Penal Code § 1546.

**24** *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967)).

**25** See *Olmstead v. United States*, 277 U.S. 438, 464–66 (1928).

**26** *Katz v. United States*, 389 U.S. 347, 351 (1967).

**27** See *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 361).

**28** *Carpenter*, 138 S. Ct. at 2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886); and *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

**29** *California v. Carney*, 471 U.S. 386, 392 (1985); see also *New York v. Class*, 475 U.S. 106, 113 (1986) (“Automobiles are justifiably the subject of pervasive regulation by the State. Every operator of a motor vehicle must expect that the State, in enforcing its regulations, will intrude to some extent upon that operator’s privacy.”).

**30** See *U.S. v. Knotts*, 460 U.S. 276, 281 (1983); see also *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion); *Town of Woodworth*, 132 So.3d 422 (La. App. 2013); *State v. Davis*, 239 P.3d 1002 (Ore. App. 2010); *State v. Myrick*, 659 A.2d 976; *Davila*, 901 N.Y.S.2d 787; *U.S. v. Diaz-Castaneda*, 494 F.3d 1146 (9th Cir. 2007); *U.S. v. Ellison*, 462 F.3d 557 (6th Cir. 2006); *Olabisiomotosho v. City of Houston*, 185 F.3d 521, 529 (5th Cir. 1999); *United States v. Walraven*, 892 F.2d 972, 974 (10th Cir. 1989); and *United States v. Matthews*, 615 F.2d 1279 (10th Cir. 1980).

**31** *Delaware v. Prouse*, 400 U.S. 648, 662 (1979).

**32** See *Knotts*, 460 U.S. at 283–84.

**33** *Carpenter*, 138 S. Ct. at 2214.

**34** *Kyllo v. United States*, 533 U.S. 27, 35 (2001).

**35** *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Carpenter*, 138 S. Ct. 2206.

**36** *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

**37** *Carpenter*, 138 S. Ct. at 2223.

**38** *Carpenter*, 138 S. Ct. at 2223.

**39** *Carpenter*, 138 S. Ct. at 2218.

**40** *Carpenter*, 138 S. Ct. at 2216.

**41** *Carpenter*, 138 S. Ct. at 2216.

**42** See, e.g., Auditor of the State of California, *Automated License Plate Readers*, 1 (finding that “99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a hot list when the image was made”).

**43** *Carpenter*, 138 S. Ct. at 2210.

**44** *Carpenter*, 138 S. Ct. at 2218–19 (quoting *Kyllo*, 533 U.S. at 36).

**45** *Carpenter*, 138 S. Ct. at 2219–20.

**46** See *United States v. Miller*, 425 U.S. 435, 443 (1976) (“The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed”).

**47** *Carpenter*, 138 S. Ct. at 2220.

**48** *Carpenter*, 138 S. Ct. at 2210.

**49** See Department of Homeland Security, “Privacy Impact Assessment for CBP License Plate Reader Technology,” Washington, DC, July 6, 2020, 8, <https://www.dhs.gov/publication/dhscbppia-049-cbp-license-plate-reader-technology> (“The only way to opt out of such surveillance is to avoid the impacted area, which may pose significant hardships and be generally unrealistic”).

**50** *United States v. Yang*, No. 18–10341, 2020 WL 2110973, at \*6–7 (9th Cir. May 4, 2020), <https://cdn.ca9.uscourts.gov/datastore/opinions/2020/05/04/18-10341.pdf>.

**51** *Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020), <https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf?ts=1587124946>.

**52** *McCarthy*, 484 Mass. at 495.

**53** *McCarthy*, 484 Mass. at 502.

**54** *McCarthy*, 484 Mass. at 506.

**55** *McCarthy*, 484 Mass. at 508–9.

**56** See *Carpenter*, 138 S. Ct. at 2210 (“At any rate, the rule the Court adopts ‘must take account of more sophisticated systems that are already in use or in development,’ . . . and the accuracy of CSLI is rapidly approaching GPS-level precision.” (quoting *Kyllo*, 533 U.S. at 36)).

**57** See Petition for Appeal, *Neal v. Fairfax County Police Department*, Case No. CL-2015–5908, 295 Va. 334 (August 29, 2019), <https://rrbmdk.egnyte.com/dl/gCZYOWOzfH>.

**58** Government Data Collection and Dissemination Practices Act, VA Code Ann. § 2.2–3800(C)(7).

**59** Petition for Appeal, *Neal v. Fairfax County Police Department*, 4.

**60** *Kansas v. Glover*, 140 S. Ct. 1183 (2020).

**61** See, e.g., *Hernandez-Lopez v. State*, 319 Ga. App. 662 (2013) (holding that an ALPR alert indicating that a car’s registered owner had an outstanding warrant gave officers reasonable suspicion to justify a traffic stop); see also *Hill v. State*, 321 Ga. App. 817 (2013) (holding that an ALPR alert from a device mounted on a police cruiser gave an officer reasonable suspicion to justify a traffic stop); and *Traft v. Commonwealth*, 539 S.W.3d 647 (Ky. 2018) (holding that an ALPR alert indicating an active bench warrant gave an officer reasonable suspicion to justify a traffic stop).

**62** *Green v. City and County of San Francisco*, 751 F.3d 1039, 1045 (9th Cir. 2014) (ruling that “an unconfirmed hit on the ALPR does not, alone, form the reasonable suspicion necessary to support an investigatory detention”).

**63** *Green*, 751 F.3d 1039 at 1041.

**64** *Green*, 751 F.3d 1039 at 1046.

**65** *Green*, 751 F.3d 1039 at 1042.

**66** *Green*, 751 F.3d 1039 at 1043.

**67** “Automated License Plate Readers: State Statutes,” National Conference of State Legislatures, Washington, DC, updated June 23, 2020, <https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx>.

**68** See, e.g., Ark. Code Ann. §§ 12–12–1803 (prohibiting use of ALPRs by individuals, partnerships, corporations, associations, or state agencies, and limits use by law enforcement); Neb. Rev. Stat. §§ 60–3206 (requiring any state agency using ALPRs to adopt and post a privacy policy); Mont. Code Ann. §§ 46–5–118 (establishing a ninety-day limit on the retention of license plate data collected by ALPRs); 23 Vt. Stat. Ann. §§ 1607–07 (“Deployment of ALPR equipment by Vermont law enforcement agencies is intended to provide access to law enforcement reports of wanted or stolen vehicles and wanted persons and to further other legitimate law enforcement purposes.”); and Md. Public Safety Code § 3–509(b)(1)(2)(c)(2)(ii) (establishing mandatory audits of ALPR systems).

**69** See generally, *Davila*, 901 N.Y.S.2d 787; see also Jason Potts, “Research in Brief: Assessing the Effectiveness of Automatic License Plate Readers,” *Police Chief* March 2018, 14, <https://www.theiacp.org/sites/default/files/2018-08/March%202018%20RIB.pdf>.

**70** Tim Cushing, “Deputies Sued after False ALPR Hit Leads to Guns-Out Traffic Stop of California Privacy Activist,” *TechDirt* (Floor64 blog), February 20, 2019, <https://www.techdirt.com/articles/20190217/08240241618/deputies-sued-after-false-alpr-hit-leads-to-guns-out-traffic-stop-california-privacy-activist.shtml>; and Cyrus Farivar, “Due to License Plate Reader Error, Cop Approaches Innocent Man, Weapon in Hand” *Ars Technica*, April 23, 2014, <http://arstechnica.com/tech-policy/2014/04/due-to-license-plate-reader-error-cop-approaches-innocent-man-weapon-in-hand>.

**71** Jessica Porter, “Aurora Police Detain Black Family after Mistaking Their Vehicle as Stolen,” ABC7 Denver, August 3, 2020, <https://www.thedenverchannel.com/news/local-news/aurora-police-detain-black-family-after-mistaking-their-vehicle-as-stolen>.

**72** See Lisa Fernandez, “Privacy Advocate Sues CoCo Sheriff’s Deputies after License Plate Reader Targets His Car Stolen,” KTVU Fox 2, February 19, 2019, <https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen>.

**73** Jonathan Dienst et al., “Suspect in NY Hanukkah Stabbings Researched Hitler, Had 2 Knives in Car: Official,” NBC4 New York, December 30, 2019, <https://www.nbcnewyork.com/news/local/what-we-know-about-monsey-stabbing-suspect/2252284/>; Carly Moore, “License Plate Readers Used in Finding Missing Tennessee Girl,” KKCO NBC11 News, August 19, 2016, <http://www.nbc11news.com/content/news/390756761.html>; and Matt Pierce, “How Technology Helped Crack the Kansas City Highway Shooter Case,” *Los Angeles Times*, April 20, 2014, <http://www.latimes.com/nation/nationnow/la-na-nn-kansas-city-highway-shooter-20140419-story.html>.

**74** See, e.g., Maass and Lipton, “Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns”; see also Crump, *You Are Being Tracked*, 13–15 (noting that “only 0.2 percent of reads [in Maryland] were associated with any crime, wrongdoing, minor registration problem, or even suspicion of a problem,” and 0.05 percent of plate reads by the Minnesota State Patrol led to citations or arrests).

**75** Auditor of the State of California, *Automated License Plate Readers*, 1.

**76** See, e.g., Crump, *You Are Being Tracked*, 8–9 (noting that a 2012 survey of 40 police departments found that 5 percent did not retain ALPR reads; 18 percent retained data for either 30 days or less or for between two and six months; and 13 percent retained ALPR reads indefinitely); Seattle Police Department, *2018 Surveillance Impact Report: Automated License Plate Recognition (ALPR) (Patrol)*, Seattle Information Technology, Seattle, WA, January 31, 2019, 21, [http://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20\(Patrol\)%20-%20Final%20SIR.pdf](http://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20(Patrol)%20-%20Final%20SIR.pdf) (noting that data is retained for 90 days); San Francisco Police Department, “Automated License Plate Recognition Vehicles,” Department Bulletin, San Francisco, CA, September 22, 2010, [https://cdn.muckrock.com/foia\\_files/2019/02/08/ALPR20DB20DGO20POLICIES.pdf](https://cdn.muckrock.com/foia_files/2019/02/08/ALPR20DB20DGO20POLICIES.pdf) (noting that plate scan information is retained for two years); Los Angeles County Sheriff’s Department, “Automated License Plate Recognition (ALPR) Privacy Policy,” Los Angeles, CA, accessed August 26, 2020, <https://web.archive.org/web/20190711152351/http://shq.lasdnews.net/content/uoa/EPC/ALPRPrivacyPolicy.pdf> (noting that plate scan information is retained for two years); and Shawn Musgrave, “Under Current Policy, Boston Police Can Keep Scanned License Plate Data Indefinitely,” *Muckrock*, October 1, 2012, <https://www.muckrock.com/news/archives/2012/oct/01/under-current-policy-boston-police-can-keep-scanned>.

**77** See Department of Homeland Security, “Privacy Impact Assessment for CBP License Plate Reader Technology,” 10 (“[A]LPR data from third party sources may, in the aggregate, reveal information about an individual’s travel over time, or provide details about an individual’s private life, leading to privacy concerns or implicating constitutionally-protected freedoms.”), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp049a-cbplprtechnology-july2020.pdf>.

**78** Auditor of the State of California, *Automated License Plate Readers*, 18.

**79** See Ali Winston, “License-Plate Readers Let Police Collect Millions of Records on Drivers,” *Reveal News* (Center for Investigative Reporting, Berkeley, CA), June 26, 2013, <https://www.revealnews.org/article-legacy/license-plate-readers-let-police-collect-millions-of-records-on-drivers>.

**80** See Neb. Rev. Stat. § 60–3206.

**81** Auditor of the State of California, *Automated License Plate Readers*, 26.

**82** Department of Homeland Security, “Privacy Impact Assessment for CBP License Plate Reader Technology,” 6.

**83** Jesse Marx, “Police Used Smart Streetlight Footage to Investigate Protesters,” *Voice of San Diego*, June 29, 2020, <https://www.voiceof-sandiego.org/topics/government/police-used-smart-streetlight-footage-to-investigate-protesters/>.

**84** See, e.g., “Privacy Policy for Flock Safety,” Flock Safety Group, Inc. (website), Atlanta, GA, updated February 22, 2017, <https://www.flock-safety.com/legal/privacy-policy> (“We may also access, use, preserve and/or disclose your personal information or Recordings to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if we have a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce our Terms of Service, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law.”).

**85** Rocco Parascandola and Tina Moore, “NYPD Unveils New \$40 Million Super Computer System that Uses Data from Network of Cameras, License Plate Readers and Crime Reports,” *NY Daily News*, August 8, 2012, <https://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135>; see also “A Conversation with Jessica Tisch ’08: Revolutionizing Police Tech with the NYPD,” *Harvard Law Today*, July 17, 2019, <https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08> (claiming that the NYPD has access to 20,000 CCTV cameras).

**86** Carol Robinson, “Birmingham Police Will Fight Crime with All-Seeing Live Technology,” *AL.com*, May 28, 2019, <https://www.al.com/news/birmingham/2019/05/birmingham-police-will-fight-crime-with-all-seeing-live-technology.html>.

**87** See, e.g., Shawn Musgrave, “Massachusetts Police Lack Policies for License Plate Scanners,” *Muckrock*, April 10, 2013, <https://www.muckrock.com/news/archives/2013/apr/10/license-plate-scanners-use-across-massachusetts/>.

**88** Sadie Gurman, “AP: Across US, Police Officers Abuse Confidential Databases,” Associated Press, September 27, 2016, <https://apnews.com/699236946e3140659ff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases>.

**89** Gurman, “Police Officers Abuse Confidential Databases.”

**90** See, e.g., Auditor of the State of California, *Automated License Plate Readers*, 33.

**91** See, e.g., Cyrus Farivar, “FBI Really Doesn’t Want Anyone to Know About ‘Stingray’ Use by Local Cops,” *Ars Technica*, February 10, 2015, <https://arstechnica.com/tech-policy/2015/02/fbi-really-doesnt-want-anyone-to-know-about-stingray-use-by-local-cops/>.

**92** Adam Goldman and Matt Apuzzo, “NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance,” *Huffington Post*, February 25, 2012, [http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over\\_n\\_1298997.html](http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html); see also *Hassan v. City of New York*, 804 F.3d 277, 285–87 (3d Cir. 2015) (listing factual allegations by plaintiffs alleging extensive, targeted surveillance of Muslim community); Diala Shamas and Nermeen Arastu, *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, Muslim American Civil Liberties Coalition, Creating Law Enforcement Accountability and Responsibility, and Asian American Legal Defense and Education Fund, New York, NY, 2013, 14, <https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf>.

**93** Dave Maass and Jeremy Gillula, *What You Can Learn from Oakland’s Raw ALPR Data*, Electronic Frontier Foundation, San Francisco, CA, January 21, 2015, <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.

**94** See, e.g., City of Chicago Office of Inspector General, *Review of the Chicago Police Department’s “Gang Database,”* Chicago, IL, April 2019, <https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf>.

**95** See, e.g., Anita Chabria, “A Routine Police Stop Landed Him on California’s Gang Database. Is It Racial Profiling?,” *Los Angeles Times*, May 9, 2019, <https://www.latimes.com/politics/la-pol-ca-california-gang-database-calgang-criminal-justice-reform-20190509-story.html>.

**96** See Alice Speri, “New York Gang Database Expanded by 70 Percent Under Mayor Bill de Blasio,” *Intercept*, June 11, 2018, <https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio/>.

**97** Kristina Bravo, “LAPD Suspends Use of CalGang Database Months after Announcing Probe of Officers Accused of Falsifying Information,” *KTLA Los Angeles*, January 20, 2020, <https://ktla.com/news/local-news/lapd-suspends-use-of-calgang-database-months-after-announcing-probe-of-officers-accused-of-falsifying-information/>.

**98** City of Chicago Office of Inspector General, *Review of the Chicago Police Department’s “Gang Database,”* 2, 6.

**99** *Hassan*, 804 F.3d at 291.

**100** Mark Bowes, “Police Recorded License Plates at Obama Inauguration,” *Richmond Times-Dispatch*, August 18, 2013, [http://www.times-dispatch.com/news/local/crime/article\\_32678a59-f9e1-5e46-8336-d5f4ba076cb7.html](http://www.times-dispatch.com/news/local/crime/article_32678a59-f9e1-5e46-8336-d5f4ba076cb7.html).

**101** Kirsten Atkins, “Statement — Kirsten Atkins, Target of Illegal Spying,” American Civil Liberties Union, New York, NY, <https://www.aclu.org/statement-kirsten-atkins-target-illegal-spying>.

**102** See, e.g., *United States v. Jones*, 565 U.S. 400, at 416 (“Awareness that the Government may be watching chills associational and expressive freedom.”).

**103** Shamas and Arastu, *Mapping Muslims*, 4.

**104** International Association of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, 13.

**105** See, e.g., Glenn Greenwald, “Government Harassing and Intimidating Bradley Manning Supporters,” *Salon*, November 9, 2010, [http://www.salon.com/2010/11/09/manning\\_2](http://www.salon.com/2010/11/09/manning_2).

**106** *State v. Donis*, 157 N.J. 44, 55 (1998).

2020-2021

**CAL CITIES OFFICERS**

**President**

Cheryl Viegas Walker  
*Mayor, El Centro*

**First Vice President**

Cindy Silva  
*Council Member, Walnut Creek*

**Second Vice President**

Ali Taj  
*Council Member, Artesia*

**Immediate Past President**

John F. Dunbar  
*Mayor, Yountville*

**Executive Director and CEO**

Carolyn M. Coleman

April 9, 2021

The Honorable Anthony Portantino  
Chair, Senate Appropriations Committee  
State Capitol, Room 2206  
Sacramento, CA 95814

**RE: SB 210 (Wiener) Automated License Plate Recognition Systems:  
Use of Data.  
Notice of OPPOSITION (As Amended 03/15/21)**

Dear Senator Portantino,

The League of California Cities (Cal Cities) must respectfully oppose Senate Bill 210. This measure would hinder law enforcement access to valuable crime fighting data captured by Automated License Plate Reader (ALPR) cameras.

Existing law outlines parameters for use, retention, and auditing functions for agencies who utilize ALPR technologies. Many communities have held public meetings to approve this technology in their jurisdictions and, as required, post their use policies prominently on their agency websites. The same governing bodies should retain authority to direct local retention regulations where necessary.

Ultimately, SB 210 would remove local control over systems that community funds have been invested into. If approved, law enforcement agencies would lose many valuable pieces of information that have historically helped find abducted children, murder suspects, kidnappers, and sex criminals.

The misconception that this technology only matches to existing "hot list" data is a harmful fallacy. There is significant administrative work that goes into reviewing license plate data manually as law enforcement agencies work around the clock to solve crimes happening within our communities.

There also appears to be a misconception that the only way to utilize the data is to enter in specific license plate numbers to find matches; that is not at all accurate. Law enforcement personnel are oftentimes tasked with reviewing data and images from nearby incidents to attempt to match suspect vehicle descriptions or partial plate information relating to criminal activity.

Cal Cities supports accountability on the part of law enforcement agencies concerning police technology and policies, as well as related oversight by local governing bodies. However, we do not support policies that restrict law enforcement agencies from utilizing technologies that would otherwise enhance their ability to prevent criminal activity in the communities they serve.

For these reasons, the League opposes SB 210. If you have any questions, please feel free to contact me at (916) 658-8252.



Sincerely,

A handwritten signature in blue ink that reads "Elisa A." with a stylized flourish.

Elisa Arcidiacono  
Legislative Representative

cc: The Honorable Scott Wiener  
Members, Senate Appropriations Committee  
Shaun Naidu, Consultant, Senate Appropriations Committee  
Kirk Feely, Consultant, Senate Republican Caucus









PUBLIC SAFETY RESULTS

# ShotSpotter's Positive Impact on Communities

## ShotSpotter Helps **Save Lives**

**Oakland, CA**

**101**

victims found and aided by police  
when no one called in shooting (2020)

[Read More](#)

**Pittsburgh, PA**

**36%**

reduction in  
homicides year-over-year

[Read More](#)

**Greenville, NC**

**29%**

reduction in  
gun violence injuries in first year

[Read More](#)

**West Palm Beach, FL**

**60% & 65%**

reduction in homicides and other gun  
incidents with injuries YTD

[Read More](#)

**Pittsburgh, PA**

**83**

Gunshot victims found  
with the help of ShotSpotter

[Read More](#)

**Miami, FL**

**35%**

reduction in  
homicides from 2014-2017

[Read More](#)

**Camden, NJ**

**4 min**

reduction in  
GSW victims transport time

[Read More](#)

**Fort Myers, FL**

**25%**

reduction in  
homicides over prior year

[Read More](#)

**Camden County, NJ**

**46%**

decrease in  
homicides by shootings

[Read More](#)



THE UNITED STATES  
CONFERENCE OF MAYORS

**Best Practice Report** showcases how West Palm Beach  
utilizes ShotSpotter to save lives. [Learn more.](#)

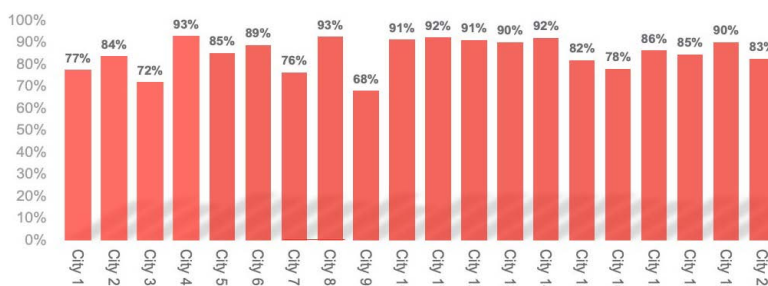
## ShotSpotter Leads Police to **Unreported** Gunfire

**88%** of gunfire incidents were not called into 911

Source: Brookings Institute, Carr and Doleac (2016):

*"The geography, incidence, and underreporting of gun violence: new evidence using ShotSpotter data"*

BROOKINGS INSTITUTE



Unreported gun fire leaves police unaware of majority of gunfire

Source: Local 911 calls for service and ShotSpotter alerts

## ShotSpotter Contributes to **Reductions in Shootings**

Cincinnati, OH

**48%**

shooting reduction in initial coverage area (Avondale)

[Read More](#)

Cincinnati, OH

**46%**

reduction in gun violence in expansion areas

[Read More](#)

St. Louis County, MO

**30%**

reduction in assaults compared to areas without ShotSpotter

[Read More](#)

Newport News, VA

**15%**

reduction in shootings (from 2018-2020)

[Read More](#)

Las Vegas, NV

**26%**

reduction in violent crime during pilot (expanding from 6 to 23 sq mi)

[Read More](#)

Fort Myers, FL

**33%**

decrease in gunfire in 2020

[Read More](#)

Oakland, CA

**66%**

reduction in shootings per square mile

[Read More](#)

Rochester, NY

**40%**

decrease in gunshot incidents

[Read More](#)

Plymouth County, MA

**36%**

decrease in firearm related crime

[Read More](#)

Savannah, GA

**6%**

drop in violent crime in 2021

[Read More](#)

Cleveland, OH

**15%**

reduction in homicides in first year in coverage area

[Read More](#)

Omaha, NE

**55%**

decrease in homicides in 2019

[Read More](#)

## ShotSpotter Alerts Lead Police to **Collect Evidence**, Seize Firearms, Make Arrests, and Solve Cases

50% to **89%**

Improvement in shell casing recovery  
in homicide cases involving a firearm  
with gunshot detection technology

12% to **41%**

Improvement in shell casing recovery  
in robberies involving a firearm with  
gunshot detection technology



*“The most promising aspect of GDT identified through this implementation evaluation is its integration with other investigative tools, such as the ATF’s NIBIN and its firearm eTrace program.”*

JUSTICE EVALUATION JOURNAL

### Pittsburgh, PA

**40%**

of crimes solved from alerts in ShotSpotter  
areas vs 10% in non-coverage areas

[Read More](#)

### Columbus, OH

**133 & 132**

arrests and guns off  
the streets in 16 months

[Read More](#)

### Newport News, VA

**886**

illegal weapons  
seized (2019)

[Read More](#)

### Toledo, OH

**70 & 50**

arrests and firearms  
seized in just over 10 months

[Read More](#)

### Denver, CO

**1,848 & 337**

shell casing connections and  
arrests (2018 - 2021)

[Read More](#)

### Bakersfield, CA

**50 & 37**

arrests and guns  
seized in the first year

[Read More](#)

## Communities Support ShotSpotter

---



**95%** agree ShotSpotter is an effective way to reduce crime

**89%** would recommend ShotSpotter to other neighborhoods



Cincinnati Price Hill ShotSpotter survey evaluation report (2019)

[Read Study](#)

## Everyday ShotSpotter Contributes to Precision Responses and Community Safety

---

### NBC5, Chicago

ShotSpotter alert lead officers to an unresponsive pregnant women with gunshot wound

She was rushed to the hospital in critical condition but later died, police said. The woman was eight months pregnant and doctors were able to deliver her baby, who remains in critical condition.

### 25 NEWS - WEEK Peoria, IL

ShotSpotter alert led officer to save a victim's life

Officers first responded to the scene for a ShotSpotter alert of multiple rounds fired. They gave aid to the victim until he was transported to an area hospital.

### TribLIVE Pittsburgh, PA

Cops responding to Shotspotter alert may have prevented a tragedy

Pittsburgh police officers responding to a Shotspotter alert find gas line ruptured by gunfire; homes evacuated

### WGN9, Chicago

ShotSpotter alert led officer to save a 13-year-old

Two Chicago police officers were first on scene for a ShotSpotter alert and credited with saving a 13-year-old by immediately transporting the boy in their squad car.

### WAVY, Virginia Beach

Man who fired gun in Virginia Beach arrested with help from newly expanded ShotSpotter tech.

Newly expanded ShotSpotter tech caught a suspect with a cache of weapons.

### @ColumbiaPDSC, Twitter

Officer rendered first aid to a serious gunshot victim after responding to ShotSpotter alert

Columbia Police responded to two ShotSpotter alerts. The male victim was found outside of a residence with serious injuries. An officer initially rendered first aid before EMS arrived.

---

### GET IN TOUCH

If you would like to learn more about ShotSpotter, please visit us at [www.shotspotter.com](http://www.shotspotter.com)

All rights reserved. Copyright 2022. The ShotSpotter logo is a registered trademark of ShotSpotter Inc.

## Independent Audit of the ShotSpotter Accuracy

### Executive Summary

According to a report from the Brookings Institution, 88 percent of gunshot incidents go unreported to police. [1] The ShotSpotter system is an acoustic gunshot detection service that detects, locates, and alerts police to gunfire, including those incidents that otherwise would have gone unreported. ShotSpotter enables law enforcement agencies to provide a precise and rapid response to detected incidents. The system uses wireless sensors throughout a coverage area to capture loud, impulsive sounds that may be gunfire. The data are transmitted to a central cloud service that filters out sounds that are clearly not gunshots and provides a location determined by triangulation enabled by sensors. Trained ShotSpotter employees, located across two ShotSpotter Incident Review Centers, listen to the pulses from the sensors that detected the incident audio with playback tools, analyze the visual waveforms to see if they match the typical pattern of gunfire, and either publish the incident as gunfire or dismiss it as non-gunfire. The entire process is intended to take less than 60 seconds from the time of the gunfire to the time law enforcement is alerted to allow for a timely law enforcement response.

ShotSpotter claims that its system is 97% accurate and has a false positive rate—the rate at which gunfire is detected when none occurred—of 0.5%. To determine the accuracy rate for its system, ShotSpotter analyzes information from clients on possible errors, determines whether an error occurred, and catalogs any errors found. In 2021, ShotSpotter commissioned Edgeworth Analytics to conduct an independent audit of the 2019 and 2020 data and analyses that it uses to support its claims. Our audit confirmed that ShotSpotter correctly detected, classified, and published gunfire incidents with 97.59% accuracy. ShotSpotter commissioned Edgeworth Analytics to conduct an additional independent audit of its 2021 data and analysis. Based on our analyses, our audit has yielded five important insights:

- ShotSpotter's accuracy in 2021 was slightly better than 2019 and 2020, and its reports of gunfire when there was none were down in 2021.
- Specifically, ShotSpotter published 146,804, 233,966, and 291,726 gunfire alerts to clients in 2019, 2020, and 2021, respectively. [2] For these years across all clients, our audit confirmed that based on client reports ShotSpotter correctly detected, classified, and published gunfire with 97.69% accuracy, which is slightly higher than the 2019 and 2020 accuracy rate of 97.59%.
- From 2019 to 2021, the ShotSpotter system published alerts of gunfire when clients subsequently indicated that none occurred 0.36% of the time, a decrease from 0.41% in 2019 and 2020.
- Despite substantial variation in the intensity of reporting of potential errors across clients, ShotSpotter's accuracy rate does not appear to be sensitive to differences in clients' propensity to report potential errors.
- No single client exerts a disproportionate effect on ShotSpotter's overall error reporting rate such that the accuracy rate would change significantly.

This report discusses Edgeworth Analytics' approach to auditing ShotSpotter's data and analysis and our additional testing, intended to ensure the validity of our results.

### ShotSpotter Data Sources

Edgeworth Analytics obtained data from ShotSpotter for 2019 to 2021. We discussed the data available and ShotSpotter's error tracking and reporting process with ShotSpotter personnel. Based on our discussions with ShotSpotter personnel, we requested the following data:

- The number of published incidents sent to clients, by location;
- Potential errors identified by clients for investigation and ShotSpotter's conclusions regarding those potential errors; and
- Several samples of "Monthly Scorecards," which are documents sent to clients summarizing the activity detected and the error rates.

ShotSpotter data on published incidents are tracked in ShotSpotter's own systems. However, information on potential errors relies on clients reporting those potential errors to ShotSpotter. When an error report comes in from a client, ShotSpotter creates a ticket and the incident is reviewed. The conclusion of the review may result in one of several outcomes:

- A gunfire incident did not occur, but ShotSpotter published an alert for one—this is referred to as a "false positive";
- A gunfire incident occurred and ShotSpotter detected it, but an alert was not published for gunfire—this is referred to as a "false negative";
- A gunfire incident occurred and was not detected by ShotSpotter—this is referred to as a "missed" incident;
- ShotSpotter failed to accurately identify the location of the gunfire to within 25 meters of the actual location—this is referred to as a "mislocated" incident; or
- The error report was incorrect, or the incident was one that ShotSpotter is not intended to detect, such as gunfire outside the coverage area, indoors, or of a small caliber weapon (i.e., less than 25mm).

We used these data to conduct our audit.

## Edgeworth Analytics Audit Results and Robustness Checks

First, Edgeworth conducted an analysis to ensure that the data were complete and accurate. Specifically, we compared the published incidents and errors detected in the Scorecards to those in the underlying data we received. Our analysis confirmed that the data appeared to be complete and accurate.

Once the data were validated, we reviewed the data and consolidated it into a format suitable for our analysis. This involved combining reporting of events across data sources and reviewing data fields and the possible outcomes of error reports. Using these data, we independently calculated the accuracy across the categories ShotSpotter uses for its reporting. Our analysis confirmed that the accuracy rate across all ShotSpotter clients for 2019, 2020, and 2021 was 97.42%, 97.70%, and 97.82%, respectively. Having audited and validated ShotSpotter's claims, we conducted additional analyses to confirm that these results are robust.

Since accuracy reporting depends on clients informing ShotSpotter of potential errors, we tested whether differences in the intensity of reporting may have unduly influenced the reported accuracy. For example, if a client with a relatively high volume of published gunshot incidents rarely reports potential errors, then the reported accuracy rate may be higher than the actual rate. To test for this issue, we identified the areas where the intensity of reporting potential errors was at or below the 5<sup>th</sup> and 10<sup>th</sup> percentile of client reporting intensity. As shown in Table 1 below, if these clients are removed from the data entirely—an extreme test—then the overall accuracy would decrease by less than 1%. Alternatively, assuming these clients with low reporting intensity all had the reporting intensity of the 5<sup>th</sup> or 10<sup>th</sup> percentile client and that *all* additional reports were erroneous ShotSpotter alerts, the overall accuracy rate would again decrease by less than 1%. [3] These accuracy rates are not statistically significantly different from the overall accuracy rate for all ShotSpotter clients.

Figure 1  
Shotspotter Accuracy Rates  
By Exclusion Threshold  
2019 and 2021

ShotSpotter Alerts [a]	Year [b]	Client Feedback Rate Threshold		
		All Data [c]	>5th Percentile [d]	>10th Percentile [e]
Excluding Selected Accounts	2019	97.39%	97.03%	96.65%
	2020	97.66%	97.26%	96.96%
	2021	97.79%	97.41%	97.26%
All Data	2019	97.42%	97.40%	96.81%
	2020	97.70%	97.68%	97.68%
	2021	97.82%	97.71%	97.42%

Note: Excluded accounts include new, pilot program, and service terminated clients as well as clients from which feedback was not expected.

Source: ShotSpotter.

Download this Report 

## Citations

[1] <https://www.brookings.edu/research/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/>

[2] A small number of ShotSpotter accounts—six in 2019, 12 in 2020, and eight in 2021—were for clients for which feedback was not expected. These included new clients, pilot programs, and clients who terminated their service, as well as some low volume clients. Excluding these accounts, there were 144,739 alerts in 2019, 229,359 alerts in 2020, and 286,438 alerts in 2021 with an accuracy rate of 97.66% on average across the years.

[3] This analysis is conservative as it is only conducted on the more restrictive set of clients excluding those not providing or expected to provide feedback.

# Privacy Audit & Assessment of **ShotSpotter, Inc.'s Gunshot Detection Technology**

PREPARED BY THE POLICING PROJECT AT NYU LAW

**The Policing Project  
at NYU School of Law**  
PolicingProject.org

---

40 Washington Square South  
Suite 302  
New York, NY 10012

---



---

# TABLE OF CONTENTS

<b>I</b>	<b>Executive Summary</b>	<b>04</b>
<b>II</b>	<b>Our Engagement with ShotSpotter Technologies: Assessment, Recommendations, and Report</b>	<b>06</b>
	A. About the Policing Project	06
	B. The Present Engagement	07
<b>III</b>	<b>How ShotSpotter Flex Works</b>	<b>10</b>
<b>IV</b>	<b>Overall Privacy Assessment</b>	<b>14</b>
<b>V</b>	<b>Personal Privacy Enhancing Recommendations</b>	<b>16</b>
	01. <i>Substantially reduce the length of audio stored on each sensor.</i>	16
	02. <i>Do not share precise sensor locations with law enforcement.</i>	17
	03. <i>Deny requests and challenge subpoenas for additional audio.</i>	17
	04. <i>Minimize the duration of audio snippets.</i>	18
	05. <i>Strictly limit which SST personnel have access to sensor audio.</i>	18
	06. <i>Require supervisor approval for any audio download longer than one minute.</i>	18
	07. <i>Create a clear audit trail for every audio download.</i>	19
	08. <i>Conduct periodic review of the audio download audit trail.</i>	19
	09. <i>Revise SST's longstanding privacy policy.</i>	19
	10. <i>Revise client-facing documents to emphasize privacy protections.</i>	19
	11. <i>Whenever possible, avoid placing sensors on particularly sensitive locations.</i>	20
<b>VI</b>	<b>Data Sharing with Third Parties</b>	<b>21</b>
<b>VII</b>	<b>Conclusion</b>	<b>24</b>
<b>VIII</b>	<b>More about the Policing Project</b>	<b>25</b>

# I. EXECUTIVE SUMMARY

ShotSpotter Inc. (“SST”) is a California-based company that operates ShotSpotter Flex (hereafter referred to as “ShotSpotter”), a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in nearly 100 jurisdictions across the country. SST’s primary customers are local law enforcement agencies.

Earlier this year, SST asked the Policing Project at New York University School of Law to conduct a thorough privacy assessment of ShotSpotter. Our engagement with SST focused on identifying the risks ShotSpotter poses to personal privacy and to suggest technological, policy, and procedural changes to address those risks. We agreed to conduct this assessment on the condition that we have complete access to all SST policies, procedures, and personnel related to ShotSpotter,<sup>1</sup> and that we have complete editorial control over our recommendations and report. In our view, SST has been notably open and transparent throughout this process.

Having conducted a thorough review of SST’s current policies and procedures, and as explained in more detail below, we believe that on the whole ShotSpotter presents relatively limited privacy risks. In our analysis, the primary personal privacy concern with ShotSpotter is the possibility that the technology could capture voices of individuals near the sensors, and conceivably could be used for deliberate voice surveillance. Although we believe the risk of this occurring is already relatively low, this report offers a variety of recommendations for how SST can make ShotSpotter even more privacy protective.

As discussed in more detail in this report, our recommendations cover a wide range of issues, chief among them that SST:

1. Substantially reduce the duration of audio stored on ShotSpotter sensors;
2. Commit to denying requests and challenging subpoenas for sensor audio;
3. Commit to not sharing specific sensor location; and
4. Improve internal controls and supervision regarding audio access.

**SST has adopted nearly all of our recommendations verbatim**, with only

---

1. Contractual arrangements prevented SST from providing us with one piece of information. See *infra* Part VI.

slight modifications or qualifications based on how ShotSpotter functions.

Although we were asked to comment on ShotSpotter's personal privacy implications, we conclude our analysis by offering some additional guidance regarding data sharing with third parties. Although we do not see this as a personal privacy issue, we believe this is one area where SST can and should refine its approach. SST has taken these comments seriously and is in the process of thinking through its response.

Throughout this process, SST has consistently demonstrated commendable commitment to modifying its technology to balance its public safety function with protections for individual privacy. The changes we asked SST to make—both to how their technology operates and their internal procedures—were certainly not without cost. SST made a conscious choice to bear these costs. We hope others follow SST's leadership in this regard; indeed, we believe this type of open audit and assessment—whether performed by us or by others—should become the norm for companies selling technologies to governments and policing agencies.

**Indeed, we believe this type of open audit and assessment—whether performed by us or by others—should become the norm for companies selling technologies to governments and policing agencies.**

## II. OUR ENGAGEMENT WITH SHOTSPOTTER

### ABOUT THE POLICING PROJECT

The Policing Project is a non-profit entity at New York University School of Law. Our mission is to partner with communities and police to promote public safety through transparency, equity, and democratic engagement. (More information about our mission is available in Part VIII or at [www.policingproject.org](http://www.policingproject.org).)

One of the Policing Project's core areas of focus is policing technologies. Certain new technologies hold great promise to make policing safer, more effective, and more accountable. But at the same time, we have serious concerns about possible invasions of privacy, inaccuracy, and perpetuation of racial bias. Rather than being "for" or "against" a new technology, we believe the proper approach is to figure out if society can benefit from a particular technology while eliminating or minimizing any harm. In this regard, cost-benefit analysis of policing technologies is both appropriate and essential. The decision to deploy any technology should have democratic approval based on public information about the potential benefits and harms. Democratic legitimacy requires the inclusion in that process of those communities most impacted by the use of the technology.

To that end, we have adopted a range of strategies. In consultation with police and affected communities, we are drafting use policies for a variety of new technologies, including drones, predictive analytics, social media monitoring, and more. We are conducting rigorous social science research into the effectiveness of certain technologies.<sup>2</sup> We are also developing tools that encourage public authorization before policing technologies are acquired or used.

**Rather than being "for" or "against" a new technology, we believe the proper approach is to figure out if society can benefit from a particular technology while eliminating or minimizing any harm.**

One of our strategies is to work directly with certain private companies in the policing technology space to assess their products; offer recommendations as to whether those products pose civil rights or civil liberties concerns; and recommend how those concerns might be mitigated, either through design, use policies, or internal procedures.<sup>3</sup> To this end, we have determined that, when invited to do so by municipalities, law

2. With the generous support of the Laura & John Arnold Foundation, the Policing Project and Professor Jillian Carr of Purdue University Krannert School of Management are conducting a cost-benefits analysis of the St. Louis County Police Department's use of ShotSpotter. This privacy assessment and our research study have from the outset remained entirely independent.

3. Relatedly, Policing Project Faculty Director Barry Friedman sits on the Axon AI and Policing Technology Ethics Board, and the Policing Project staffs the Board. See <http://www.policingproject.org/axon-ethics-board>

---

enforcement agencies, or private vendors, we will conduct an audit and assessment of policing technologies. SST has exercised commendable leadership in opening itself up to this assessment. We hope this becomes the norm for companies selling technologies that pose civil liberties or civil rights concerns, including those involving racial inequities. Such evaluation is essential so that communities can make wise acquisition and regulatory decisions.

Throughout our work, we disclose any conceivable conflicts, particularly when private companies are involved. Since 2018, SST has provided the Policing Project with unrestricted funding (as do other entities) for our policing technology work in general. SST compensated us for our time and travel in conducting this audit and assessment. SST CEO Ralph Clark also sits on our Advisory Board.<sup>4</sup> Note that our Board is *advisory* only with no legal authority or governing powers over the organization. This pre-existing relationship played a large part in initiating this work.

## THE PRESENT ENGAGEMENT

In February 2019, during the course of discussions of adopting ShotSpotter in Toronto, segments of that community raised a number of reservations, including privacy-related concerns.<sup>5</sup> After the Toronto Police Department ultimately decided not to pursue ShotSpotter, SST contacted the Policing Project to discuss how it could address concerns like those raised in Toronto. At that time, as discussed above, we already were developing a model for the audit and assessment of policing technologies. Thus,

we suggested SST engage us to conduct an audit and assessment of ShotSpotter from a privacy perspective.

Before going further, we think it essential to explain that this report is in no way a comment on the concerns raised in Toronto (or any other city). Each community has its unique laws, concerns, and history, and the Policing Project believes that every community should decide for itself what policing technologies are appropriate for their specific needs. This is the essence of front-end accountability, which motivates all our work. Our aim is to provide information to the public that can aid in sound and informed decision-making about policing technologies.

**We hope that for companies selling technologies that pose civil liberties or civil rights concerns, including those involving racial justice, it becomes the norm to have products evaluated in this way.**

In April 2019, SST officially engaged the Policing Project to conduct a thorough privacy assessment of its policies and procedures for ShotSpotter, and to make concrete suggestions as to how SST could address privacy concerns. Because we were

---

4. To view our full advisory board, visit: <http://www.policingproject.org/our-advisory-board>.

5. See, e.g., Jeff Gray, *Toronto police end ShotSpotter project over legal concerns*, THE GLOBE AND MAIL (Feb. 13, 2019), <https://www.theglobeandmail.com/canada/toronto/article-toronto-police-end-shotspotter-project-over-legal-concerns/>.

---

asked to conduct a *privacy*-focused assessment, we focused on what sort of data is captured, aggregated, mined, retained, and shared. We did not analyze other potential benefits or costs of ShotSpotter or any other SST technology. For example, we have not evaluated how well SST's gun detection technology actually works (its rate of false positives or negatives) or the process by which ShotSpotter reports are admitted into evidence at criminal trials. We have not explored or evaluated any other potential civil rights or civil liberties concerns.

**We believe it is essential that private companies in the policing technology space take seriously their obligation to minimize their impact on civil rights and civil liberties.**

Our assessment process began with a thorough document review—both of publicly available information and internal SST materials, such as contracts, training materials, and documents provided to law enforcement customers. We conducted a site visit to SST's Newark, California headquarters, interviewed numerous SST personnel, and observed SST's Incident Review Center in action. We followed up with additional questions and received additional information. We provided SST with a set of recommendations in May, giving SST time to evaluate and respond to our recommendations before the publication of this report.

We have had complete control over the substance of our recommendations and the contents of this report. SST has reviewed it for factual errors only.

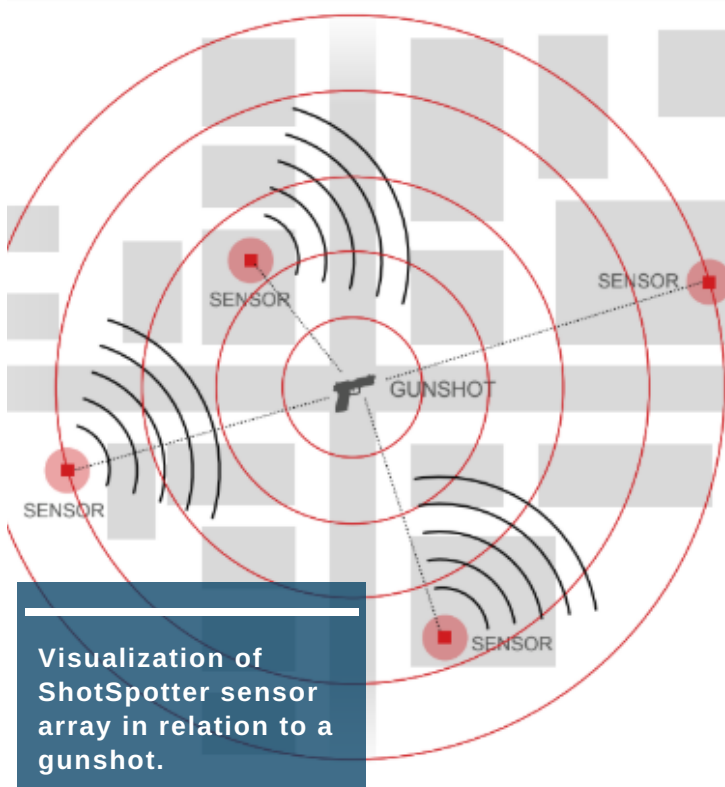
This is our first such engagement. Although we do not think this type of private engagement can or should take the place of community voice or official regulation, we believe it is essential that private companies in the policing technology space take seriously their obligation to minimize their impact on civil rights and civil liberties. We see this type of engagement—whether performed by us or others having the relevant expertise—as an important model for improving the transparency and accountability of policing technologies across the country.



# III. HOW SHOTSPOTTER FLEX WORKS

According to SST, ShotSpotter is a “gunshot detection, location, and forensic analysis” technology. Specifically, ShotSpotter analyzes sound to detect that gunfire has occurred, locate the source of that gunfire, and determine certain characteristics of the gunfire (such as how many shots were fired and the precise timing of those shots).

The technology has two basic components: (1) an array of microphone-equipped sensors spread across the coverage area, and (2) the ShotSpotter Incident Review Center (“IRC”) at SST headquarters in Newark, California.



The process begins with SST working with the customer to determine the desired physical boundaries for ShotSpotter’s gunshot detection technology. Ultimately, the choice of boundaries is one for the customer, considering the needs and resources of the particular community. The larger the coverage area, the greater the cost.

Once the coverage area is set, SST engineers work to determine how many sensors are needed and where they should be placed in order to achieve reliable detection throughout the area. Sensors are equipped with microphones that are similar to a typical smartphone microphone at picking up sound. SST personnel install the sensors on buildings and lampposts typically 20-30 feet above the ground. Sensors are placed this high so as to maximize their range, require lower sensor density, and to minimize street-level audio. The sensor network is then tested to ensure proper operation.

Once operational, these sensors are continuously “listening” and a proprietary AI-enhanced algorithm is constantly analyzing incoming audio. The algorithm reviews the audio for loud “impulsive” sounds—that is, loud sounds that start and end suddenly (similar to a gunshot). In addition to actual gunfire, impulsive sounds

---

that trigger the algorithm can include certain construction noises, helicopters, motorcycles, fireworks, and other similar sounds. Whenever ShotSpotter's algorithm detects an impulsive sound, the algorithm attempts to identify these sounds (e.g., "gunfire," "helicopter," "construction"). Although all audio, including street noise, traffic, or human voice, are inputs to the algorithm, only gunshot-like sounds ("impulsive" sounds) actually trigger the sensor and the next stage of the process.

notifications from customer locations around the world to determine whether the impulsive sounds detected by the ShotSpotter algorithm are actual gunshots.<sup>6</sup> The IRC is notified of the majority, but not all, of the impulsive sounds that trigger three sensors. As the ShotSpotter algorithm has improved over time, SST has determined that its system is sufficiently accurate in identifying particular types of impulsive sounds, such as helicopters or fireworks, so that these



**Technicians in the ShotSpotter Incident Review Center**

When three or more sensors are triggered at the same time—that is, they detect an impulsive sound (such as a gunshot)—the IRC is notified as to the time and location of the event. Requiring three sensors to detect a sound is necessary to determine a precise location. It also means that softer sounds (e.g., a car door) will not trigger a notification of the IRC. There is no human involvement until after the IRC is notified via an encrypted cellular network.

In the IRC, SST personnel constantly review

type of incidents often are not sent to the IRC and are discarded as non-gunfire.

The IRC personnel's individualized review of each notification includes three components related to the captured audio:

- 1). Personnel are provided with the ShotSpotter algorithm's best assessment of the nature of the sound (e.g., "gunshot," "helicopter," "construction," "fireworks"), including a confidence threshold.

---

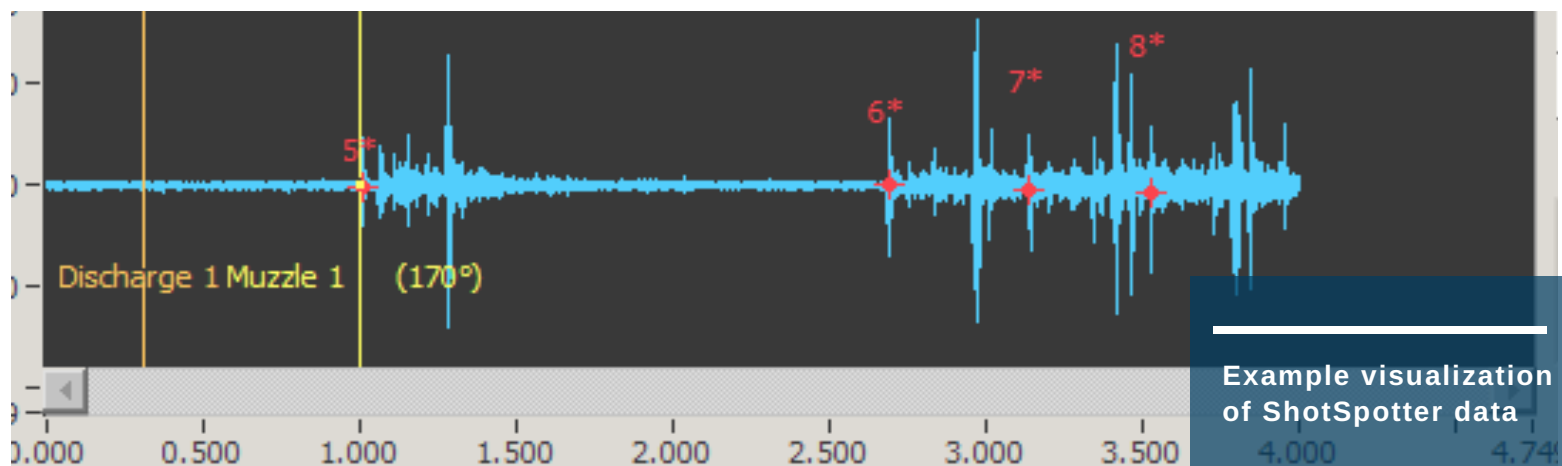
6. IRC personnel work in eight-hour shifts, with two to six specialists and one supervisor per shift. These personnel receive substantial training and testing in this role, though a review of this training or of accuracy rates was outside of the scope of our privacy assessment.

2). Personnel listen to brief audio snippets of the incident from each of the nearby sensors. Snippets include up to one second of audio prior to the incident, the gunshot incident itself, and one second of audio after the incident. The pre- and post-incident audio is provided to help reviewers better assess the nature of the incident itself by giving them a sense of the ambient noise immediately prior to and after the incident. This is the only audio IRC personnel are provided. These audio snippets are retained indefinitely by SST.

3). Personnel also are presented with a visualization of the audio from each of the nearby sensors. The following is a sample visualization, which SST personnel are trained to read:

information and a single audio snippet, to the relevant law enforcement agency via a password-protected application on a mobile phone, in-car laptop, or computer. In addition to the audio snippets, SST provides ShotSpotter customers with detailed information about the location, sequence, and timing of each shot during an incident. According to SST, the typical time from gunshot to alert is less than one minute.

This is the ordinary process in the vast majority of cases. On occasion, however, law enforcement customers contact ShotSpotter about a possible missed gunshot. In such cases, ShotSpotter asks customers to provide their best information about date/time/location of the incident, as well as some proof that the incident occurred (e.g., casings, eyewitness statements).<sup>7</sup>



Based on this acoustic information, as well as other related data (e.g., time of day, location), the IRC reviewer makes a determination as to whether the acoustic event was a gunshot.

If the reviewer finds it was a gunshot, the reviewer sends an alert, including location

With this information in hand, a limited number of authorized employees, either IRC personnel or forensic engineers, begin a review of stored audio from nearby sensors, to determine if any of the sensors detected the gunshot. SST personnel cannot listen to sensor audio in real time. Instead, IRC personnel must begin by reviewing graphic

7. An "ear"-witness—someone who claims they heard a gunshot—is not sufficient to trigger this review process.

---

visualizations of the audio (similar to those pictured above), not by listening to the audio itself. They focus on impulsive events at the relevant location, at the relevant time, and if they locate one, select that portion of the audio to download and listen to. Downloaded audio recordings in these cases have up to two seconds of audio prior to the incident, the incident itself, and up to four seconds after the incident. The pre- and post-incident audio is again provided for a baseline ambient noise level so as to better assess the incident. By listening to the audio from multiple sensors, reviewers can determine whether a gunshot was detected. If so, that snippet is sent to the law enforcement agency.

**A sensor is only accessed in the event that SST is presented with evidence of a missed gunshot and only saved in the event that a missed or mislocated gunshot is detected.**

In order to make this review process possible, each sensor locally stores 72 hours of audio. Sensors constantly overwrite stored audio and replaced it with more recent audio. Therefore, in order to review for a missed gunshot, law enforcement must provide SST with notice of the possible missed gunshot within 72 hours.

Other than the snippets, discussed above, which are stored indefinitely, audio stored on a sensor is only accessed in the event

that SST is presented with evidence of a missed gunshot and only saved in the event that a missed or mislocated gunshot is detected.<sup>8</sup>

Although ShotSpotter acoustic sensors can be integrated into other technologies (such as smart lamp posts), no matter what the physical configuration, only SST personnel have access to ShotSpotter sensors and their stored audio.

---

8. The only other audio that SST retains are limited samples (such as samples of wind or other noise) for research and development purposes—specifically, to train its algorithm to perform more accurately.

# IV. OVERALL PRIVACY ASSESSMENT

SST describes ShotSpotter as a gunshot detection, location, and forensic analysis technology. But some have raised the concern that ShotSpotter might be used as a voice surveillance tool—that is, that it could be used to listen to and record conversations occurring near ShotSpotter sensors. In particular, communities that have been disproportionately impacted by policing, which are most often communities of color, have expressed concern that ShotSpotter might enter a city under the auspices of gunshot detection, but be utilized for targeted voice surveillance in neighborhoods already stricken by gun violence.<sup>9</sup> This concern has been bolstered by a handful of occasions in the past that human voice has been captured by sensors and used in a criminal prosecution.<sup>10</sup>

We wholly agree that from a privacy perspective, it would be of serious concern if ShotSpotter were used for voice surveillance. Voice surveillance could take two forms—persistent surveillance and targeted surveillance. The former might occur if sensors constantly were recording (and SST was listening to and/or retaining)

voice audio and sharing such audio with law enforcement for any purpose. Surveillance also could be “targeted,” *i.e.*, listening in to specific locations or after-the-fact review of sensor audio in search of relevant voice recordings.

Having conducted a thorough review of SST’s policies and procedures, we conclude that the risk of voice surveillance is extremely low in practice. This conclusion is not meant to minimize or dismiss the concerns that others have raised to date. Indeed, it is surely possible that ShotSpotter sensors will, on occasions, capture some intelligible voice audio related to a gunfire incident. Still, based on our understanding of how ShotSpotter operates today, we have little concern that the system will be used for anything approaching voice surveillance.

We reach this conclusion based on our assessment of the variety of safeguards already built in to how ShotSpotter operates, as well as the recommendations SST has agreed to implement at our behest (discussed below). Of particular

---

9. See, e.g., Lyndsay Winkley, *San Diego police to continue using gunshot detection, despite some criticism*, THE SAN DIEGO UNION TRIBUNE (Oct. 7, 2017), <https://www.sandiegouniontribune.com/news/public-safety/sd-me-sdpd-shotspotter-20171005-story.html>; Josh Sanburn, *Shots Fired*, TIME (Sept. 21, 2017), <https://time.com/4951192/shots-fired-shotspotter>; Means Coleman, R. & Brunton, D., *You Might Not Know Her, But You Know Her Brother: Surveillance Technology, Respectability Policing, and the Murder of Janese Talton Jackson*. 18 SOULS: A CRITICAL J. OF BLACK POLITICS, CULTURE, & SOC. 408–20 (Dec. 2016), [https://www.academia.edu/31517733/Souls\\_A\\_Critical\\_Journal\\_of\\_Black\\_Politics\\_Culture\\_and\\_Society\\_You\\_might\\_not\\_know\\_her\\_but\\_you\\_know\\_her\\_brother\\_Surveillance\\_Technology\\_Respectability\\_Policing\\_and\\_the\\_Murder\\_of\\_Janese\\_Talton\\_Jackson](https://www.academia.edu/31517733/Souls_A_Critical_Journal_of_Black_Politics_Culture_and_Society_You_might_not_know_her_but_you_know_her_brother_Surveillance_Technology_Respectability_Policing_and_the_Murder_of_Janese_Talton_Jackson)

10. See, e.g., Alexandra S. Gecas, *Gunfire Game Changer or Big Brother’s Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to ShotSpotter Technology*, 2016 UNIV. ILL. L. REV. 1073, 1088 (“ShotSpotter acknowledged three extremely rare ‘edge cases’ out of three million detected incidents in the last decade where the sensors recorded people shouting in a public street at the location where the sensors detected gunfire.” (internal quotation marks omitted)), <https://illinoislawreview.org/wp-content/uploads/2016/07/Gecas.pdf>.

importance to our conclusion is the fact that although sensors constantly are “listening,” audio is only temporarily stored (formerly 72 hours; soon to be 30 hours), and then a very select amount of audio is retained only if the computer algorithm or human reviewer detects a gunshot. All other audio is routinely purged from SST’s systems.

Moreover, we view as essential the fact that the audio review and retention process is centralized within SST—that is, that neither law enforcement customers nor third parties have access to the raw audio or can determine what audio to download and retain. (Our recommendations address requests and subpoenas for audio.) It should be noted that prior to 2012, police agencies were in control of the audio review and download process locally, but a technology and business model change resulted in SST having centralized control over its sensors and audio through its IRC. Currently, no police department has control over any audio except the snippets provided by SST as part of its alerts.

We do note, however, that although no third parties have access to ShotSpotter stored audio, and ShotSpotter’s review and analysis is centralized, ShotSpotter alerts can trigger a range of responses by law enforcement—from dispatching police officers to the location, to programming CCTV cameras to turn toward the direction of an alert, to factoring into predictive policing software, to reinforcing stereotypes regarding particular neighborhoods. We fully appreciate that the mere fact of additional police response—be it in person or CCTV cameras—is itself a concern to some communities. But this is not unique to ShotSpotter; indeed, this can be the case for citizen-initiated reports of gunshots. The range of possible police responses to ShotSpotter alerts highlights how every technology, no matter how privacy protective, must also be used in ways that are racially just, transparent, and subject to democratic approval.

## V. PERSONAL PRIVACY ENHANCING RECOMMENDATIONS

Although we perceive that ShotSpotter, under current operating procedures, presents a low privacy risk, we nonetheless have a variety of recommendations designed to further minimize the risk that ShotSpotter might inadvertently or deliberately be used for voice surveillance. We provided these recommendations to SST in advance of this report and have incorporated SST's responses below. As evident from these responses, SST has adopted all of our recommendations, with only slight modifications or qualifications based on how ShotSpotter functions.

### **01** Substantially reduce the length of audio stored on each sensor.

At present, in order to allow IRC personnel to search for possible missed gunshots, ShotSpotter sensors locally store 72 hours of recent audio, after which the audio is permanently deleted. As explained above, law enforcement customers can report possible missed shots to SST so long as they have evidence that shots were fired. With a rough location and time, IRC personnel or forensic engineers follow the process described previously to first review graphic visualizations of the audio to determine whether any sensors captured a possible gunshot. If so, audio is downloaded, and if it is determined to be a gunshot, an audio snippet is transmitted to law enforcement.

This review process somewhat increases the possibility that human voice will be captured and reviewed because: (1) the process is initiated by law enforcement, and some might be concerned those agencies are interested in obtaining sensor audio for the purpose of voice surveillance; and (2) IRC reviewers or forensic engineers must manually select and listen to additional audio to determine if there was an undetected gunshot. Arguably then, if SST were to completely eliminate all stored audio, the chance of voice surveillance would be substantially limited. But taking this dramatic step also would deprive SST and its customers of the ability to look back for missed gunshots.

We are informed that the IRC processes approximately three to four "missed or mislocated gunshot" requests per day. Balancing this valuable service against the limited possibility of voice surveillance generally, we do not recommend SST take the dramatic step of eliminating stored audio entirely. Instead, we recommend SST drastically cut back the duration of stored audio. Put another way: SST should delete stored audio in a much shorter time frame than 72 hours.

Our understanding from SST is that most missed gunshots are reported by law enforcement customers within 30 hours. As such, SST can accomplish its goal of searching for missed gunshots while reducing the period of stored audio from 72 hours to 30 hours.

---

By reducing the length of time that SST stores audio, SST will lower the possibility that its technology can be seen as a surveillance device, or that law enforcement even will attempt to use the sensor buffer for investigative purposes other than missed gunshots.

**SST has adopted this recommendation** and has implemented a software update that is currently being pushed out to all of its sensors across the country. This rollout will be complete by early August 2019. Customers have already been informed of this change in policy.

## 02 Do not share precise sensor locations with law enforcement.

SST works with law enforcement to set ShotSpotter's coverage area. Once the area is set, SST engineers alone determine precise sensor locations necessary in order to ensure even coverage. SST does not provide law enforcement with access to a database or list of precise sensor locations, nor does SST respond to requests for sensor locations from police or the public. SST says it fights subpoenas for requests to have the precise sensor locations. As a general matter, law enforcement has no need to know the precise sensor locations.<sup>11</sup>

We recommend formalizing the practice that law enforcement customers not be given precise sensor locations in SST company policy. By withholding this information, SST minimizes the possibility (or the allure) that law enforcement officers

investigating a particular incident would view ShotSpotter sensors as an investigative tool like CCTV and request audio from a sensor.

**SST has adopted this recommendation** and now clearly states, in both public and client-facing documents, that law enforcement will not have access to precise sensor locations, requests for sensor locations will not be honored, and subpoenas will be resisted in court.

## 03 Deny requests and challenge subpoenas for additional audio.

No matter what internal controls SST places on its technology, and no matter the internal emphasis on privacy and avoiding voice surveillance, there always will remain the possibility that third parties—police, prosecutors, civil litigants, etc.—may request or subpoena extended sensor audio beyond the short snippets provided upon a detected gunshot in an effort to capture voice. No matter how uncommon an occurrence, we believe it prudent to be alert to and prepared for this possibility.

Although a corporate policy to deny requests and challenge legal subpoenas will not necessarily be decisive in court, it should weigh heavily against parties making any such request.

**SST has adopted this recommendation** in both public and client-facing documents, that requests for extended audio will not be honored and subpoenas will be resisted in court.

---

<sup>11</sup> We understand that on occasion a police officer (generally a patrol officer) will accompany SST personnel when SST asks for consent to place a sensor. The officer does not accompany personnel during installation. Although this provides a lone officer with knowledge of the general area of a few sensors, this is not the type of systematic knowledge that concerns us.

---

## 04 Minimize the duration of audio snippets.

Prior to this privacy assessment, in cases of a law enforcement agency requesting research on a possible missed or mislocated gunshot, SST policy was to provide law enforcement personnel with an audio snippet of up to two seconds of audio from immediately before the gunshot, the audio of the gunshot itself, and up to four seconds of audio from immediately after incident. For live-captured incidents, however, SST provided only one second before and one second after.

In the few past instances in which human voice was captured incidentally by ShotSpotter sensors, that voice audio was captured as part of the gunshot audio snippet. In order to minimize the chance of incidentally capturing and transmitting voice audio to law enforcement, we recommend standardizing and minimizing the duration of audio from before and after the gunshot. Specifically, we suggest SST provide at most one second of audio from before and after any incident.

**SST has adopted this recommendation** and has now implemented an automated process where all snippets include only one second of pre- and post-incident audio.

## 05 Strictly limit which SST personnel have access to sensor audio.

Despite efforts to mitigate privacy concerns by avoiding certain locations for sensors and placing them high off the

ground, the possibility will always remain that ShotSpotter sensors will capture voice audio. As such, access to the sensors must be sharply controlled. In addition to ensuring that sensors and the SST cloud are adequately encrypted and protected against external attack, SST must take steps to fortify its internal operations.<sup>12</sup> Our first recommendation on this front is that SST conduct an internal review of which personnel have access to sensor audio and ensure that access is limited only to those personnel who actually need access to perform their work.

**SST has adopted this recommendation** and has already completed its review of personnel with access to sensor audio. As a result of this review, SST has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential.

## 06 Require supervisor approval for any audio download longer than one minute.

In our view, the greatest risk for invasion of personal privacy comes when SST personnel access actual stored sensor audio (as opposed to the audio visualizations typically used to locate gunshot-like events). Although we have no reason to believe that SST personnel abuse this privilege, in order to deter and detect possible misuse, we recommend SST implement a safeguard that requires supervisor approval before an SST employee is permitted to download extended audio. In order to strike a balance between allowing SST personnel to search

---

<sup>12</sup>. It is also key, as noted above, that third parties (customers or not) never are given access to these sensors.

---

quickly for missed gunshots, while still installing a layer of protection, we recommend requiring supervisor approval for audio downloads of longer than one minute per incident.

**SST has adopted this recommendation.**

## **07** Create a clear audit trail for every audio download.

Further, we recommend that for every instance in which an SST employee accesses stored sensor audio, SST ensure there exists a clear audit trail describing what audio was accessed, the SST employee who accessed the audio, the supervisor who approved the download (under Recommendation No. 6, above), the law enforcement agency and officer who made the request, and the evidentiary basis for the request.

**SST has adopted this recommendation.**

## **08** Conduct periodic review of the audio download audit trail.

In addition to creating an audit trail (Recommendation No. 7, above) for when stored sensor audio is accessed, we recommend SST create a regular process by which supervisory personnel review this audit trail. This review should ensure that audio is being accessed only when necessary and according to proper procedures. Such a review also should be on the lookout for any law enforcement agencies that are using the process at a much higher rate, SST personnel who listen

to a significantly longer duration of audio than necessary, or other patterns that may require corrective action.

**SST has adopted this recommendation.**

## **09** Revise SST's longstanding privacy policy.

In addition to making internal changes to its operations, we recommended SST make changes to a number of its public-facing and client-facing documents, to emphasize that ShotSpotter should only be used for gunshot detection, and not voice surveillance, and to document the steps SST has taken to emphasize privacy protections.

SST has long had a privacy policy.<sup>13</sup> Although that policy addressed many relevant privacy issues, with our privacy assessment, we suggested SST make revisions and updates. In particular, we suggested SST revise the policy for clarity and to focus on privacy protections.

**SST has adopted this recommendation.**

The updated policy is available at: <https://www.shotspotter.com/privacy-policy><sup>14</sup>

## **10** Revise client-facing documents to emphasize privacy protections.

SST provides law enforcement customers with a variety of documents that touch on privacy-related issues, such as Best Practices, Strategies & Recommendations and Model Policy Elements. We think it is important that SST provides this type of

---

13. For reference, ShotSpotter's previous privacy policy, dated March 31, 2015, is available at <https://www.shotspotter.com/apps/privacy/>.

14. It is a core tenet of the Policing Project that new policing technologies should be adopted transparently and with public input. Although this is not technically part of our privacy audit, we applaud SST for urging its customers to engage the public in a discussion about the acquisition and use of its products as the first principle of its privacy policy.

---

support. In fact, we think it irresponsible for technology companies to provide surveillance technologies to law enforcement agencies without a draft use policy. We have suggested that SST revise these documents to emphasize many of the same principles outlined in its new privacy policy—specifically, that its technology cannot be used for voice surveillance, that the sensor audio storage cannot be used to obtain “extended” or “additional” audio but only can be used to search for missed gunshots and that subpoenas for audio will be contested.

**SST has adopted this recommendation** and has already made these changes.

## **11** **Whenever possible, avoid placing sensors on particularly sensitive locations.**

Although ShotSpotter is not especially calibrated to record human voice and SST takes measures to avoid this occurrence—for example, by not using particularly sensitive microphones, placing sensors high above the ground, and ensuring that only gunshot-like sounds trigger an IRC notification—there remains the possibility that voice will be captured by a sensor incidentally. Knowing this, we raised with SST a general concern about the location of sensors. Specifically, we raised whether SST could minimize the impact of incidental voice capture (and also allay public concerns) by avoiding placing sensors in locations that present concerns for the surrounding community based on protected First Amendment characteristics, prior experience with policing, or other social vulnerabilities. For example, our conversations with SST included discussions

of public housing campuses, where residents often are already subjected to a great deal of surveillance, and houses of worship, particularly those that have been subject to unlawful government surveillance in the past. Other examples of sensitive locations may include hospitals, healthcare clinics, or schools.

SST explained that an absolute ban on these types of locations simply cannot be implemented without major disruption of ShotSpotter’s coverage and performance. For example, SST explained that there are occasions when it must use certain public buildings, including government-owned housing, in order to maintain the consistency of its detection system. In fact, many jurisdictions that choose to use ShotSpotter suffer from gun violence in close proximity to public housing. SST explained that placing sensors quite high, often on rooftops, could mitigate incidental voice capture, but entirely avoiding those structures would severely limit ShotSpotter’s utility to these jurisdictions. The best across-the-board commitment SST can make in this context is to instruct its personnel to make reasonable efforts to avoid sensitive locations when less sensitive locations are possible.

Deciding between these trade-offs is a classic example of the value of benefit-cost analysis. Jurisdictions that have decided to utilize ShotSpotter plainly believe in its utility in detecting and alerting law enforcement to gunfire. Given that, and the relatively minimal concerns with privacy that we believe ShotSpotter presents, it makes sense to place sensors where they will be effective. As noted above, ShotSpotter will seek to minimize those locations when possible.

# I. DATA SHARING WITH THIRD PARTIES

As discussed above, ShotSpotter generates two categories of data as it operates: First, other than the limited audio used to improve its gunshot detection algorithm,<sup>15</sup> the only audio data SST retains are the short audio snippets of loud “impulsive” sounds detected by three or more sensors. Second, for each detected gunshot, SST retains metadata, including detailed date, time, GPS location, and certain gunfire characteristics (e.g., number of shots). In aggregate, SST maintains the most comprehensive data set of gunfire information in the country.

Under current contractual arrangements, in all but a few cases, SST retains ownership of this data. As a practical matter, this means that in addition to sharing data with its customer, SST has the legal authority to share, license, or sell the data as it pleases. SST’s position is that it is within its right to control and share this data because it is a private company using proprietary technology to offer a service to law enforcement. On the other hand, there are those who have expressed concern with this model, insisting that because ShotSpotter is used by law enforcement, its data, like other law enforcement data, should be public.<sup>16</sup> We do not take a position on this debate, but do offer our views about situations in which SST might share ShotSpotter data beyond its local law enforcement customers.

Although not technically a matter of personal privacy and thus somewhat outside the scope of our assessment, we have chosen to comment on this complex issue because we feel it is essential that SST take steps to clarify its third-party data sharing practices. SST has disclosed to us that it shares data with hospitals and researchers. SST has also informed us that, due to contractual arrangements, it cannot share the identity of all other third parties with which it shares such data. We obviously cannot comment on the implications of SST sharing data with unknown entities. Nor can we anticipate all the possible situations where third-party sharing may arise in the future. Knowing this, we have done our best to offer some general guidance on this issue based on our experience:

**First**, we consider it absolutely bedrock that jurisdictions have access to not only gunfire alerts but also their own aggregate data (*i.e.* data from gunfire alerts aggregated in a manner that easily allows jurisdictions to see how often, when, and where gunfire is occurring). Access to clear, aggregate gunfire data is vital so that the public can make informed public safety decisions. Moreover, realizing that jurisdictions often lack the internal capability to analyze the data in rigorous ways, we believe SST should allow

15. See *supra* note 8.

16 See, e.g., Jason Tashea, *Should the public have access to data police acquire through private companies?*, AMERICAN BAR ASSOCIATION JOURNAL (Dec. 1, 2016), [http://www.abajournal.com/magazine/article/public\\_access\\_police\\_data\\_private\\_company](http://www.abajournal.com/magazine/article/public_access_police_data_private_company).

---

jurisdictions to share their data with outside researchers, so long as the work is in furtherance of local public safety objectives.

At the same time, we understand there may be compelling public safety reasons why SST feels it should hold back certain detailed information. If so, SST should make those reasons clear and public. For example, one could imagine that for privacy and safety reasons law enforcement or victims might not want precise GPS data regarding specific incidents made public. Similarly, there is a plausible concern that certain third parties could make use of precise GPS data in ways that undermine communities (see discussion below regarding insurers). The conclusions SST reaches on this issue should be explained in its written policies, so the merits can be evaluated.

**Second**, although our understanding is that SST does not currently share audio snippets with any third parties, SST must address if, when, and how it will do so in the future. In addressing this issue, we suggest that sharing audio snippets with third parties should be subject to at least the same safeguards as with law enforcement customers, if not more.<sup>17</sup> Because we see little risk to personal privacy when the snippets are generated to begin with, we see little additional risk when it comes to sharing these snippets. Still, we think impacted communities may rightfully expect more details about SST's audio-sharing practices going forward.

**Third**, we suggest SST develop and make public its principles on when it will share non-audio data (e.g., gunfire time and location) with third parties. Unlike audio data, which SST does not currently share, SST does share gunfire alert data.

This data can take multiple forms—from sharing alerts in real-time, similar to what law enforcement receives, to sharing only high-level aggregate data. In our view, sharing alerts in real-time raises significantly different concerns than sharing aggregate data, and we urge SST to exercise great caution when considering doing so. We raise this caution for the simple reason that real-time alerts can trigger a variety of real-time responses, over which SST will not have any control (and which we cannot predict). For example, it is one thing, if a hospital uses real-time alerts to deploy ambulances; it is quite another thing if a news agency uses real-time alerts to deploy camera crews. Even sharing alerts with outside law enforcement agencies creates the possibility for additional law enforcement response.

Whether real-time alerts or aggregate data, we believe that SST should address how and whether it will inform jurisdictions that data from their communities is being shared. SST has a range of options here, from asking jurisdictions for consent to share the data to sharing the data without notice. In our view, the degree of transparency that is appropriate depends on the specificity of the data being shared:

---

17. To be perfectly clear, we view sharing access to raw sensor audio as completely unacceptable (as we would if law enforcement were given such access). SST does not do this, not with customers and not with third parties.

---

On one end of the spectrum, real-time alerts with full metadata should reasonably involve the same degree of transparency and public engagement as the decision to implement ShotSpotter to begin with. On the other hand, when it comes to including a jurisdiction's information in an aggregate, nation-wide report, we see little need for specific notice.<sup>18</sup>

What's more, the identity of the third party seeking access to SST's data is critically important. In certain communities, for example, any information sharing with U.S. Immigration and Customs Enforcement (ICE) would be a non-starter. In fact, there are those who may view information sharing with any federal law enforcement agency quite differently than sharing with local law enforcement as local communities have much more of a say in crafting local enforcement priorities (e.g., sanctuary policies, decriminalizing low-level offenses) than they do over federal law enforcement.<sup>19</sup>

Sharing with private parties is equally complex. For example, there are those third parties whose efforts are aimed at strengthening communities such as through improved public health and public safety (e.g., hospitals). Sharing with these third parties is unlikely to cause concern. Moreover, we cannot understate the importance of providing researchers with

quality data. There remains a tremendous knowledge gap in the public safety sphere.<sup>20</sup> At the same time, we think SST should avoid sharing data with third parties who likely would use the data to target or undermine the very communities that SST's technology avers to benefit. By way of example, we can imagine insurance companies using gunshot data as some have used race—as a proxy for actuarial risk and charging minority communities higher insurance rates or even denying coverage.<sup>21</sup>

These are complicated issues and we do not claim to have all the answers. In truth, the answers may vary from community to community. But just as SST has taken the burden upon itself to implement and make public its robust personal-privacy practices, we fully expect it will do the same when it comes to data sharing.

---

18. One example of this type of high-level reporting is the aggregate data SST includes in its National Gunfire Index. See ShotSpotter Inc., 2017 National Gunfire Index, <https://www.shotspotter.com/2017NGI/>.

19. We refer here to federal law enforcement agencies, not federal research institutions. One could imagine, for example, a time in the future when the Center for Disease Control might once again be permitted to conduct research into gun violence, and might find SST's data useful.

20. See, e.g., Barry Friedman & Kate Mather, Policing, *U.S. Style: With Little Idea of What Really Works*, JUST SECURITY (July 10, 2019), <https://www.justsecurity.org/64865/policing-u-s-style-with-little-idea-of-what-really-works/>. Although SST may want to vet the credentials of researchers who want SST's data to ensure their work is generally of high quality, we believe the country would greatly benefit from rigorous social science research that utilizes SST's gunfire data.

21. See, e.g., Julia Angwin, et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, PROPUBLICA (April 5, 2017), <https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk>.

## VII. CONCLUSION

ShotSpotter gunshot detection technology offers law enforcement a tool to improve their response to gun violence, including responding to gun-fire incidents that previously went unreported. But nearly every public safety tool comes with privacy and civil liberties tradeoffs. It is incumbent on law enforcement and the communities they serve to understand these tradeoffs before acquiring any new technology.

It is both inappropriate and unfair to place the entire burden of developing costs and benefits on the public. It is essential that technology providers both make these tradeoffs clear (by transparently explaining how their products operate) and by taking meaningful steps to improve their technology's design and operation to maximize public safety benefits while minimizing intrusions on civil liberties. We hope that this report helps accomplish both of those goals regarding ShotSpotter.

In response to this report, SST has undertaken significant internal efforts to implement our recommendations and make ShotSpotter more privacy protective. These changes were not costless, and in some cases significantly impacted the technology's operation. Still, SST made a conscious decision to embrace this tradeoff. Other policing technology companies should follow SST's leadership and proactively embrace their responsibility in protecting individual liberty.

**Other policing technology companies should follow SST's leadership and proactively embrace their responsibility in protecting individual liberty.**

## VIII. MORE ABOUT THE POLICING PROJECT

The Policing Project at New York University's School of Law is an independent nonprofit research and public policy organization focused on ensuring just and effective policing through democratic accountability. The Policing Project works across a host of issues—from use of force and racial profiling, to facial recognition, to reimagining public safety—in close collaboration with stakeholders who typically find themselves at odds. We bring a new approach to these fraught areas—one grounded in democratic values and designed to promote transparency, racial justice, and equitable treatment for all.

Our work is focused on policing “accountability,” but also on changing what people mean when they demand accountability. When people unhappy with policing talk about a lack of “accountability,” they typically mean that when an officer harms someone, or surveillance techniques are deployed inappropriately, no one is held responsible—officers are rarely disciplined or criminally prosecuted, courts admit evidence the police have seized illegally, and civil lawsuits are not successful. This is back-end accountability. It kicks in only after something has gone wrong, or is perceived to have gone wrong. Back-end accountability is important, but it can only

target misconduct. As such, there is a limit to what it can accomplish to guide policing before it goes awry.

Our work focuses on ensuring accountability and democratic participation on the front end. Front-end or democratic accountability involves promoting public voice in setting transparent, ethical, and effective policing policies and practices *before* the police or government act. The goal is achieving public safety in a manner that is equitable, non-discriminatory, and respectful of public values. This is how we think of accountability in most of government, yet this is all too rare in policing. We are working to change that.

Today, the Policing Project partners with civic leaders, law enforcement agencies, grassroots community organizations, and advocacy groups across the country to promote public safety through transparency, equity, and democratic engagement. Our work is carried out through demonstration projects, researching and evaluating existing oversight models, engaging in public advocacy, convening conferences and roundtables with academics and law enforcement personnel, and engaging in targeted litigation around policing issues.

Learn more about us at  
**[www.PolicingProject.org](http://www.PolicingProject.org)**.



AUGUST 2021

# THE CHICAGO POLICE DEPARTMENT'S USE OF SHOTSPOTTER TECHNOLOGY

CITY OF CHICAGO  
OFFICE OF INSPECTOR GENERAL



JOSEPH M. FERGUSON  
INSPECTOR GENERAL FOR THE CITY OF CHICAGO

DEBORAH WITZBURG  
DEPUTY INSPECTOR GENERAL FOR PUBLIC SAFETY

## TABLE OF CONTENTS

I.	EXECUTIVE SUMMARY .....	2
II.	BACKGROUND .....	4
A.	SHOTSPOTTER ACOUSTIC GUNSHOT DETECTION TECHNOLOGY .....	4
B.	SHOTSPOTTER NETWORK IN CHICAGO .....	6
III.	METHODOLOGY .....	10
A.	SHOTSPOTTER ALERT DATA.....	10
B.	JOINING SHOTSPOTTER ALERT DATA TO INVESTIGATORY STOP REPORT DATA .....	11
IV.	DATA ANALYSIS .....	13
A.	SHOTSPOTTER ALERTS: VOLUME AND DISTRIBUTION .....	13
B.	SHOTSPOTTER ALERTS: INCIDENT DISPOSITIONS.....	14
C.	INVESTIGATORY STOP REPORTS ASSOCIATED WITH SHOTSPOTTER ALERT EVENT NUMBERS .....	16
D.	INVESTIGATORY STOP REPORTS WITH "SPOTTER" AND/OR "SST" IN WRITTEN NARRATIVE .....	18
V.	CONCLUSION.....	22
	APPENDIX A: SHOTSPOTTER ALERT INCIDENT DISPOSITIONS.....	23

## TABLE OF FIGURES

FIGURE 1: SHOTSPOTTER GUNSHOT DETECTION TECHNOLOGY .....	5
FIGURE 2: TYPICAL PROCESS FROM SHOTSPOTTER ALERT TO CHICAGO POLICE ARRIVAL ON SCENE .....	8
FIGURE 3: SHOTSPOTTER ALERTS BY CPD DISTRICT AND BEAT .....	13
FIGURE 4: SHOTSPOTTER ALERTS AND LIKELY GUN-RELATED CRIMINAL INCIDENT DISPOSITIONS .....	15
FIGURE 5: LAW ENFORCEMENT OUTCOMES DOCUMENTED ON INVESTIGATORY STOP REPORTS MATCHED TO CONFIRMED SHOTSPOTTER ALERTS.....	16

## ACRONYMS

CPD	Chicago Police Department
MCC	Municipal Code of Chicago
MJC	MacArthur Justice Center
OEMC	Office of Emergency Management and Communications
OIG	Office of Inspector General
SDSC	Strategic Decision Support Center
SST	ShotSpotter Technology

## I. EXECUTIVE SUMMARY

Pursuant to the Municipal Code of Chicago (MCC) §§ 2-56-030 and -230, the Public Safety section of the Office of Inspector General (OIG) initiated an inquiry into the Chicago Police Department's (CPD) use of ShotSpotter acoustic gunshot detection technology and CPD's response to ShotSpotter alert notifications. As part of this ongoing inquiry, OIG has analyzed data collected by CPD and the City of Chicago Office of Emergency Management and Communications (OEMC) regarding all ShotSpotter alert notifications that occurred between January 1, 2020 and May 31, 2021, and investigatory stops confirmed to be associated with CPD's response to a ShotSpotter alert.

In this report, OIG details ShotSpotter's functionality and descriptive statistics regarding law enforcement activity related to CPD's response to ShotSpotter alerts. OIG does not issue recommendations associated with this descriptive data. OIG is issuing this analysis of the outcomes of ShotSpotter alerts to provide the public and City government officials—to the extent feasible given the quality of OEMC and CPD's data—with clear and accurate information regarding CPD's use of ShotSpotter technology.

The City's three-year contract with ShotSpotter began on August 20, 2018, through August 19, 2021, at a cost of \$33 million.<sup>1</sup> In November 2020, well before the end of the contract term, CPD requested an extension of the contract and in December 2020, the City exercised an option to extend it, setting a new expiration date for August 19, 2023.<sup>2</sup> In March 2021, CPD requested approval for an annual 5% increase in the cost per square mile of the contract.

OIG's descriptive analysis of OEMC data and investigatory stop report (ISR) data collected for ShotSpotter alert incidents that occurred between January 1, 2020 and May 31, 2021, revealed the following:

1. A total of 50,176 ShotSpotter alerts were confirmed as probable gunshots by ShotSpotter, issued an event number—a unique record identification number assigned to

---

<sup>1</sup> The initial contract was neither competitively bid nor a non-competitive sole source contract, but a reference contract entered pursuant to MCC §2-92-649. Article 1 of the contract states "The City, pursuant to Chapter 2-92-649 ("Reference Contract Ordinance") of the Municipal Code of Chicago ("MCC"), desires to enter into an agreement with the Contractor for the purchase of ShotSpotter Flex gunfire detection, alert and analytic subscription services by using an existing contract ("Reference Contract") of another unit of government. There exists a contract by and between the City of Louisville, Kentucky, and Contractor; these two parties entered into a contract on January 31, 2017 for the provision by the Contractor of a subscription for gunshot detection software and services. The City of Louisville awarded the Contract pursuant to a publicly advertised Request for Proposals. The Reference Contract Ordinance grants the Chief Procurement Officer ("CPO") of the City the authority to enter into a new contract (a "City Contract") based on a Reference Contract." City of Chicago, "Contract Number 71366," August 22, 2018, accessed July 21, 2021, <https://webapps1.chicago.gov/vcsearch/city/contracts/71366>.

<sup>2</sup> City of Chicago, "Contract Number 71366: Modifications/Amendments," December 22, 2020, accessed July 21, 2021, <https://webapps1.chicago.gov/vcsearch/city/contracts/71366>. Section 5.5 of the original contract allows for a 24-month extension.

distinct “events” of police activity—and dispatched by OEMC; each of these resulted in a CPD response to the location reported by the ShotSpotter application.

2. Of the 50,176 confirmed and dispatched ShotSpotter alerts, 41,830 report a disposition—the outcome of the police response to an incident. A total of 4,556 of those 41,830 dispositions indicate that evidence of a gun-related criminal offense was found, representing 9.1% of CPD responses to ShotSpotter alerts.
3. Among the 50,176 confirmed and dispatched ShotSpotter alerts, a total of 1,056 share their event number with at least one ISR, indicating that a documented investigatory stop was a direct result of a particular ShotSpotter alert. That is, at least one investigatory stop is documented under a matching event number in 2.1% of all CPD responses to ShotSpotter alerts. Some of those events are also among those with dispositions indicating that evidence of a gun-related criminal offense was found, where an investigatory stop might have been among the steps which developed evidence of a gun-related criminal offense.
4. Through a separate keyword search analysis of all ISR narratives within the analysis period, OIG identified an additional 1,366 investigatory stops as potentially associated with ShotSpotter alerts whose event number did not match any of the 50,176 confirmed and dispatched ShotSpotter alerts. OIG’s review of a sample of these ISRs indicated that many of these keyword search “hits” were in narratives referring to the general volume of ShotSpotter alerts in a given area rather than a response to a specific ShotSpotter alert.

OIG concluded from its analysis that CPD responses to ShotSpotter alerts rarely produce documented evidence of a gun-related crime, investigatory stop, or recovery of a firearm. Additionally, OIG identified evidence that the introduction of ShotSpotter technology in Chicago has changed the way some CPD members perceive and interact with individuals present in areas where ShotSpotter alerts are frequent.

## II. BACKGROUND

There are a number of possible ways to measure law enforcement activity and outcomes arising from ShotSpotter alerts. In light of limitations in data quality and reporting, OIG focuses on two such metrics. First, OIG examines instances in which CPD's immediate response to ShotSpotter produces evidence sufficient for the incident to be coded as a crime, and specifically, a gun-related crime. Second, OIG reports on the frequency with which CPD reports an investigatory stop in a way which allows it to be associated with a ShotSpotter alert, and whether those investigatory stops produce gun crime-related outcomes.

The information in this report relating to the technical operations of the ShotSpotter system and the process for confirming ShotSpotter alerts and dispatching police to respond to those alerts is sourced primarily from publicly available records. Where the publicly available records are silent or ambiguous on these topics, OIG has identified issues for possible future study.

### A. SHOTSPOTTER ACOUSTIC GUNSHOT DETECTION TECHNOLOGY

ShotSpotter is a gunshot detection system that uses a network of acoustic sensors to identify and locate suspected gunshots. ShotSpotter sensors rely on an algorithm to flag noises suggestive of gunshots, and the ShotSpotter system approximates the location of the possible gunshots via triangulation and multilateration—two techniques for computing the source location of a sound based on the time of arrival and angle of arrival of sound waves at multiple surrounding sensors.<sup>3</sup> Then, a human “acoustic expert” at ShotSpotter’s Incident Review Center, located at a ShotSpotter corporate office, reviews these readings. The acoustic expert listens to the audio flagged by the algorithm to determine whether to classify the detected noise as a gunshot or gunshots and alert local police. Sounds that are not gunshots may activate ShotSpotter sensors. ShotSpotter’s public-facing description of its system acknowledges the potential for fireworks to produce false positive alerts, due to the similarities in the impulsive nature of the sound and the distance the impulsive sound produced by either gunshots or fireworks can travel.<sup>4</sup> ShotSpotter acoustic experts are responsible for filtering out these false positive alerts from the confirmed alerts that are forwarded to local police. ShotSpotter currently operates in more than 100 U.S. cities.<sup>5</sup>

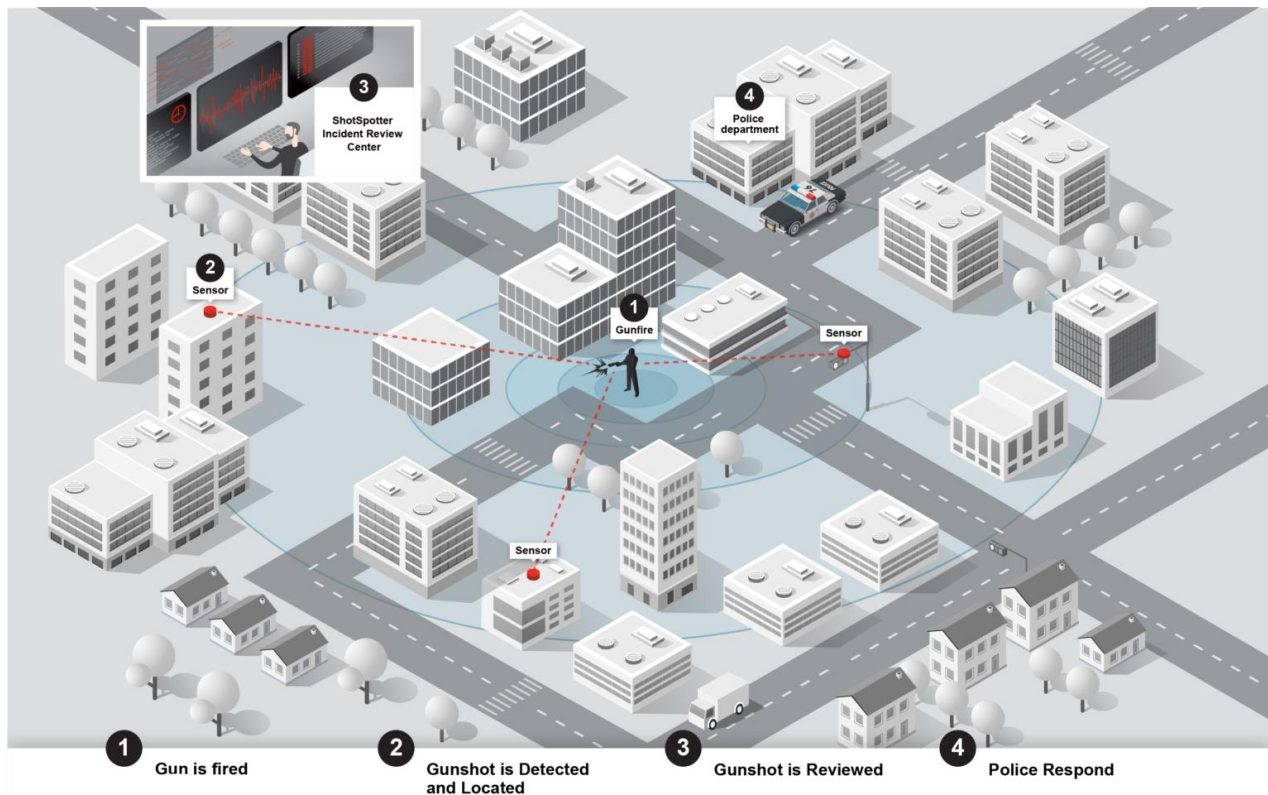
---

<sup>3</sup> Triangulation identifies the location of a noise based on angle of arrival (AoA) and multilateration identifies the location of a noise based on time difference of arrival (TDoA). ShotSpotter’s patented technology uses both AoA and TDoA to identify the location where a noise suggestive of gunshots originated. ShotSpotter, “Gunshot Detection Technology,” September 2, 2014, accessed June 14, 2021, <https://www.shotspotter.com/system/content/uploads/mediakit/Gunshot-detection-WP.pdf>.

<sup>4</sup> In 2014, ShotSpotter produced a white paper that explains, in detail, the technical science behind the acoustic gunshot detection technology, including a discussion of false positive alerts. ShotSpotter, “Gunshot Detection Technology,” September 2, 2014, accessed June 14, 2021, <https://www.shotspotter.com/system/content/uploads/mediakit/Gunshot-detection-WP.pdf>.

<sup>5</sup> “ShotSpotter Respond FAQ,” *ShotSpotter*, December 2020, accessed June 14, 2021, <https://www.shotspotter.com/wp-content/uploads/2020/12/ShotSpotter-Respond-FAQ-Dec-2020.pdf>.

FIGURE 1: SHOTSPOTTER GUNSHOT DETECTION TECHNOLOGY



Source: ShotSpotter.<sup>6</sup>

Research published by the Brookings Institution—a nonprofit research organization—in 2016 found that only 12.4% of incidents of shots fired in Washington, DC, resulted in a resident calling 911 to report that they heard noise suggestive of gunshots.<sup>7</sup> A 2020 study of ShotSpotter in St. Louis, MO, found, following installation of ShotSpotter sensors, a *decrease* of approximately 30% in the volume of 911 calls reporting shots fired, an 80% overall *increase* in volume of police responses to incidents of reported gunshots, and no significant reduction in crime attributable to the installation of ShotSpotter sensors.<sup>8</sup>

In 2021, the Journal of Urban Health published a ShotSpotter study conducted by several researchers, including individuals affiliated with the Center for Gun Policy and Research at the Johns Hopkins Bloomberg School of Public Health and several hospitals in Hartford, CT. The

<sup>6</sup> ShotSpotter, “Gunshot Detection,” accessed June 14, 2021, <https://www.shotspotter.com/law-enforcement/gunshot-detection/>.

<sup>7</sup> Jillian B. Carr and Jennifer L. Doleac, “The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using ShotSpotter Data,” Brookings Institution, April 2016, accessed June 14, 2021, <https://www.brookings.edu/research/the-geography-incidence-and-underreporting-of-gun-violence-new-evidence-using-shotspotter-data/>.

<sup>8</sup> Dennis Mares and Emily Blackburn, “Acoustic Gunshot Detection Systems: a Quasi-Experimental Evaluation in St. Louis, MO,” *Journal of Experimental Criminology* 17, no. 2 (2020): 193–215, <https://doi.org/10.1007/s11292-019-09405-x>.

analysis concerned the impact of ShotSpotter technology on homicides and arrests for murder and weapons across 68 large metropolitan counties between 1999 and 2016. This study found that implementing ShotSpotter technology had no significant impact on firearm-related homicides or arrest outcomes.<sup>9</sup>

## B. SHOTSPOTTER NETWORK IN CHICAGO

Gunshot detection technology was deployed in Chicago as a feature of the second generation of police observation device cameras installed between September and December of 2003.<sup>10</sup> According to a CBS2 News story in 2012, the City later determined the gunshot detection systems of the early 2000s were “too expensive and ineffective.”<sup>11</sup> In 2012, under CPD’s then-Superintendent Garry McCarthy, ShotSpotter sensors were installed in sections of CPD’s 3<sup>rd</sup>, 7<sup>th</sup>, 8<sup>th</sup>, and 11<sup>th</sup> Districts, with McCarthy stating that the technology had improved “dramatically.”<sup>12</sup> In 2018, the City of Chicago entered into a three-year, \$33 million dollar contract with ShotSpotter to provide network coverage in 12 police Districts over 100 square miles, making Chicago ShotSpotter’s largest customer.<sup>13</sup> On December 22, 2020, the City exercised an option to extend the current contract with ShotSpotter through August 19, 2023.<sup>14</sup> The City’s Violence Reduction Dashboard reports that, as of May 2021, ShotSpotter sensors have been installed in CPD’s 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, 6<sup>th</sup>, 7<sup>th</sup>, 8<sup>th</sup>, 9<sup>th</sup>, 10<sup>th</sup>, 11<sup>th</sup>, 15<sup>th</sup>, and 25<sup>th</sup> Districts.<sup>15</sup>

Currently, ShotSpotter is one of the tools used by analysts in CPD’s Strategic Decision Support Centers (SDSCs), CPD District-based centers that are “equipped with crime-reduction tools and technology to assist [CPD] members with district-crime forecasting and achieving the primary

---

<sup>9</sup> Mitchell L. Doucette, Christa Green, Jennifer Necci Dineen, David Shapiro, and Kerri M. Raissian, “Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: a Longitudinal Analysis, 1999–2016,” *Journal of Urban Health*, April 30, 2021, accessed June 14, 2021, <https://doi.org/10.1007/s11524-021-00515-4>.

<sup>10</sup> Chicago Police Department, “Police Observation Device (POD) Cameras,” accessed June 14, 2021, <https://home.chicagopolice.org/information/police-observation-device-pod-cameras/>.

<sup>11</sup> “Chicago Police Testing New Gunshot-Detection Technology,” *CBS News*, October 25, 2012, accessed May 19, 2021, <https://chicago.cbslocal.com/2012/10/25/chicago-police-testing-new-gunshot-detection-technology/>.

<sup>12</sup> “Chicago Police Testing New Gunshot-Detection Technology,” *CBS News*, October 25, 2012, accessed May 19, 2021, <https://chicago.cbslocal.com/2012/10/25/chicago-police-testing-new-gunshot-detection-technology/>.

<sup>13</sup> City of Chicago, “Contract Number 71366,” August 22, 2018, accessed June 14, 2021, <https://webapps1.chicago.gov/vcsearch/city/contracts/71366>. The contract itself specifies a dollar amount of \$33 million. A press release from ShotSpotter Inc. stated that the value of the contract was \$23 million. ShotSpotter, “Chicago Signs \$23 Million Multi-Year Agreement with ShotSpotter to Extend Gunshot Detection Coverage into Next Decade,” September 5, 2018, accessed June 14, 2021, <https://www.shotspotter.com/press-releases/chicago-signs-23-million-multi-year-agreement-with-shotspotter-to-extend-gunshot-detection-coverage-into-next-decade/>.

<sup>14</sup> City of Chicago, “Contract Number 71366: Modifications/Amendments,” December 22, 2020, accessed July 21, 2021, <https://webapps1.chicago.gov/vcsearch/city/contracts/71366>.

<sup>15</sup> City of Chicago, “Violence Reduction Dashboard Glossary,” accessed June 14, 2021, <https://www.chicago.gov/city/en/sites/vrd/home.html>. OEMC data identifies some ShotSpotter alerts occurring in CPD Districts not reported to house ShotSpotter sensors.

mission of district crime-reduction.”<sup>16</sup> The first SDSCs were established in 2017 in partnership with the University of Chicago Crime Lab.<sup>17</sup> After a shots fired incident is detected and confirmed by a ShotSpotter-employed “acoustic expert” at a ShotSpotter office, the alert is displayed on the ShotSpotter application, which is accessible by the CPD members assigned to the SDSC (“SDSC analysts”), OEMC, and CPD members who are equipped with the ShotSpotter mobile application on CPD-issued smartphones. SDSC analysts monitor the ShotSpotter application for these incoming alerts. When alerts come through, pursuant to CPD directives, SDSC analysts are responsible for initiating the dispatch process by contacting OEMC to report the ShotSpotter alert.<sup>18</sup> OEMC personnel will then issue an event number—a unique identification number assigned to every distinct incident of police activity—for a ShotSpotter alert and dispatch CPD units to respond.<sup>19</sup>

---

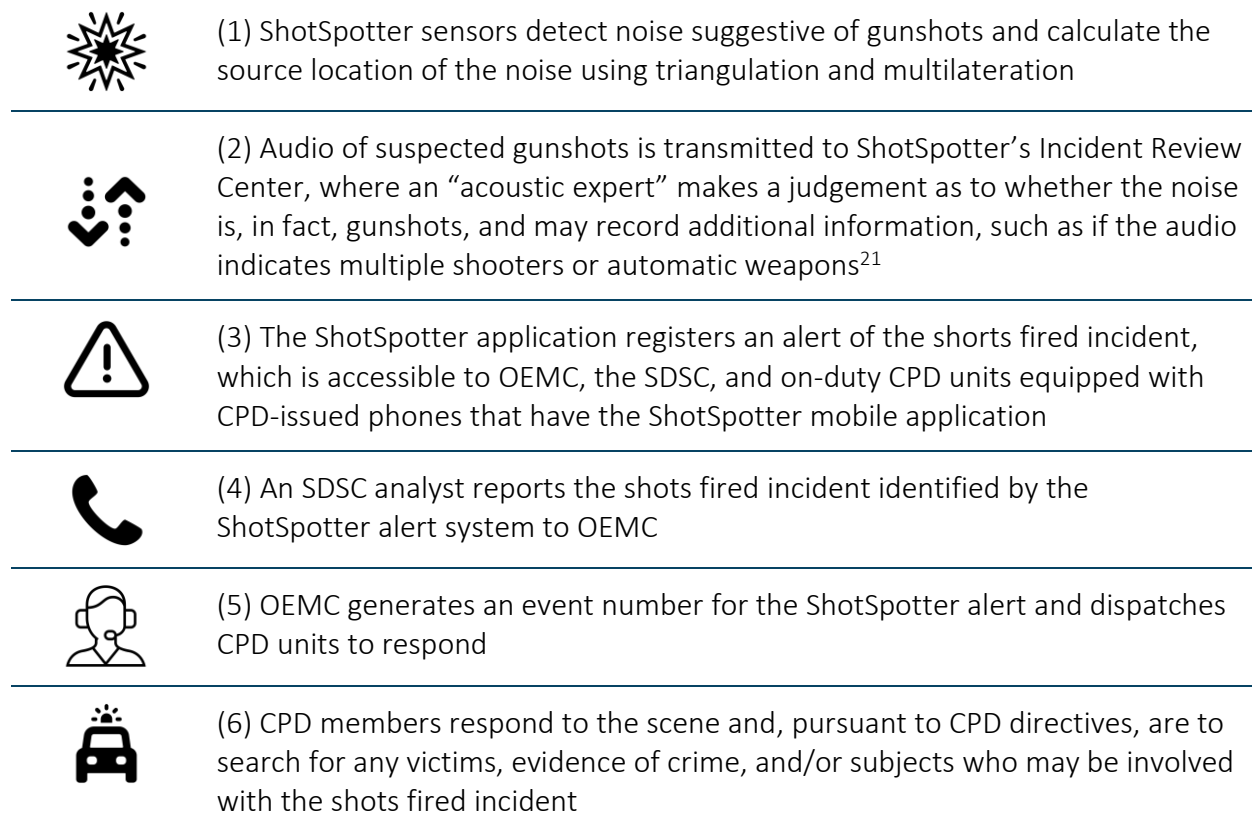
<sup>16</sup> Chicago Police Department, “Special Order S03-02-01: Strategic Decision Support Centers: Operations and Accountability,” IV.A., July 26, 2019, accessed July 19, 2021, <http://directives.chicagopolice.org/directives/data/a7a57b85-16c2efbe-c2416-c2fa-edbba6051837c01c.pdf?hl=true>.

<sup>17</sup> Chicago Tribune Editorial Board, “A high-tech ray of hope in the fight against gun violence in Englewood,” *Chicago Tribune*, December 15, 2017, accessed May 19, 2021, <https://www.chicagotribune.com/opinion/editorials/ct-edit-englewood-20171215-story.html>, and University of Chicago, “A \$10 million grant will support Crime Lab collaboration for police innovation,” April 12, 2018, accessed June 25, 2021, <https://news.uchicago.edu/story/10-million-grant-will-support-crime-lab-collaboration-police-innovation>.

<sup>18</sup> SDSCs were initially staffed by analysts who were employed by the University of Chicago Crime Lab. In January 2020, after a transitional phase during which CPD hired analysts and the University of Chicago Crime Lab trained them, the University of Chicago Crime Lab analysts moved out of the CPD District SDSCs. University of Chicago Crime Lab, “Strategic Decision Support Centers (SDSCs),” accessed June 14, 2021, <https://urbanlabs.uchicago.edu/programs/strategic-decision-support-centers-sdscs>, and Chicago Police Department, “Strategic Decision Support Center: A User Manual,” 2019. While OEMC receives alerts from ShotSpotter’s “acoustic experts” concurrent with the SDSCs, CPD’s directive provides that “ShotSpotter incidents will be dispatched from the District’s Strategic Decision Support Center (SDSC) to field units through the Office of Emergency Management and Communications (OEMC).” Chicago Police Department, “Special Order S03-19: ShotSpotter Flex Program,” IV.B., July 5, 2017, accessed June 25, 2021, [directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true](http://directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true).

<sup>19</sup> Chicago Police Department, “Strategic Decision Support Center: A User Manual,” 2019.

**FIGURE 2: TYPICAL PROCESS FROM SHOTSPOTTER ALERT TO CHICAGO POLICE ARRIVAL ON SCENE<sup>20</sup>**



Source: OIG analysis.

CPD established its first special order concerning ShotSpotter on July 5, 2017, replacing a department notice issued in 2012.<sup>22</sup> CPD Special Order S03-19: ShotSpotter Flex Program states that ShotSpotter will be used as part of CPD's Gang Violence Reduction Strategy.<sup>23</sup> S03-19 establishes that ShotSpotter alerts will prompt "an immediate dispatch with the priority of in

<sup>20</sup> This figure is demonstrative of major steps in the typical sequence of events from a ShotSpotter noise detection to alert to arrival of CPD units on scene. The information in this figure is gathered from multiple sources, and it does not purport to be exhaustive of every aspect of this sequence of events, nor is this typical sequence the only possible way for CPD members to arrive on scene of a ShotSpotter alert. CPD units are equipped with the ShotSpotter mobile application and may respond directly to any alerts that originate from the application rather than an assigned dispatch from OEMC.

<sup>21</sup> ShotSpotter, "See how ShotSpotter Gunshot detection works," accessed June 14, 2021, video, <https://www.shotspotter.com/law-enforcement/gunshot-detection/>.

<sup>22</sup> Chicago Police Department, "Special Order S03-19: ShotSpotter Flex Program," July 5, 2017, accessed June 25, 2021, [directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true](https://directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true).

<sup>23</sup> Chicago Police Department, "Special Order S03-19: ShotSpotter Flex Program," July 5, 2017, accessed June 25, 2021, [directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true](https://directives.chicagopolice.org/directives/data/a7a57b85-15d1331c-51715-d133-2e1831b972745907.pdf?hl=true), and Chicago Police Department, "General Order G10-01: Gang Violence Reduction Strategy," February 8, 2019, accessed June 25, 2021, [http://directives.chicagopolice.org/directives/data/a7a57bf0-136d1d31-16513-6d1d-382b311ddf65fd3a.pdf?hl=true](https://directives.chicagopolice.org/directives/data/a7a57bf0-136d1d31-16513-6d1d-382b311ddf65fd3a.pdf?hl=true).

progress crimes involving the use of a firearm.”<sup>24</sup> Responding CPD members are cautioned to “take a safe and strategic approach while responding to the incident, being aware that an offender or multiple offenders may be on scene.”<sup>25</sup> SDSC analysts are responsible for analyzing and reporting notable observations and/or trends in ShotSpotter alerts and assisting command staff in developing a strategic response.<sup>26</sup>

At the conclusion of any law enforcement activity, the primary responding CPD unit is to report a disposition—the outcome of the incident—to OEMC. OEMC will then record the corresponding disposition code in the record for the event number. Criminal incidents are assigned an Illinois Uniform Crime Reporting code.<sup>27</sup> Incidents that are not criminal in nature but require the completion of a case report, such as a traffic crash, are assigned a non-criminal incident code.<sup>28</sup> For incidents that do not require the completion of a case report, CPD also defines a set of “miscellaneous incident” disposition codes.<sup>29</sup> When a CPD member responds to a ShotSpotter alert, they are to take investigative steps which may include interviewing witnesses, conducting investigatory stops, running license plates, searching for shell casings, etc. If these activities produce evidence of a shooting or any other criminal activity, a corresponding criminal incident code will be assigned. If there is no such evidence, then the event will receive a miscellaneous incident disposition code.

---

<sup>24</sup> Chicago Police Department, “Special Order S03-19: ShotSpotter Flex Program,” IV.B., July 5, 2017. Whether criminal activity that prompts a ShotSpotter alerts is, in fact, still “in progress” when OEMC sends the dispatch would depend in part on how long the process depicted in Figure 2 took.

<sup>25</sup> Chicago Police Department, “Special Order S03-19: ShotSpotter Flex Program,” VII.C.2., July 5, 2017.

<sup>26</sup> Chicago Police Department, “Special Order S03-19: ShotSpotter Flex Program,” VII.E., July 5, 2017.

<sup>27</sup> Chicago Police Department, “Illinois Uniform Crime Reporting (IUCR) Codes,” accessed July 13, 2021, <https://data.cityofchicago.org/Public-Safety/Chicago-Police-Department-Illinois-Uniform-Crime-R/c7ck-438e>. According to the City of Chicago Office of Public Safety Administration, crime classification codes are “derived from the Federal Bureau of Investigation's (FBI) National Incident-Based Reporting System (NIBRS) Uniform Crime Reporting (UCR) Program.” NIBRS codes report the crime type and UCR codes report the specific criminal offense. City of Chicago Office of Public Safety Administration, “Definition & Description of Crime Types,” accessed July 20, 2021, [https://gis.chicagopolice.org/pages/crime\\_details](https://gis.chicagopolice.org/pages/crime_details).

<sup>28</sup> Chicago Police Department, “Incident Reporting Table (CPD 63.451),” accessed July 13, 2021, [http://directives.chicagopolice.org/forms/CPD-63.451\\_Table.pdf](http://directives.chicagopolice.org/forms/CPD-63.451_Table.pdf).

<sup>29</sup> Chicago Police Department, “Miscellaneous Incident Reporting Table (CPD 11.484),” accessed June 25, 2021, <http://directives.chicagopolice.org/forms/CPD-11.484.pdf>.

### III. METHODOLOGY

#### A. SHOTSPOTTER ALERT DATA

OIG analyzed OEMC data for confirmed dispatched ShotSpotter alerts between January 1, 2020 and May 31, 2021.<sup>30</sup> ShotSpotter alerts reported to OEMC are stored in the same database in which OEMC documents other event records related to police service, including 911 calls for service that OEMC receives from the public and notifications of police-initiated events such as investigatory stops received from police officers.<sup>31</sup> Each of the events recorded in this database is assigned an event number, which is a unique identification number assigned to every distinct incident of police activity.<sup>32</sup> Multiple records associated with a single incident of police activity (a single “event”) should, in principle, be assigned the same event number. Accompanying information about events recorded in the OEMC database includes location information, a “final” designation of the type of event, and the “disposition” of the incident.<sup>33</sup>

OIG identified for analysis 50,176 ShotSpotter alerts in OEMC’s data between January 1, 2020 and May 31, 2021. This represents the number of instances in which ShotSpotter sensors registered an alert that, after review by ShotSpotter’s “acoustic experts” and personnel in CPD’s SDSCs, was sent on to OEMC, dispatched by OEMC, and recorded as an event of final type “SST” by OEMC, short for ShotSpotter Technology. This means that CPD members responded to 50,176

---

<sup>30</sup> A dispatched event is any event marked as “dispatched” in OEMC’s database or supplied with a dispatch date and time.

<sup>31</sup> Chicago Police Department, “General Order G03-01: Communications Systems and Devices,” III.B-E, May 30, 2014, accessed July 21, 2021, <http://directives.chicagopolice.org/directives/data/a7a57be2-1287e496-14312-87e6-e46a12b808498f0d.pdf?ownapi=1>.

<sup>32</sup> Chicago Police Department, “General Order G03-01: Communications Systems and Devices,” III.C-D, May 30, 2014.

<sup>33</sup> The event type designations that OEMC applies to 911 calls for service can be seen on OIG’s dashboards, along with the volume of calls received that are designated to each event type. City of Chicago Office of Inspector General, “911 Calls,” accessed June 21, 2021, <https://informationportal.igchicago.org/911-calls-for-cpd-service/>. The OEMC database includes many other data fields as well, and OIG made two methodological decisions on how to treat these data fields that had a marginal impact on the total population of ShotSpotter alerts identified in the period of analysis. First, the OEMC database designates both an “initial type” and a “final type” for each event. In the period of analysis, OIG identified 171 records for which the “initial type” was “SST” (ShotSpotter) and the “final type” was recorded as something else. OEMC personnel have reported to OIG that discrepancies between “initial type” and “final type” occur for two main reasons: (1) an officer responding to the event updates the type to align with the situation; or (2) the OEMC operator receives added details during the call and updates the type. Accordingly, these 171 records were excluded from OIG’s analysis. Secondly, OEMC’s database has a field to indicate if events are “duplicate.” In the period of analysis, there are 8,379 events with an “initial type” and/or “final type” of “SST” that are also tagged as “duplicate” events. Upon examination of these records, OIG determined that elimination of events tagged as “duplicate” would result in the loss of valuable information, such as event numbers tagged as “duplicate” that matched to event numbers recorded on investigatory stop reports. Additionally, in this review of ShotSpotter alert data, OIG is concerned with law enforcement outcomes of each individual ShotSpotter alert that receives a dispatch, regardless of whether multiple alerts are associated with what may be considered one incident; that is, for these purposes, the relevant unit of analysis is a distinct ShotSpotter alert event number. Therefore, events tagged as “duplicate” with a “final type” of “SST” were included in the analysis.

individual reports of probable gunshots identified by ShotSpotter between January 1, 2020 and May 31, 2021.

OIG used OEMC's "Location" field information and geocoding technology to map ShotSpotter alerts by CPD Beat. In the OEMC data available to OIG, 90.4% of the 50,176 events with a "final type" of a ShotSpotter alert in the analysis period listed locations that included datapoints for the corresponding CPD District and Beat. For the remaining 4,825 alerts, OIG cleaned all available location data and successfully geocoded 3,896 records to capture geographic datapoints for a cumulative total of 98.1% of the ShotSpotter alerts in the analysis period.

While the ShotSpotter application is notionally communicating geographic coordinates to OEMC and SDSCs with every alert, it is nevertheless true that, for a small percentage of those alerts, the location data that is ultimately stored in OEMC's database is incomplete or in a format that is incompatible with geocoding software. Information transfers from ShotSpotter to CPD to OEMC may introduce alterations or errors in the location information associated with the initial ShotSpotter alerts by the time OEMC personnel make a database entry (See Figure 2 for an overview of the multiple steps and actors that are part of this process). OIG did not exclude event numbers for ShotSpotter alerts that occurred outside the boundaries of CPD Districts confirmed to have ShotSpotter sensors or the immediately adjacent beats, and instead relied on OEMC's reporting of ShotSpotter alerts regardless of their location.<sup>34</sup>

## **B. JOINING SHOTSPOTTER ALERT DATA TO INVESTIGATORY STOP REPORT DATA**

OIG joined data from CPD's ISR database to OEMC's ShotSpotter event data to identify investigatory stops initiated after and related to ShotSpotter alerts using recorded event numbers. As described in the previous section, OEMC issues event numbers to ShotSpotter alerts, and CPD directives require that CPD members record the relevant event number when completing ISRs.<sup>35</sup> These event numbers should, in principle, allow for cross referencing of multiple reports and data records that are created in relation to a single "event."

OIG queried ISR records and matched event numbers to the set of 50,176 confirmed ShotSpotter alerts, returning 1,056 event numbers shared by both a ShotSpotter alert and one or more approved ISRs.<sup>36</sup> CPD members documenting an investigatory stop are required to complete a

---

<sup>34</sup> ShotSpotter sensors are currently installed in the 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, 6<sup>th</sup>, 7<sup>th</sup>, 8<sup>th</sup>, 9<sup>th</sup>, 10<sup>th</sup>, 11<sup>th</sup>, 15<sup>th</sup>, and 25<sup>th</sup> CPD Districts. City of Chicago, "Violence Reduction Dashboard Glossary," accessed June 14, 2021, <https://www.chicago.gov/city/en/sites/vrd/home.html>. Among the 49,247 ShotSpotter alerts that were successfully geocoded, 294 (0.6%) were located in a CPD District outside the 12 with confirmed ShotSpotter sensors, and 226 of those were located in a CPD Beat immediately adjacent to a CPD District with confirmed ShotSpotter sensors.

<sup>35</sup> Chicago Police Department, "Special Order S04-13-09: Investigatory Stop System," VIII.A.3, July 10, 2017, accessed July 20, 2021, <http://directives.chicagopolice.org/directives/data/a7a57b99-151b6927-49f15-1b69-2c32e99868b316b0.pdf?ownapi=1>

<sup>36</sup> Additional records reflecting investigatory stop reports in a status other than "approved" were excluded from analysis. Where duplicate ISR records by event number and subject reported disagreement as to whether (1) a gun

narrative account of the stop; OIG searched for additional ISRs which may be associated with ShotSpotter alerts by conducting keyword searches of the narrative field. By searching for the keywords "SPOTTER" and "SST," OIG identified an additional 1,366 ISRs that contained one of these keywords but for which the ISR event number did not match any of the 50,176 ShotSpotter alert event numbers in the analysis period.<sup>37</sup> These 1,366 ISRs were associated with 917 distinct event numbers. Review of a sample of 72 of these reports—one randomly sampled report from each CPD District with confirmed ShotSpotter sensors (12) for each quarter (6) in the analysis period—revealed important results relating to both the quality of CPD's record keeping and the outcomes of ShotSpotter events, described further below in section IV.D.

The keyword search analysis provides an estimate of the volume of investigatory stops associated with ShotSpotter alerts that cannot be matched by event number, but it does not provide conclusive results as to the true number of investigatory stops conducted as part of the law enforcement response to a ShotSpotter alert.<sup>38</sup> For this reason, OIG restricted quantitative and geographic analysis to the set of 1,740 ISRs associated with 1,056 ShotSpotter alert event numbers through an exact event number match.

---

was recovered, (2) an arrest was made, (3) a search was performed, and/or (4) a pat down was performed, OIG preserved the ISR record which indicated the observation did occur, using a hierarchical scheme indicated by the order as listed. CPD members frequently record only the last five digits of the ten-digit event number, and this occurred in 843 (79.8%) of the matched ISRs. OIG performed data management transformations on these ISR event numbers to recreate the complete ten-digit event number to facilitate event number matching.

<sup>37</sup> This set of 1,366 ISRs corresponded to 917 distinct event numbers.

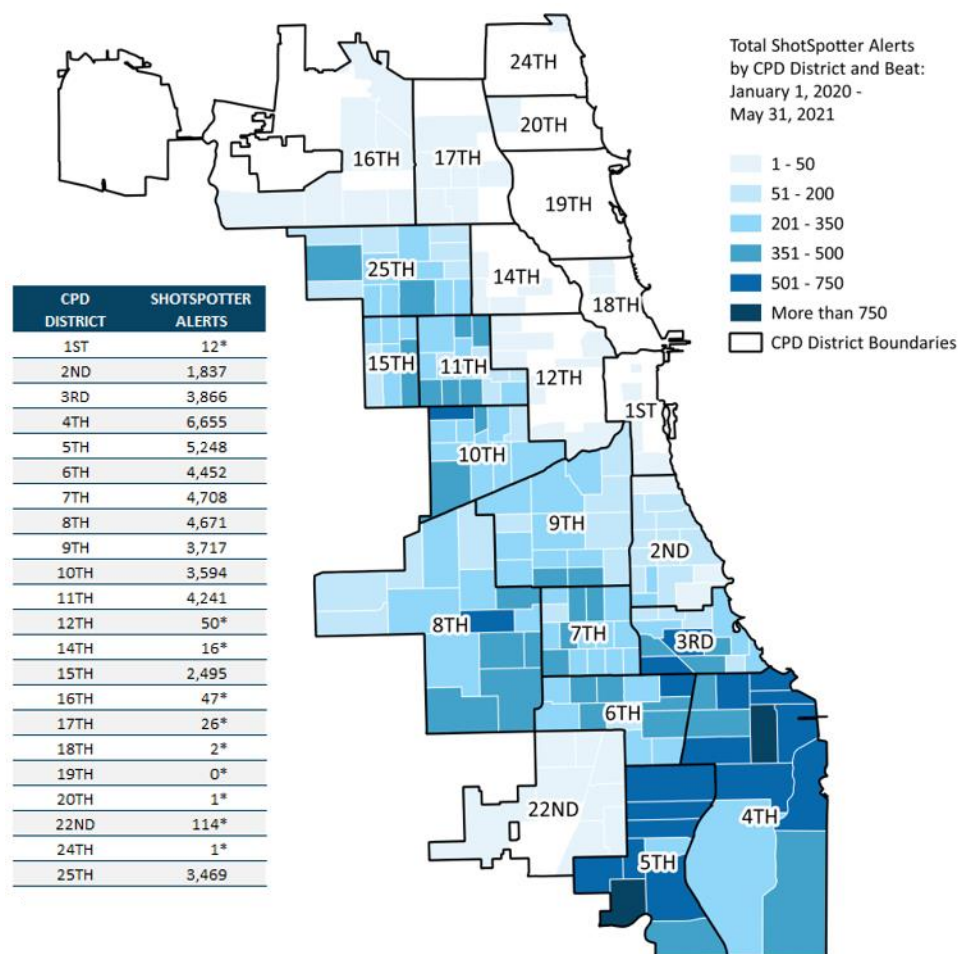
<sup>38</sup> OIG relied upon CPD documentation of investigatory stops; where CPD did not document an investigatory stop, OIG was unable to identify and analyze such law enforcement activity. Additionally, OIG's review of the random sample of 72 narratives revealed that many references to ShotSpotter in ISR narratives did not concern *specific ShotSpotter alerts*, but rather reflected mention of the *overall volume of ShotSpotter alerts in a given area*, meaning these keyword search "hits" would not be appropriately classified as a CPD response to a unique ShotSpotter alert.

## IV. DATA ANALYSIS

### A. SHOTSPOTTER ALERTS: VOLUME AND DISTRIBUTION

Between January 1, 2020 and May 31, 2021, a total of 50,176 ShotSpotter alerts were confirmed by ShotSpotter acoustic experts and dispatched as an event of final type "SST" by OEMC. This means that CPD members responded to 50,176 individual reports of probable gunshots identified by ShotSpotter between January 1, 2020 and May 31, 2021. Nearly a quarter of ShotSpotter events during the analysis period are concentrated in CPD's 4<sup>th</sup> (South Chicago) and 5<sup>th</sup> (Calumet) Districts, totaling 11,903 (23.7%) confirmed ShotSpotter alerts.

FIGURE 3: SHOTSPOTTER ALERTS BY CPD DISTRICT AND BEAT<sup>39</sup>



Source: OIG analysis.

<sup>39</sup> OIG did not exclude event numbers for ShotSpotter alerts that occurred outside the boundaries of CPD Districts confirmed to have ShotSpotter sensors or the immediately adjacent CPD Beats, and instead relied on OEMC's reporting of ShotSpotter alerts regardless of their location. Among the 49,247 ShotSpotter alerts that were successfully geocoded, 294 (0.6%) were located in a CPD District outside the 12 with confirmed ShotSpotter sensors. The ShotSpotter alert totals reported in Districts which are not confirmed to have ShotSpotter sensors are marked with an asterisk (\*) in the Figure 3 table.

In light of limitations in data quality and reporting, OIG focuses on two metrics for law enforcement activity and outcomes arising from ShotSpotter alerts. First, OIG examines instances in which CPD's immediate response to ShotSpotter produces evidence sufficient for the incident to be coded as a crime, and specifically, a gun-related crime. Second, OIG reports on the frequency with which CPD reports an investigatory stop in a way which allows it to be associated with a ShotSpotter alert, and whether those investigatory stops produce gun crime-related outcomes.

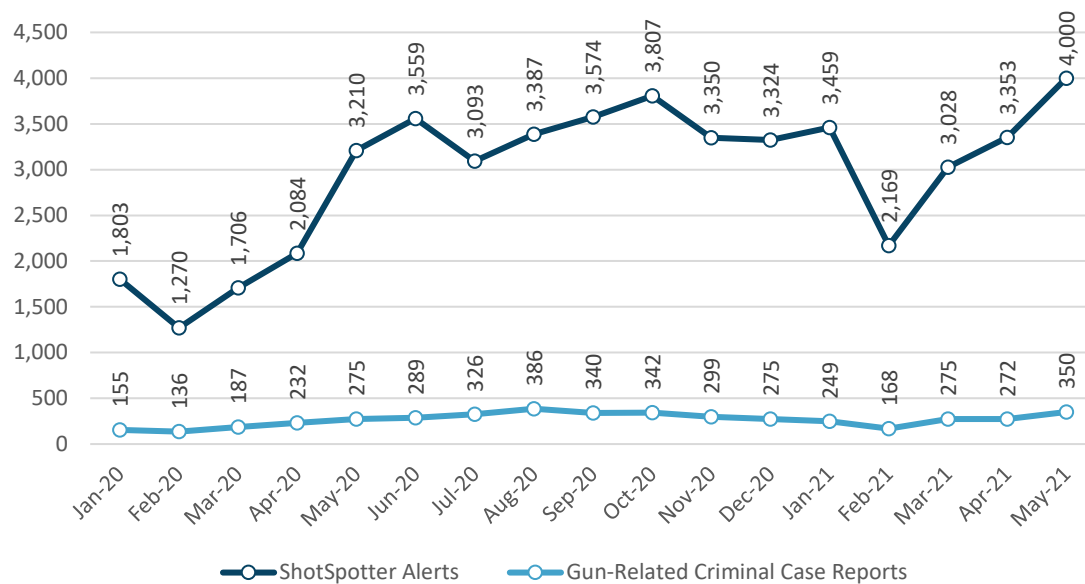
## **B. SHOTSPOTTER ALERTS: INCIDENT DISPOSITIONS**

In 8,346 of the 50,176 confirmed ShotSpotter alerts (16.6%), no disposition code indicating the final outcome of the event was recorded in the OEMC event record. The remaining 41,830 ShotSpotter alerts reported either a criminal incident disposition, a non-criminal incident disposition, or a miscellaneous incident disposition. Criminal incident dispositions account for 13.2% of OEMC records that include disposition data, representing 5,504 criminal case reports completed following a CPD response to a ShotSpotter alert. Of that total, 4,556 criminal case reports—82.8% of criminal incident dispositions and 10.9% of all records reporting a disposition—listed charges which are likely related to gun violence or illegal gun possession.<sup>40</sup> Figure 4 below displays the monthly total of ShotSpotter alerts alongside the monthly total of ShotSpotter alerts which recorded likely-gun-related crime disposition.

---

<sup>40</sup> Of the incident dispositions recorded in relation to ShotSpotter alerts during the analysis period, OIG determined the following primary charge types to be likely indicative of gun-related crime: homicide, aggravated vehicular hijacking, armed robbery with a handgun/firearm, aggravated battery with a handgun/firearm, aggravated domestic battery with a handgun/firearm, aggravated assault with a handgun/firearm, reckless firearm discharge, unlawful use of a handgun/firearm, and use of metal piercing bullets. Not all statutes in the Illinois Criminal Code designate whether or not a violent crime was committed with a gun, and in others, the use of a gun is an aggravating factor, but other factors such as the age of the victim may cause the charge to be aggravated. OIG elected to categorize some dispositions as related to gun violence, notwithstanding that some percentage may not have involved a gun. For example, homicides may be committed with a weapon other than a gun, or without a weapon, but OIG cannot ascertain which did not involve a gun from the available OEMC data on ShotSpotter alert dispositions and therefore opted to include all homicides. In 2020, 692 of the 770 homicides (89.9%) that occurred in Chicago were fatal shootings. City of Chicago, "Violence Reduction Dashboard," accessed July 9, 2021, <https://www.chicago.gov/city/en/sites/vrd/home.html>. See also Appendix A.

FIGURE 4: SHOTSPOTTER ALERTS AND LIKELY GUN-RELATED CRIMINAL INCIDENT DISPOSITIONS



Source: OIG analysis.

A miscellaneous incident disposition was recorded for 36,039 of the ShotSpotter alert events occurring during the analysis period. The most common type of miscellaneous incident disposition recorded was “19-P,” listed in CPD’s Miscellaneous Incident Reporting Table as “Other Miscellaneous Incident-Other Police Service.”<sup>41</sup> The “19-P” disposition code was applied to 29,480 ShotSpotter alert events, representing 70.5% of all events with a recorded disposition. Among the 36,039 events with a miscellaneous incident disposition, OIG identified a total of 468 investigatory stops that shared an event number with a ShotSpotter alert, including 407 investigatory stops under ShotSpotter alert events closed with a “19-P” disposition.

A recent analysis of disposition codes associated with ShotSpotter alerts in Chicago by the MacArthur Justice Center (MJC) reaches a conclusion consistent with what is reported here: a large percentage of ShotSpotter alerts cannot be connected to any verifiable shooting incident. In May 2021, attorneys for MJC published findings from their analysis in an amicus brief filed on behalf of their clients—several local nonprofit organizations—in Cook County Circuit Court in support of a criminal defendant seeking a hearing on the reliability of ShotSpotter alerts. MJC analyzed OEMC data for ShotSpotter alert notifications between July 1, 2019 and April 14, 2021, and found that 85.6% of incidents in which CPD members respond to ShotSpotter alerts did not result in the completion of a criminal case report.<sup>42</sup>

<sup>41</sup> Chicago Police Department, “Miscellaneous Incident Reporting Table (CPD 11.484),” accessed June 25, 2021, <http://directives.chicagopolice.org/forms/CPD-11.484.pdf>.

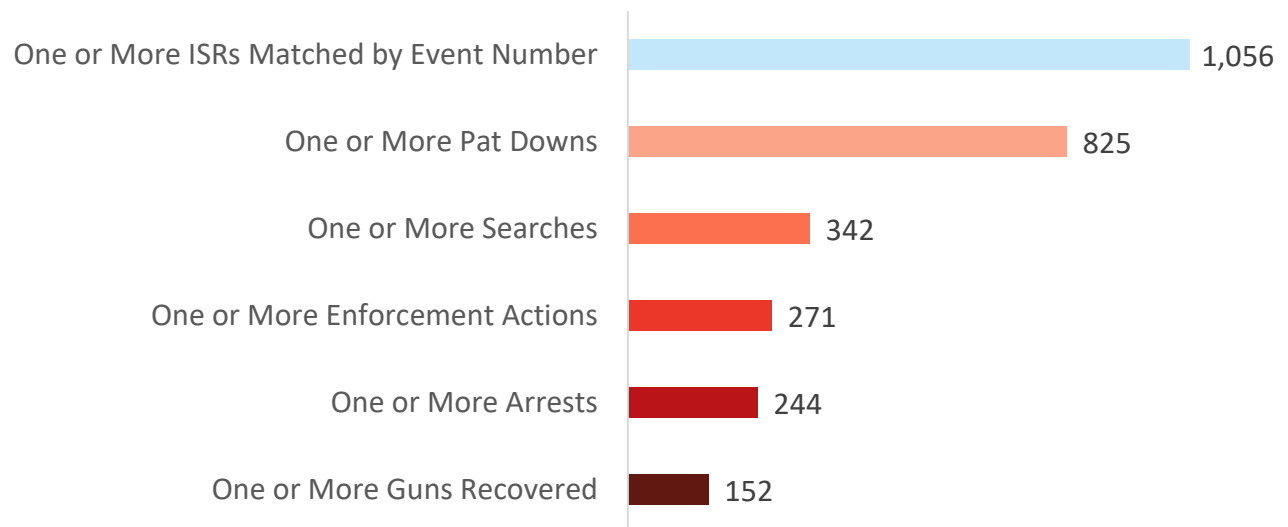
<sup>42</sup> MacArthur Justice Center, “ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study,” May 3, 2021, accessed June 25, 2021, <https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/>. The fullest description of MJC’s methodology for its analysis is provided in its amicus brief filed in the Circuit

## C. INVESTIGATORY STOP REPORTS ASSOCIATED WITH SHOTSPOTTER ALERT EVENT NUMBERS

Among the 50,176 ShotSpotter alerts between January 1, 2020 and May 31, 2021, a total of 1,056 were matched to one or more investigatory stop reports (ISRs) through a shared event number, representing 2.1% of all ShotSpotter alert event numbers. Because multiple people might be stopped at or near the scene of a ShotSpotter alert, the total number of people stopped is higher than the total number of event number matches. The total number of people stopped in these events is 1,740, and 422 ShotSpotter alert events match event numbers to multiple ISRs. This means that for 40% of ShotSpotter alerts that have event numbers that match ISRs, multiple people were stopped (422 out of 1,056 alerts). In this set, the maximum number of people stopped following a single ShotSpotter alert is seven.

Figure 5 displays law enforcement outcomes for the ShotSpotter alerts matched to ISRs via event number. The 1,056 matched event numbers indicate that investigatory stops are documented as associated with a specific ShotSpotter alert in only 2.1% of the 50,176 CPD dispatches to ShotSpotter alerts.<sup>43</sup> “Enforcement actions” include issuance of citations and ordinance violations in addition to arrests. According to the data collected in the associated ISRs, fewer than 2 in 10 investigatory stops following ShotSpotter alerts resulted in the recovery of a gun, with a high rate of 17.2% in the 11<sup>th</sup> District and a low of 4.7% in the 9<sup>th</sup> District.

**FIGURE 5: LAW ENFORCEMENT OUTCOMES DOCUMENTED ON INVESTIGATORY STOP REPORTS MATCHED TO CONFIRMED SHOTSPOTTER ALERTS**



Source: OIG analysis.

Court of Cook County. Motion for Leave to File Brief as Amici Curiae in Support of Defendant's Motion for a *Frye* Hearing, *State of Illinois v. Michael Williams*, at 15, (May 3, 2021) (20CR0988601).

<sup>43</sup> OIG identified an additional 1,366 ISRs under event numbers that did not match a confirmed ShotSpotter alert event number yet the narrative section of the ISR included a reference to ShotSpotter. OIG's review of these ISRs is detailed in Section IV-D.

Figure 5 only includes arrests and gun recoveries reported on ISRs with an event number matched to a ShotSpotter alert and therefore does not include any arrests or gun recoveries that were not associated with a documented investigatory stop recorded under a ShotSpotter alert event number. The outcomes reported in Figure 5 represent all law enforcement outcomes reported in ISRs bearing an event number that can be matched to a ShotSpotter alert.<sup>44</sup>

The following case studies present instances in which investigatory stops matched to specific ShotSpotter alerts by a shared event number resulted in arrests. In Case 1, the subject was arrested for a gun-related offense. In Case 2, the ShotSpotter alert provided the articulated reasonable suspicion for the investigatory stop, yet the subject was arrested for narcotics possession, not any gun-related charges.

#### CASE 1: GUN-RELATED ARREST FOLLOWING RESPONSE TO SHOTSPOTTER ALERT

ISR #005187115

IN SUMMARY R\O'S<sup>45</sup> WERE DISPATCHED TO A SHOT SPOTTER AT [location]. WHILE ENROUTE TO [location] R\O'S OBSERVED A WHITE CHEVROLET TRAVELING AT A HIGH RATE OF SPEED TURN WEST BOUND ONTO [street] FROM [street]. R\O'S KNOWING A SHOT SPOTTER HAD JUST BEEN TRIGGERED IN THE AREA INITIATED A STOP ON THE VEHICLE. R\O'S MET WITH THE [subject]. R\O'S ASKED THE DRIVER WHERE HE WAS COMING FROM TO WHICH HE RELATED THE HOUSE, R\O'S ASKED HIM HIS THE ADDRESS OF WHERE HE WAS COMING FROM AND HE RELATED [address]. [Address] IS A MULTI UNIT BUILDING WHICH IS ALSO CONNECTED TO [location] MEANING THE DRIVER WAS IN THE AREA OF THE SHOT SPOTTER. UPON LEARNING HIS NAME R\O'S RAN HIS NAME VIA LEADS<sup>46</sup> WHICH RETURNED HIM REVOKED IN IL. AT THIS TIME R\O'S ASKED THE DRIVER AND PASSENGER TO STEP OUT AND A SEARCH OF THE VEHICLE WAS CONDUCTED BY R\O [officer]. UPON SEARCHING THE VEHICLE R\O'S RECOVERED FROM THE DRIVERS SIDE FLOOR BOARD UNDER THE DRIVERS SEAT A LOADED BLUE STEEL 9MM SEMI-AUTOMATIC GLOCK 17 4.48IN BARREL SERIAL#[number]. THE BUTT OF THE GUN WAS PROTRUDING IN PLAIN VIEW FROM UNDER THE DRIVER SEAT WHICH INITIATED R\O'S SEARCH OF THE VEHICLE. AT THIS TIME R\O'S DETAINED THE DRIVER AND PLACED HIM IN THE BACK OF THE MARKED SQUAD CAR. MIRANDA WAS READ AT 0301HRS AND THE DRIVER CONSENTED TO QUESTIONS. THE DRIVER WAS ASKED IF HE HAD A VALID CONCEAL CARRY, WHICH HE RELATED HE DID NOT. THE DRIVER WAS ASKED IF HE HAD A FOID<sup>47</sup> CARD WHICH HE RELATED HE DID NOT. THE DRIVER WAS THEN ASKED IF HE WAS A CONVICTED FELON TO WHICH HE RELATED HE WAS. AT THIS TIME R\O'S INFORMED HIM HE WAS IN CUSTODY. THE OFFENDER WAS TRANSPORTED TO THE 006TH DISTRICT FOR FURTHER PROCESSING, THE VEHICLE WAS SUBJECT TO IMPOUNDMENT AS THE DRIVER WAS REVOKED. WHILE ENROUTE TO THE 006TH

<sup>44</sup> Investigatory stops that are related to ShotSpotter alerts may be documented under a separate event number without identification of the related ShotSpotter alert (or an investigatory stop might not be documented at all), guns might be recovered when no people are present at the scene, and arrests might be made (on gun-related charges or something else) without an investigatory stop taking place first.

<sup>45</sup> Reporting officers (R/Os).

<sup>46</sup> Law Enforcement Agencies Data System (LEADS).

<sup>47</sup> Firearm Owner's Identification (FOID).

DISTRICT STATION THE OFFENDER RELATED MULTIPLE TIMES HE WAS SORRY, AND THAT NO ONE GOT HURT. WHEN ASKED WHAT HE MEANT BY THAT THE OFFENDER GOT QUIET. FELONY REVIEW CONTACTED AND FELONY APPROVAL WAS GIVEN AT 0534HRS FOR UUW<sup>48</sup> BY A FELON.

## CASE 2: NARCOTICS ARREST FOLLOWING RESPONSE TO SHOTSPOTTER ALERT

ISR #004941914

EVENT#14451. BWC RECORDED INCIDENT. IN SUMMARY, A/O'S WERE RESPONDING TO A SHOT SPOTTER OF ONE ROUND ON THE SIDE OF THE BUILDING OF [address] A/O'S<sup>49</sup> OBSERVED [subject] (OFFENDER) WALK OUT FROM THE SIDE OF THE BUILDING AT [address]. A/O'S CONDUCTED AN INVESTIGATORY STOP OF THE OFFENDER AT ABOVE LOCATION. A/O OBSERVED A LARGE BULGE IN THE OFFENDER'S BACK POCKET AND FRONT POCKET. A/O'S THEN PERFORMED A PROTECTIVE PAT DOWN OF SUBJECT AND FOUND AN OPEN 24OZ CAN OF ``STEEL RESERVE`` ALCOHOL IN THE OFFENDER'S BACK POCKET (INV#[number]). A/O FOUND A SMALL GLASS BOTTLE THAT APPEARED TO HAVE BEEN FASHIONED INTO DRUG PARAPHERNALIA (INV#[number]) IN OFFENDERS FRONT POCKET. OFFENDER RELATED HE USES THIS OBJECT AS A PIPE TO SMOKE CRACK-COCAINE. A/O'S PLACED OFFENDER INTO CUSTODY AND PERFORMED A NARCOTICS SEARCH OF THE OFFENDER. A/O RECOVERED A SMALL FOLDED PIECE OF WHITE PAPER CONTAINING WHITE POWDER ROCK-LIKE SUBSTANCE SUSPECT CRACK COCAINE (INV#[number]). OFFENDER RELATED TO A/O'S THAT THE SUBSTANCE WAS A SMALL AMOUNT OF CRACK-COCAINE. OFFENDER TRANSPORTED TO 004TH DISTRICT BY [unit] FOR PROCESSING.

## D. INVESTIGATORY STOP REPORTS WITH “SPOTTER” AND/OR “SST” IN WRITTEN NARRATIVE

As described above in the methodology section, keyword searching in ISR narratives identified a substantial number of ISRs that are likely associated with ShotSpotter events, but keyword searching also captures ISRs that only include discussion of the general volume of ShotSpotter alerts in a given area and do not refer to specific alerts.

A total of 1,366 investigatory stop reports (ISRs) completed between January 1, 2020 and May 31, 2021, include the keywords “SPOTTER” or “SST” but did not have an event number match to a confirmed ShotSpotter alert.<sup>50</sup> OIG examined in detail the narratives from a random sample of 72 of these ISRs—one report randomly selected from each CPD District confirmed to have

<sup>48</sup> Unlawful Use of a Weapon (UUW).

<sup>49</sup> Arresting officers (A/Os).

<sup>50</sup> OIG included the keyword “SST” in its search methodology to increase the chances of capturing any ISR that could be definitively linked to a ShotSpotter alert, although it made little difference to the number of search results returned. In the analysis period, only 32 ISR narratives contained the text string “SST.” In most cases, “SST” was actually used as an abbreviation for “ShotSpotter” or “ShotSpotter Technology.” A few of the results were false positives: “asisst” [sic] appeared in four ISR narratives; “arresstee” [sic] and “asst” each appeared in three narratives; and “invesstigation” [sic] appeared in two narratives.

ShotSpotter sensors for each quarter during the analysis period—and found that many stops recorded under a different event number did reference the ShotSpotter alert event number in their ISR narrative. Among the 72 ISR narratives OIG reviewed, 13 ISRs (18.1%) identified a ShotSpotter alert by its correct event number as the prompt for the investigatory stop recorded under a separate event number.

In reviewing ISR narratives for mentions of ShotSpotter alerts, OIG also identified 10 ISRs (13.9%) in which reporting officers referred to the *aggregate results of the ShotSpotter system* as informing their decision to initiate a stop or their course of action during the stop, even when they were not responding to a specific ShotSpotter alert. For example, some officers during the reporting period identified the fact of being in an area known to have frequent ShotSpotter alerts as an element of the reasonable suspicion required to justify the stop.<sup>51</sup> Other officers reported conducting “protective pat downs” following a stop because they knew themselves to be in areas where ShotSpotter alerts were frequent.

These cases suggest that the exercise of matching individual ShotSpotter alerts to subsequent associated investigatory stops alone may underrepresent the extent to which the introduction of ShotSpotter technology in Chicago has changed the way CPD members perceive and interact with individuals present in areas where ShotSpotter alerts are frequent. At least some officers, at least some of the time, are relying on ShotSpotter results in the aggregate to provide an additional rationale to initiate stop or to conduct a pat down once a stop has been initiated.

Below, OIG reproduces in full the narratives from three ISRs that cite the frequency of ShotSpotter alerts in a given area as an element of the reasonable suspicion upon which an investigatory stop is predicated. Of the ten stops partially predicated on the high volume of ShotSpotter alerts in the area, OIG was able to identify in its sample only one instance in which the stop led to an arrest, described below as Case 3. In Cases 4 and 5, the investigatory stops predicated, in part, on reasonable suspicion due to the frequency of ShotSpotter alerts in the area did not produce any evidence of the subject’s involvement in gun-related crime. While

---

<sup>51</sup> In *Terry v. Ohio*, 392 U.S. 1 (1968), the United States Supreme Court established that police may temporarily stop and detain a person if the police have “reasonable, articulable suspicion that criminal activity is afoot.” *Illinois v. Wardlow*, 528 U.S. 119, 124 (2000). As the Supreme Court has described, “[a]n individual’s presence in an area of expected criminal activity, standing alone, is not enough to support a reasonable . . . suspicion that a person is committing a crime.” *Id.* However, “officers are not required to ignore the relevant characteristics of a location in determining whether the circumstances are sufficiently suspicious to warrant further investigation” and, thus, “the fact that the stop occurred in a ‘high crime area’ [is] among the relevant contextual consideration in a *Terry* analysis.” *Id.* (quoting *Adams v. Williams*, 407 U.S. 143, 144, 147-48 (1972)). The Illinois Compiled Statutes codify the holding in *Terry* at 725 ILCS 5/107-14 and 725 ILCS 5/108-1.01. CPD’s directives state, “Reasonable Articulable Suspicion is an objective legal standard that is less than probable cause but more substantial than a hunch or general suspicion. Reasonable Articulable Suspicion depends on the totality of the circumstances which the sworn member observes and the reasonable inferences that are drawn based on the sworn member’s training and experience. Reasonable Articulable Suspicion can result from a combination of particular facts, which may appear innocuous in and of themselves, but taken together amount to reasonable suspicion.” Chicago Police Department, “Special Order S04-13-09: Investigatory Stop System,” July 10, 2017, accessed June 14, 2021, <http://directives.chicagopolice.org/directives/data/a7a57b99-151b6927-49f15-1b69-2c32e99868b316b0.pdf?hl=true>.

these cases alone do not support inferences or generalizations about the likelihood of any particular outcome, they do demonstrate in concrete detail how perceptions of ShotSpotter alert frequency may impact policing behavior.

In Case 3, the reporting officer cites “multiple bonafide Shot Spotter events in the area” where they observed the subject and initiated the stop. In Case 4, the reporting officer describes being “on patrol in an area known for its high volume of Shot Spotter notifications” and describes “perform[ing] a protective pat down based on the known violent area and [the subject’s] suspicious behavior.” In Case 5, the reporting officer states that “due to many Shot Spotter alerts and gang activity in the proximity to this location, [reporting officers] reasonably believed [a large weighted object in the subject’s front hoodie pocket] to possibly be a firearm.”

### CASE 3: OFFICER CITING FREQUENCY OF SHOTSPOTTER ALERTS AS AN ELEMENT OF REASONABLE SUSPICION FOR A STOP LEADING TO AN ARREST

ISR #008994781

EVENT#08135 BWC IN USE. R/O'S WERE ON PATROL IN A HIGH CRIME AREA WITH MULTIPLE ONGOING GANG AND NARCOTIC CONFLICTS, SPECIFICALLY AN ONGOING GANG WAR BETWEEN [gang] AND [gang]/ ALSO, MULTIPLE BONAFIDE SHOT SPOTTER EVENTS IN THE AREA. THIS AREA IS PRIORITY ZONE #2 IN THE 007TH DISTRICT. R/O'S TURNED S/B ON [street] FROM [street]. R/O'S OBSERVED WHO THE R/O'S NOW KNOW AS [subject] LOOK IN R/O'S DIRECTION, GRAB HIS WAISTBAND, AND BEGAN TO SKIP TOWARDS THE FRONT DOOR OF THE RESIDENCE [address], BEFORE FULL SPRINTING INTO THE RESIDENCE. [subject] THEN ENTERED SAID RESIDENCE. R/O'S THEN BEGAN TO TOUR THE AREA IN THE WEST ALLEY ON THE [location] AND [subject] (OFFENDER) THEN EMERGED FROM THE GANGWAY AT [address]. R/O [officer] THEN GAVE CHASE AND [subject] (OFFENDER) CONTINUED TO FLEE. R/O [officer] CONTINUED CHASING OFFENDER, AT WHICH TIME [subject] (OFFENDER) JUMPED A FENCE AND A BLACK FIREARM FELL FROM HIS PERSON. [subject] (OFFENDER) THEN PICKED SAID FIREARM BACK UP AND CONTINUED TO RUN. P.O [officer] GAVE A DIRECTION OF FLIGHT VIA OEMC RADIO AND R/O [officer] WAS ABLE TO CUT OFF AND OBSERVE [subject] (OFFENDER) THROW A BLACK FIREARM ONTO THE ROOF AT [address]. R/O [officer] WAS ABLE TO PLACE [subject] (OFFENDER) INTO CUSTODY WITHOUT INCIDENT. R/O'S REQUESTED CFD TRUCK 41 TO RETRIEVE THE FIREARM FROM THE ROOF. FIREARM RECOVERY DOCUMENTED ON BWC. R/O'S RECOVERED 1 LOADED BLUE STEEL MASTERPIECE ARMS MPA DEFENDER 9MM WITH A 4.5 INCH BARRELL YIELDING SERIAL #[number], ATTACHED WAS A BLACK HIGH CAPACITY MAGAZINE WITH MULTIPLE LIVE ROUNDS (INV#[number]). R/O'S THEN TRANSPORTED ARRESTEE TO THE 007TH DISTRICT FOR FURTHER PROCESSING. A SUBSEQUENT NAME CHECK REVEALED THE ARRESTEE DOES NOT POSSESS A CCL<sup>52</sup> NOR FOID. NAME CHECK CLEAR. ARRESTEE IS A SELF-ADMITTED [gang]. NOT A FELON. NO WANTS/WARRANTS/IA'S. GUN DESK NOTIFIED WEAPON IS CLEAR NOT REGISTERED PER [officer].

<sup>52</sup> Concealed Carry License (CCL).

#### CASE 4: OFFICER CITING FREQUENCY OF SHOTSPOTTER ALERTS AS AN ELEMENT OF REASONABLE SUSPICION FOR A STOP

ISR #010151171

EVENT # 13516. BWC INCIDENT. R/O'S ON PATROL IN AN AREA KNOWN FOR ITS HIGH VOLUME OF SHOT SPOTTER NOTIFICATIONS AND PERSON WITH A GUN CALL. IN THAT, WHILE ON PATROL R/O'S OBSERVED THE ABOVE STATED VEHICLE PARKED AT THE ABOVE STATED ADDRESS MORE THAN 12 INCHES FROM THE CURB WHICH IS A VIOLATION CODE OF MCC 9-64-020(A). R/O UTILIZED HIS UNMARKED POLICE VEHICLE SPOT LIGHT AND SHINNED [sic] IT TOWARDS THE WINDSHIELD OF THE ABOVE STATED VEHICLE. IT WAS AT THIS TIME, R/O OBSERVED A M/1 NKA ABOVE SUBJECT SEATED IN THE FRONT PASSENGER SEAT. R/O THAN NOTICED THE ABOVE SUBJECT REACH TOWARDS THE CENTER OF HIS WAIST LINE AND BEGAN TO ADJUST THE TOP PART OF HIS PANTS. IN ADDITION, R/O THEN OBSERVED THE ABOVE SUBJECT BEND HIS UPPER BODY FORWARD CAUSING BOTH OF HIS ARMS TO BE NON VISIBLE. R/O EXITED HIS POLICE VEHICLE AND APPROACHED THE PARKED VEHICLE FROM THE PASSENGER SIDE AND BEGAN TO COMMUNICATE WITH THE ABOVE SUBJECT. R/O REQUESTED FROM THE ABOVE SUBJECT TO PROVIDE PROOF OF IDENTIFICATION AT WHICH TIME HE FAILED TO PROVIDE ONE. WHILE COMMUNICATION WITH THE ABOVE SUBJECT, R/O SMELLED AN ODOR OF ALCOHOLIC BEVERAGE EMITTING FROM THE VEHICLE AND NOTICED THE ABOVE SUBJECTS HANDS TO TREMBLE. BASED ON R/O'S EXPERIENCE IN NUMEROUS WEAPONS VIOLATION ARRESTS, R/O REASONABLY BELIEVED THE ABOVE SUBJECT WAS IN POSSESSION OF A FIREARM. R/O REQUESTED THE ABOVE SUBJECT TO EXIT THE VEHICLE FOR FURTHER INVESTIGATION. UPON DOING SO, R/O PERFORMED A PROTECTIVE PAT DOWN BASED ON THE KNOWN VIOLENT AREA AND ABOVE SUBJECTS SUSPICIOUS BEHAVIOR [ADJUSTING WAIST LINE, BENDING UPPER BODY FORWARD, AND TREMBLING HANDS]. NEGATIVE RESULTS OF ANY WEAPONS. THE ABOVE SUBJECT THEN RELATED TO R/O THAT THERE WAS A BOTTLE OF ALCOHOL IN THE VEHICLE AND THAT HE HAD BEEN DRINKING. R/O'S PERFORMED A SEARCH OF THE VEHICLE FOR THE POSSIBILITY OF ANY OPEN CONTAINERS OF ALCOHOL IN THE VEHICLE. R/O'S DISCOVERED A BOTTLE OF COURVOISIER ALCOHOLIC BEVERAGE WITH A BROKEN SEAL LOCATED ON THE FLOOR BOARD IN FRONT OF THE REAR PASSENGER SEAT. NAME CHECK OF ABOVE SUBJECT CLEAR. ABOVE SUBJECT WAS GIVEN A VERBAL WARNING AND WAS RELEASED WITHOUT INCIDENT. ABOVE SUBJECT REFUSED AN ISR RECEIPT.

#### CASE 5: OFFICER CITING FREQUENCY OF SHOTSPOTTER ALERTS AS AN ELEMENT OF REASONABLE SUSPICION FOR A PAT DOWN

ISR #011102767

EVENT 02301. BWC ACTIVE. IN SUMMARY, R/OS WERE ON ROUTINE PATROL DRIVING NORTHBOUND ON [street] APPROACHING [street] WHEN R/OS SAW LISTED SUBJECT CROSSING STREET WALKING SOUTHBOUND ON [street]. AT THIS TIME, LISTED SUBJECT GAVE THE MIDDLE FINGER TO R/OS AND YELLING OBSCENITIES AT R/OS. R/OS THEN NOTICED A LARGE WEIGHTED OBJECT IN HIS FRONT HOODIE POCKET. DUE TO MANY SHOT SPOTTER ALERTS AND GANG ACTIVITY IN THE PROXIMITY TO THIS LOCATION, R/OS REASONABLY BELIEVED THIS WEIGHT OBJECT TO POSSIBLY BE A FIREARM. R/OS THEN CONDUCTED A STREET STOP AT THE LISTED LOCATION. R/OS THEN CONDUCTED A PAT DOWN WITH

NEGATIVE FINDINGS OF WEAPONS. SUBJECT [sic] HAD A BAG AROUND HIS SHOULDER, AND R/OS ASKED IF THEY COULD LOOK INSIDE TO WHICH SUBJECT GAVE PERMISSION. R/OS SEARCHED THE BAG AND FOUND A SMALL SEALED, ODORLESS, CHILDPROOF CONTAINER WITH SUSPECT CANABIS INSIDE IT. SUBJECT GAVE R/OS HIS IL ID CARD AND R/OS RAN NAME THROUGH [sic] LEADS AND CLEAR,<sup>53</sup> WITH A FINDING OF NO WANTS OR WARRANTS AT THIS TIME. THROUGHOUT THIS EVENT, SUBJECT WAS VERY VERBALLY AGGRESSIVE BY CONTINUOUSLY YELLING AT R/OS AND CALLING R/OS OBSCENITIES. SUBJECT REFUSED AN ISR RECEIPT AND THE STOP WAS CONCLUDED WITHOUT INCIDENT.

## V. CONCLUSION

Through this descriptive report, OIG aims to provide the public and City government officials with clear and accurate information regarding CPD's use of ShotSpotter technology.

From quantitative analysis of ShotSpotter data and other records, OIG concludes that CPD responses to ShotSpotter alerts rarely produce evidence of a gun-related crime, rarely give rise to investigatory stops, and even less frequently lead to the recovery of gun crime-related evidence during an investigatory stop. If this result is attributable in part to missing or non-matched records of investigatory stops that *did* take place as a direct consequence of a ShotSpotter alert, CPD's record-keeping practices are obstructing a meaningful analysis of the effectiveness of the technology. Additionally, from qualitative review of ISR narratives, OIG found evidence that CPD members' generalized perceptions of the frequency of ShotSpotter alerts in a given area may be substantively changing policing behavior.

The operational value of ShotSpotter is ultimately a question of relative costs and benefits. There may be a law enforcement benefit in the use of ShotSpotter alert information to dispatch CPD members quickly to scenes where there is some evidence available that shots may have been fired. On the other hand, there are real and potential costs associated with use of the system, including financial resources, the time and attention of CPD members, and the risk that CPD members dispatched as a result of a ShotSpotter alert may respond to incidents with little contextual information about what they will find there—raising the specter of poorly informed decision-making by responding members. For this weighing of costs and benefits to accrue in favor of the continued use of ShotSpotter technology, CPD and the City would be well-served by being able to clearly demonstrate its law enforcement value. Such a value is not clearly demonstrated by presently available data.

Because the ability to match ShotSpotter events to other police records, including ISRs, is so limited, it may not be possible at present to reach a well-informed determination as to whether ShotSpotter is a worthwhile operational investment as an effective law enforcement tool for the City and CPD. Better data on law enforcement outcomes from ShotSpotter alerts would be valuable to support the City's future assessments of whether to further extend, amend, or discontinue its contractual relationship with ShotSpotter.

---

<sup>53</sup> Citizen Law Enforcement Analysis and Reporting (CLEAR).

## APPENDIX A: SHOTSPOTTER ALERT INCIDENT DISPOSITIONS

The following table lists the disposition code and abbreviated description for 41,830 ShotSpotter alert event numbers dispatched between January 1, 2020 and May 31, 2021, for which a disposition was recorded in the OEMC database.

For the full extent of available incident dispositions and corresponding full descriptions, see the Chicago Police Department's Incident Reporting Guide ([CPD 63.451](#)) and the Chicago Police Department's Miscellaneous Incident Reporting Table ([CPD 11.484](#)).

DISPOSITION CODE AND DESCRIPTION	#	%
<b>CRIMINAL INCIDENT DISPOSITIONS</b>	<b>5,504</b>	<b>13.2%</b>
<b>GUN-RELATED CRIMINAL DISPOSITIONS<sup>54</sup></b>	<b>4,556</b>	<b>10.9%</b>
1477 - WEAPONS VIOLATION - RECKLESS FIREARM DISCHARGE	1,622	3.9%
041A - BATTERY - AGGRAVATED: HANDGUN	1,131	2.7%
051A - ASSAULT - AGGRAVATED: HANDGUN	434	1.0%
141A - WEAPONS VIOLATION - UNLAWFUL USE HANDGUN	416	1.0%
141B - WEAPONS VIOLATION - UNLAWFUL USE OTHER FIREARM	380	0.9%
110 - HOMICIDE - FIRST DEGREE MURDER	242	0.6%
143A - WEAPONS VIOLATION - UNLAWFUL POSS OF HANDGUN	239	0.6%
031A - ROBBERY - ARMED: HANDGUN	23	0.1%
051B - ASSAULT - AGGRAVATED: OTHER FIREARM	11	0.0%
033A - ROBBERY - ATTEMPT: ARMED - HANDGUN	10	0.0%
143B - WEAPONS VIOLATION - UNLAWFUL POSS OTHER FIREARM	9	0.0%
550 - ASSAULT - AGGRAVATED PO: HANDGUN	7	0.0%
041B - BATTERY - AGGRAVATED: OTHER FIREARM	7	0.0%
488 - BATTERY - AGGRAVATED DOMESTIC BATTERY: HANDGUN	6	0.0%
326 - ROBBERY - AGGRAVATED VEHICULAR HIJACKING	6	0.0%
555 - ASSAULT - AGG PRO.EMP: HANDGUN	4	0.0%
1460 - WEAPONS VIOLATION - POSS FIREARM/AMMO:NO FOID CARD	3	0.0%
650 - BURGLARY - HOME INVASION	2	0.0%
031B - ROBBERY - ARMED: OTHER FIREARM	1	0.0%
1476 - WEAPONS VIOLATION - USE OF METAL PIERCING BULLETS	1	0.0%
143C - WEAPONS VIOLATION - UNLAWFUL POSS AMMUNITION	1	0.0%
450 - BATTERY - AGGRAVATED PO: HANDGUN	1	0.0%

<sup>54</sup> OIG determined these primary charge types to be likely indicative of gun violence or other gun-related crime, acknowledging that there is not a perfect correspondence between all of these specific charge types and use of a gun (for example, as noted above in Section IV.B, many but not all homicides in Chicago are perpetrated with guns).

<b>OTHER CRIMINAL DISPOSITIONS<sup>55</sup></b>	<b>948</b>	<b>2.3%</b>
1320 - CRIMINAL DAMAGE - TO VEHICLE	403	1.0%
1310 - CRIMINAL DAMAGE - TO PROPERTY	363	0.9%
1365 - CRIMINAL TRESPASS - TO RESIDENCE	17	0.0%
2093 - NARCOTICS - FOUND SUSPECT NARCOTICS	11	0.0%
486 - BATTERY - DOMESTIC BATTERY SIMPLE	9	0.0%
560 - ASSAULT - SIMPLE	8	0.0%
454 - BATTERY - AGG PO HANDS NO/MIN INJURY	7	0.0%
460 - BATTERY - SIMPLE	7	0.0%
554 - ASSAULT - AGG PO HANDS NO/MIN INJURY	6	0.0%
530 - ASSAULT - AGGRAVATED: OTHER DANG WEAPON	6	0.0%
1330 - CRIMINAL TRESPASS - TO LAND	6	0.0%
610 - BURGLARY - FORCIBLE ENTRY	6	0.0%
470 - PUBLIC PEACE VIOLATION - RECKLESS CONDUCT	5	0.0%
2027 - NARCOTICS - POSS: CRACK	5	0.0%
1812 - NARCOTICS - POSS: CANNABIS MORE THAN 30GMS	4	0.0%
141C - WEAPONS VIOLATION - UNLAWFUL USE OTHER DANG WEAPON	4	0.0%
430 - BATTERY - AGGRAVATED: OTHER DANG WEAPON	4	0.0%
2022 - NARCOTICS - POSS: COCAINE	4	0.0%
3710 - INTERFERENCE WITH PUBLIC OFFICER - RESIST/OBSTRUCT/DISARM	4	0.0%
2024 - NARCOTICS - POSS: HEROIN(WHITE)	3	0.0%
5007 - OTHER OFFENSE - OTHER WEAPONS VIOLATION	3	0.0%
320 - ROBBERY - STRONGARM - NO WEAPON	3	0.0%
630 - BURGLARY - ATTEMPT FORCIBLE ENTRY	2	0.0%
920 - MOTOR VEHICLE THEFT - ATT: AUTOMOBILE	2	0.0%
910 - MOTOR VEHICLE THEFT - AUTOMOBILE	2	0.0%
2028 - NARCOTICS - POSS: SYNTHETIC DRUGS	2	0.0%
5111 - OTHER OFFENSE - GUN OFFENDER: ANNUAL REGISTRATION*	2	0.0%
502P - OTHER OFFENSE - FALSE/STOLEN/ALTERED TRP	2	0.0%

<sup>55</sup> OIG's classification of "gun-related criminal disposition" intends to identify criminal offenses likely to indicate the *use or unlawful possession* of a handgun or other firearm and does not extend to offenses based on offender registry status or violations of concealed carry regulations. Additionally, OIG excluded officer-involved shooting dispositions, as the determination regarding whether such incidents are justified, not justified and/or criminal is not immediately determined at the time of occurrence. Dispositions marked with an asterisk (\*) are identified as gun-related but not within OIG's classification of "gun-related criminal disposition" for the purposes of this report. The full list of offenses involving guns excluded from OIG's classification as a "gun-related criminal disposition" are: 1479 - CONCEALED CARRY LICENSE VIOLATION - ARMED UNDER THE INFLUENCE, 1480 - CONCEALED CARRY LICENSE VIOLATION - OTHER, 5072 - WEAPON / FIREARM TURN IN, 5110 - OTHER OFFENSE - GUN OFFENDER: DUTY TO REGISTER, 5111 - OTHER OFFENSE - GUN OFFENDER: ANNUAL REGISTRATION, 5140 - OFFICER-INVOLVED SHOOTING - GUNSHOT INJURY / NOT FATAL, 5141 - OFFICER-INVOLVED SHOOTING - NO INJURY.

325 - ROBBERY - VEHICULAR HIJACKING	2	0.0%
620 - BURGLARY - UNLAWFUL ENTRY	2	0.0%
1020 - ARSON - BY FIRE	2	0.0%
820 - THEFT - \$500 AND UNDER	2	0.0%
1360 - CRIMINAL TRESPASS - TO VEHICLE	2	0.0%
1090 - ARSON - ATTEMPT ARSON	2	0.0%
461 - BATTERY - AGG PO HANDS ETC SERIOUS INJ	2	0.0%
3730 - INTERFERENCE WITH PUBLIC OFFICER - OBSTRUCTING JUSTICE	1	0.0%
1822 - NARCOTICS - MANU/DEL: CANNABIS OVER 10 GMS	1	0.0%
1710 - OFFENSE INVOLVING CHILDREN - ENDANGERING LIFE/HEALTH CHILD	1	0.0%
1340 - CRIMINAL DAMAGE - TO STATE SUP PROP	1	0.0%
2025 - NARCOTICS - POSS: HALLUCINOGENS	1	0.0%
4386 - OTHER OFFENSE - VIOLATION OF CIVIL NO CONTACT ORDER	1	0.0%
312 - ROBBERY - ARMED: KNIFE/CUTTING INSTRUMENT	1	0.0%
4387 - OTHER OFFENSE - VIOLATE ORDER OF PROTECTION	1	0.0%
1305 - CRIMINAL DAMAGE - CRIMINAL DEFACEMENT	1	0.0%
453 - BATTERY - AGGRAVATED PO: OTHER DANG WEAP	1	0.0%
581 - STALKING - AGGRAVATED	1	0.0%
1025 - ARSON - AGGRAVATED	1	0.0%
810 - THEFT - OVER \$500	1	0.0%
2092 - NARCOTICS - SOLICIT NARCOTICS ON PUBLICWAY	1	0.0%
5110 - OTHER OFFENSE - GUN OFFENDER: DUTY TO REGISTER*	1	0.0%
1350 - CRIMINAL TRESPASS - TO STATE SUP LAND	1	0.0%
520 - ASSAULT - AGGRAVATED: KNIFE/CUTTING INSTR	1	0.0%
2021 - NARCOTICS - POSS: BARBITUATES	1	0.0%
545 - ASSAULT - PRO EMP HANDS NO/MIN INJURY	1	0.0%
1480 - CONCEALED CARRY LICENSE VIOLATION - OTHER*	1	0.0%
558 - ASSAULT - AGG PRO.EMP: OTHER DANG WEAPON	1	0.0%
497 - BATTERY - AGGRAVATED DOMESTIC BATTERY: OTHER DANG WEAPON	1	0.0%
580 - STALKING - SIMPLE	1	0.0%
5001 - OTHER OFFENSE - OTHER CRIME INVOLVING PROPERTY	1	0.0%
2012 - NARCOTICS - MANU/DELIVER: COCAINE	1	0.0%
2820 - OTHER OFFENSE - TELEPHONE THREAT	1	0.0%
2026 - NARCOTICS - POSS: PCP	1	0.0%
5011 - OTHER OFFENSE - LICENSE VIOLATION	1	0.0%
330 - ROBBERY - AGGRAVATED	1	0.0%
1345 - CRIMINAL DAMAGE - TO CITY OF CHICAGO PROPERTY	1	0.0%

501A - OTHER OFFENSE - ANIMAL ABUSE/NEGLECT	1	0.0%
420 - BATTERY - AGGRAVATED: KNIFE/CUTTING INSTR	1	0.0%
2826 - OTHER OFFENSE - HARASSMENT BY ELECTRONIC MEANS	1	0.0%
1479 - CONCEALED CARRY LICENSE VIOLATION - ARMED WHILE UNDER THE INFLUENCE*	1	0.0%
<b>NON-CRIMINAL INCIDENTS</b>	<b>287</b>	<b>0.7%</b>
<b>NON-CRIMINAL GUN-RELATED DISPOSITIONS</b>	<b>1</b>	<b>0.0%</b>
151 - HOMICIDE - JUSTIFIABLE HOMICIDE	1	0.0%
<b>OTHER NON-CRIMINAL DISPOSITIONS</b>	<b>286</b>	<b>0.7%</b>
99B - TRAFFIC CRASH - INJURY/DEATH	111	0.3%
5071 - FOUND PROPERTY	71	0.2%
99A - TRAFFIC CRASH - NO INJURY/DRIVE AWAY	54	0.1%
940 - STOLEN VEHICLE RECOVERED - AUTO STOLEN OUTSIDE CHICAGO	13	0.0%
5081 - NON-CRIMINAL INCIDENT - PROPERTY	6	0.0%
5080 - NON-CRIMINAL INCIDENT - PERSONS	6	0.0%
5091 - FIRE DAMAGE - DAMAGE TO REAL PROPERTY/NON-CRIMINAL	4	0.0%
9999 - CANCELLATION OF RD NUMBER - RD NUMBER OBTAINED IN ERROR	4	0.0%
5082 - ORDER OF PROTECTION NOTIFICATION - NOT PREVIOUSLY SERVED/NO OTHER CRIMINAL ACT	4	0.0%
5090 - FIRE DAMAGE - DAMAGE TO PERSON PROPERTY/NON-CRIMINAL	3	0.0%
6055 - FOUND PERSON - INCAPACITATED PERSON FOUND	2	0.0%
5072 - WEAPON/FIREARM TURN IN*	2	0.0%
5088 - INJURY TO CITY EMPLOYEE - NON-CRIMINAL/NON-TRAFFIC	1	0.0%
5086Z - ATTEMPT SUICIDE - NOT IN POLICE CUSTODY	1	0.0%
5085Z - SUICIDE - NOT IN POLICE CUSTODY	1	0.0%
5141 - OFFICER-INVOLVED SHOOTING - NO INJURY*	1	0.0%
5079Z - MENTAL HEALTH TRANSPORT	1	0.0%
5140 - OFFICER-INVOLVED SHOOTING - GUNSHOT INJURY/NON-FATAL*	1	0.0%
<b>MISCELLANEOUS INCIDENT DISPOSITIONS</b>	<b>36,039</b>	<b>86.2%</b>
19P - OTHER MISC INC - OTHER POLICE SERVICE	29,480	70.5%
19B - OTHER MISC INC - NO PERSON CAN BE FOUND	4,987	11.9%
19A - OTHER MISC INC - NOT BONA FIDE INCIDENT	585	1.4%
5P - DISTURBANCE - OTHER - OTHER POLICE SERVICE	216	0.5%
5B - DISTURBANCE - OTHER - NO PERSON CAN BE FOUND	189	0.5%
4P - DISTURBANCE - NOISE - OTHER POLICE SERVICE	136	0.3%
19E - OTHER MISC INC - PERPETRATOR GONE ON POLICE ARRIVAL	61	0.1%
4B - DISTURBANCE - NOISE - NO PERSON CAN BE FOUND	39	0.1%
11P - SUSPICIOUS AUTO/PERSONS - OTHER POLICE SERVICE	38	0.1%

1P - DISTURBANCE - DOMESTIC - OTHER POLICE SERVICE	37	0.1%
19D - OTHER MISC INC - NO POLICE SERVICE NECESSARY	32	0.1%
11B - SUSPICIOUS AUTO/PERSONS - NO PERSON CAN BE FOUND	30	0.1%
14P - AUTO/BURGLAR/HOLDUP ALARM - OTHER POLICE SERVICE	21	0.1%
1B - DISTURBANCE - DOMESTIC - NO PERSON CAN BE FOUND	15	0.0%
18B - TRAFFIC ACCIDENT - NO PERSON CAN BE FOUND	13	0.0%
5E - DISTURBANCE - OTHER - PERPETRATOR GONE ON POLICE ARRIVAL	11	0.0%
18P - TRAFFIC ACCIDENT - OTHER POLICE SERVICE	9	0.0%
5A - DISTURBANCE - OTHER - NOT BONA FIDE INCIDENT	9	0.0%
19C - OTHER MISC INC - NO SUCH ADDRESS	9	0.0%
19PZ - OTHER MISC INC - OTHER POLICE SERVICE	9	0.0%
5D - DISTURBANCE - OTHER - NO POLICE SERVICE NECESSARY	8	0.0%
10P - ANIMAL BITE - OTHER POLICE SERVICE	8	0.0%
9P - PERSON DOWN - OTHER POLICE SERVICE	8	0.0%
19O - OTHER MISC INC - ADVISED LEGAL HELP	8	0.0%
19L - OTHER MISC INC - INFORMATION REPORT SUBMITTED	7	0.0%
19H - OTHER MISC INC - ADVISED TO RECONTACT POLICE IF REPEATED/RETURNED	7	0.0%
19K - OTHER MISC INC - TAKEN TO DISTRICT STATION	7	0.0%
19F - OTHER MISC INC - PEACE RESTORED	5	0.0%
19R - OTHER MISC INC - ARREST MADE	5	0.0%
5F - DISTURBANCE - OTHER - PEACE RESTORED	4	0.0%
1A - DISTURBANCE - DOMESTIC - NOT BONA FIDE INCIDENT	4	0.0%
11E - SUSPICIOUS AUTO/PERSONS - PERPETRATOR GONE ON POLICE ARRIVAL	3	0.0%
4A - DISTURBANCE - NOISE - NOT BONA FIDE INCIDENT	3	0.0%
5L - DISTURBANCE - OTHER - INFORMATION REPORT SUBMITTED	2	0.0%
19M - OTHER MISC INC - ISSUED TRAFFIC CITATION	2	0.0%
6B - ILLEGAL PARKING - NO PERSON CAN BE FOUND	2	0.0%
1F - DISTURBANCE - DOMESTIC - PEACE RESTORED	2	0.0%
19N - OTHER MISC INC - ISSUED ORDINANCE COMPLAINT	2	0.0%
2P - DISTURBANCE - TEENS - OTHER POLICE SERVICE	2	0.0%
16P - FIRE - OTHER POLICE SERVICE	2	0.0%
4D - DISTURBANCE - NOISE - NO POLICE SERVICE NECESSARY	2	0.0%
11A - SUSPICIOUS AUTO/PERSONS - NOT BONA FIDE INCIDENT	2	0.0%
4E - DISTURBANCE - NOISE - PERPETRATOR GONE ON POLICE ARRIVAL	2	0.0%
19BZ - OTHER MISC INC - NO PERSON CAN BE FOUND	2	0.0%
5N - DISTURBANCE - OTHER - ISSUED ORDINANCE COMPLAINT	1	0.0%

7I - SICK REMOVAL - REMOVED TO HOSPITAL OR DETOXIFICATION FACILITY	1	0.0%
3P - DISTURBANCE - DRUNK - OTHER POLICE SERVICE	1	0.0%
1E - DISTURBANCE - DOMESTIC - PERPETRATOR GONE ON POLICE ARRIVAL	1	0.0%
1E - DISTURBANCE - DOMESTIC - PERPETRATOR GONE ON POLICE ARRIVAL	1	0.0%
19AZ - OTHER MISC INC - NOT BONA FIDE INCIDENT	1	0.0%
17P - ESCORT - OTHER POLICE SERVICE	1	0.0%
5O - DISTURBANCE - OTHER - ADVISED LEGAL HELP	1	0.0%
15B - INHALATOR - NO PERSON CAN BE FOUND	1	0.0%
4M - DISTURBANCE - NOISE - ISSUED TRAFFIC CITATION	1	0.0%
13P - LOST PERSON FOUND - OTHER POLICE SERVICE	1	0.0%
9B - PERSON DOWN - NO PERSON CAN BE FOUND	1	0.0%
12E - CITIZEN CALL FOR HELP - PERPETRATOR GONE ON POLICE ARRIVAL	1	0.0%
11F - SUSPICIOUS AUTO / PERSONS - PEACE RESTORED	1	0.0%

The City of Chicago Office of Inspector General (OIG) is an independent, nonpartisan oversight agency whose mission is to promote economy, efficiency, effectiveness, and integrity in the administration of programs and operations of City government. OIG achieves this mission through,

- administrative and criminal investigations by its Investigations Section;
- performance audits of City programs and operations by its Audit and Program Review Section;
- inspections, evaluations and reviews of City police and police accountability programs, operations, and policies by its Public Safety Section; and
- compliance audit and monitoring of City hiring and human resources activities by its Compliance Section.

From these activities, OIG issues reports of findings and disciplinary and other recommendations to assure that City officials, employees, and vendors are held accountable for violations of laws and policies; to improve the efficiency, cost-effectiveness government operations and further to prevent, detect, identify, expose and eliminate waste, inefficiency, misconduct, fraud, corruption, and abuse of public authority and resources.

OIG's authority to produce reports of its findings and recommendations is established in the City of Chicago Municipal Code §§ 2-56-030(d), -035(c), -110, -230, and 240.

## PROJECT TEAM

Kari Pennington, Investigative Analyst

Robert Owens, Chief Performance Analyst

## PUBLIC INQUIRIES

Communications: (773) 478-8417 | [communications@igchicago.org](mailto:communications@igchicago.org)

## TO SUGGEST WAYS TO IMPROVE CITY GOVERNMENT

Visit: [igchicago.org/contact-us/help-improve-city-government](https://igchicago.org/contact-us/help-improve-city-government)

## TO REPORT FRAUD, WASTE, AND ABUSE IN CITY PROGRAMS

Call OIG's toll-free hotline: (866) 448-4754 / TTY: (773) 478-2066

Or visit: [igchicago.org/contact-us/report-fraud-waste-abuse/](https://igchicago.org/contact-us/report-fraud-waste-abuse/)

*Cover image courtesy of ShotSpotter. Icons by Adrien Coquet, Evan Shuster, Gautam Arora, Wani Cantik, and Goran Markovic from [the Noun Project](#).*

*Alternate formats available upon request.*



JULY 29, 2021

eff.org



# It's Time for Police to Stop Using ShotSpotter

## ESPAÑOL

*Update (October 22): Earlier this month, SpotSpotter [filed a lawsuit](#) alleging that the Vice report linked below contains false and defamatory statements.*

Court documents recently reviewed by [VICE](#) have revealed that ShotSpotter, a company that makes and sells [audio gunshot detection](#) to cities and police departments, may not be as accurate or reliable as the company claims. In fact, the documents reveal that employees at ShotSpotter may be altering alerts generated by the technology in order to justify arrests and buttress prosecutors' cases. For many reasons, including the concerns raised by these recent reports, police must stop using technologies like ShotSpotter.

Acoustic gunshot detection relies on a series of sensors, often placed on lamp posts or buildings. If a gunshot is fired, the sensors detect the specific acoustic signature of a gunshot and send the time and location to the police. Location is gauged by measuring the amount of time it takes for the sound to reach sensors in different locations.

According to [ShotSpotter](#), the largest vendor of acoustic gunshot detection technology, this information is then verified by human acoustic experts to confirm the sound is gunfire, and not a car backfire, firecracker, or other sounds that could be mistaken for gunshots. The sensors themselves can only determine whether there is a loud noise that somewhat resembles a gunshot. It's still up to people listening on headphones to say whether or not shots were fired.

In a [recent statement](#), ShotSpotter denied the VICE report and claimed that the technology is “100% reliable.” Absolute claims like these are always dubious. And according to the testimony of a ShotSpotter employee and expert witness in [court documents reviewed by VICE](#), claims about the accuracy of the classification come from the marketing department of the company—not from engineers.

Moreover, ShotSpotter presents a real and disturbing threat to people who live in cities covered in these AI-augmented listening devices—which all too often are over-deployed in [majority Black and Latine neighborhoods](#). It's important to note that many of ShotSpotter's claims of accuracy are generated by marketers, not engineers. A [recent study](#) of Chicago showed how, over the span of 21 months, ShotSpotter sent police to dead-end reports of shots fired over 40,000 times—although some [experts and studies](#) have disputed this claim. This shows—again—that the technology is not as accurate as the company's marketing department claims. It also means that police officers routinely are deployed to neighborhoods expecting to encounter an armed shooter, and instead encounter innocent pedestrians and neighborhood residents. This creates a real risk that police officers will interpret anyone they encounter near the projected site of the loud noises as a threat—a scenario that could easily result in civilian casualties, especially in over-policed communities.

In addition to its history of false positives, the danger it poses to pedestrians and residents, and the company's dubious record of altering data at the behest of police departments, there is also a civil liberties concern posed by the fact that these microphones intended to detect gunshots can also record human voices.

Yet people in public places—for example, having a quiet conversation on a deserted street—are often entitled to a reasonable expectation of privacy, without overhead microphones unexpectedly recording their conversations. Federal and state eavesdropping [statutes](#) (sometimes called wiretapping or interception laws) typically prohibit the recording of private conversations absent consent from at least one person in that conversation.

In at least two criminal trials, prosecutors sought to introduce as evidence audio of voices recorded on acoustic gunshot detection systems. In the California case [People v. Johnson](#), the court admitted it into evidence. In the Massachusetts case [Commonwealth v. Denison](#), the court did not, ruling that a [recording of “oral communication” is prohibited “interception”](#) under the Massachusetts Wiretap Act.

It's only a matter of time before police and prosecutors' reliance on ShotSpotter leads to tragic consequences. It's time for cities to stop using ShotSpotter.

**TAGS:**

**STREET LEVEL SURVEILLANCE**

---

## JOIN EFF LISTS

### Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

**SUBMIT**

---

ELECTRONIC FRONTIER FOUNDATION  
eff.org  
Creative Commons Attribution License









## NOTE

# Against Geofences

Haley Amster & Brett Diehl\*

**Abstract.** Law enforcement is increasingly relying on a new tool when investigating crimes with no suspects: geofence warrants. Geofence warrants take advantage of geofence technology, which constructs a virtually bounded geographic area and identifies all users present within that area during a given time window. Google, the primary recipient of geofence warrants, has adopted a policy of objecting to any geofence request that is not a probable-cause warrant. So far, law enforcement has complied. This has caused courts and litigators to defer the question of whether, under *Carpenter v. United States*, a probable-cause warrant is necessary. Instead, these parties have located the legality of geofence warrants in less explored regions of the Fourth Amendment as applied to new technologies: probable-cause and particularity requirements, the few exceptions to those requirements, and the proper execution of a warrant.

This Note fills an analytical void by providing a comprehensive examination of these less explored regions. The Note first provides a technology primer, detailing the three steps involved in geofence warrants: the initial data dump, selective expansion, and unmasking. It then provides background on relevant Fourth Amendment law, explaining why the familiar “reasonable expectation of privacy” test has not yet proven dispositive in geofence-warrant litigation. After cataloguing burgeoning geofence litigation, the Note examines the initial data dump, identifying the difficulty of meeting probable-cause and particularity requirements due to the inherent breadth of the search. Here the Note

---

\* Haley Amster is a law clerk at Covington & Burling LLP; J.D., Stanford Law School, 2021. Brett Diehl is a trial attorney at Federal Defenders of San Diego, Inc.; J.D., Stanford Law School, 2021.

Our deepest gratitude to Robert Weisberg for his encouragement, guidance, and insights. Thanks to Michael W. McConnell, Morgan N. Weiland, and the rest of the Constitutional Law Center for their support and guidance. Thanks to Jonathan Abel, David Sklansky, Jonathan Mayer, Orin Kerr, John Ellis, Rick Salgado, Todd Hinnen, Sierra Villaran, Laura Koenig, the participants of the Constitutional Law Center’s Works-in-Progress Workshop, and the students of the Legal Studies Workshop for their helpful comments and feedback throughout the drafting process. Thanks to editors and friends—Marty Berger, Marc Brunton, Julia Irwin, Jenny Jiao, Dan Kim, Matt Krantz, David Levin, Caro Sundermeyer, Daphne Thompson, Mitchell Wong, Jeffrey Xia, and Peggy Xu—who made this Note better with their insightful edits and commentary. And thanks to Tal Klement for immediately recognizing the many questions that geofence warrants raise. All views expressed are our own and do not reflect those of any current or former employers.

answers the question of whether probable cause must be shown for each device included in a digital search, based in part on jurisprudence regarding checkpoints, area warrants, and searches of many people in a commercial location. The Note next examines the selective expansion and unmasking steps, arguing (1) that geofence warrants are unconstitutional general warrants because of the discretion given to law-enforcement officials in warrant execution; and (2) that these steps may impermissibly increase a warrant's scope or constitute multiple searches under one warrant. The Note concludes by considering the broader implications of corporate policy shaping Fourth Amendment guardrails.

**Table of Contents**

Introduction .....	388
I. The Technology Behind a Geofence Request.....	393
A. The SensorVault.....	394
B. Warrant Execution .....	398
1. Initial data dump.....	399
2. Selective expansion .....	404
3. Unmasking.....	405
II. Geofences and the Fourth Amendment.....	406
A. Is a Geofence a Fourth Amendment “Search”?.....	406
B. Probable Cause, Particularity, and Warrant Execution .....	410
III. How Courts Are Handling Geofence Warrants .....	411
A. Northern District of Illinois Magistrate Opinions .....	412
1. Pharmaceutical sale investigation: first denial.....	413
2. Pharmaceutical sale investigation: second denial .....	414
3. Pharmaceutical sale investigation: third denial.....	415
4. Arson investigation.....	416
B. District of Kansas Magistrate Opinion.....	417
C. Ongoing State and Federal Litigation .....	419
D. Preliminary Takeaways from the Early Litigation.....	421
IV. Constitutionality of the Initial Data Dump.....	422
A. Probable Cause.....	422
1. Geofences as <i>Ybarra</i> searches .....	423
2. Geofences as checkpoints.....	425
3. Geofences as area warrants .....	427
4. Takeaways.....	429
B. Issues with the Particularity Requirement.....	431
V. Constitutionality of Selective Expansion and Unmasking .....	433
A. Geofences as General Warrants .....	433
B. Selective Expansions as Increases in Scope .....	435
C. Multiple Searches.....	436
VI. Corporate Policy and Fourth Amendment Protections.....	437
A. Absence of Legislation .....	438
B. Corporate Constitutional Policy .....	440
Conclusion.....	444

### Introduction\*

Suppose a law-enforcement officer investigating a hit-and-run sets up a checkpoint near the site of the incident. The investigating officer stops each passerby and examines their cell phone location history to determine if they were present at the crime scene. This officer would be in violation of the Fourth Amendment for employing a checkpoint in the “ordinary enterprise of investigating” a crime.<sup>1</sup> Now suppose that officer obtains a warrant compelling Google to do the same thing—digitally. Different result?<sup>2</sup>

Since roughly 2016, law enforcement has used geofence warrants to help revive criminal investigations gone cold.<sup>3</sup> These warrants have become increasingly common,<sup>4</sup> and there are even indications that a warrant-authorized geofence was used to investigate the January 6, 2021 attempted insurrection at the U.S. Capitol.<sup>5</sup>

Geofence warrants “work in reverse” from traditional search warrants.<sup>6</sup> Instead of law enforcement requesting that a third-party provider produce the location history of a particular suspect’s device, geofence warrants proceed first by giving investigators access to data for all cellular devices that were present near a crime scene around the time when the crime occurred. Through a series

---

\* This Note is current as of November 2021. Subsequent changes in the legal landscape are not addressed.

1. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 44, 48 (2000) (invalidating a checkpoint employed “primarily for the ordinary enterprise of investigating crimes”); cf. *Illinois v. Lidster*, 540 U.S. 419, 423, 427–28 (2004) (upholding a checkpoint because its primary purpose was not to “determine whether a vehicle’s occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others”).
2. Credit is due to Dennis Martin for inspiring our introduction. See Dennis Martin, Note, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 693 (2018).
3. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), <https://perma.cc/P75R-DZCU> (to locate, select “View the live page”). We use “geofence warrant” to align with the term most commonly used by litigators and commentators. See, e.g., *id.* But the precise term is “reverse location” warrant. See, e.g., Thomas Brewster, *To Catch a Robber, the FBI Attempted an Unprecedented Grab for Google Location Data*, FORBES (Aug. 15, 2018, 9:00 AM EDT), <https://perma.cc/XG3N-JEGG>; Tyler Dukes, *To Find Suspects, Police Quietly Turn to Google*, WRAL.COM (Mar. 15, 2018, 5:05 AM), <https://perma.cc/RFU9-XDF7>.
4. Alfred Ng, *Privacy Groups Demand Google Disclose Details on Geofence Warrants*, CNET (Dec. 8, 2020, 5:00 AM PT), <https://perma.cc/TGS4-DUE5>.
5. Statement of Facts at 5–6, *United States v. Groseclose*, No. 21-mj-00250 (D.D.C. Feb. 22, 2021), 2021 U.S. Dist. Ct. Pleadings LEXIS 132, ECF No. 1-1; Drew Harwell & Craig Timberg, *How America’s Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM EDT), <https://perma.cc/Q257-LHYT>.
6. Sidney Fussell, *Creepy “Geofence” Finds Anyone Who Went Near a Crime Scene*, WIRED (Sept. 4, 2020, 7:00 AM), <https://perma.cc/Y3S8-ZT8Q>.

of iterative steps between the provider and law enforcement—without the further involvement of a magistrate judge—the provider produces additional location data with the goal of (1) helping law enforcement figure out which devices could have been those of the perpetrators; and (2) ultimately revealing the identities of the suspects.

Such sweeping searches can unearth the location history of a startling number of users. One 2019 geofence warrant authorized a geofence covering a total of 29,387 square meters (or 7.4 acres—about the size of five and a half American football fields) over a period of nine hours.<sup>7</sup> In response, the provider returned to law enforcement the location data of 1,494 cell phones.<sup>8</sup>

So far, Google has been the primary recipient of geofence warrants. This is in large part due to Google's location-history database, the SensorVault. Google uses the SensorVault to target advertisements, determine when stores are busy, help users track their movements, and provide traffic estimates.<sup>9</sup> But law-enforcement officials now also use the SensorVault for criminal investigations. In response to increasing government requests for information, Google has crafted a three-step, self-directed process for law-enforcement officials trying to obtain user data. As Google explained in a 2020 court filing, it has "instituted a policy of objecting to any warrant that fail[s] to include" its mandated tailoring process.<sup>10</sup>

In recent years, the number of SensorVault-directed geofence warrants has grown rapidly. According to data released by Google, geofence warrants "recently constitut[ed] more than 25% of all [U.S.] warrants" received by the company.<sup>11</sup> Google disclosed that it received 982 geofence-warrant requests in

---

7. Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented "Geofence" Search*, FORBES (Dec. 11, 2019, 7:45 AM EST), <https://perma.cc/34QP-XMKY>.

8. *Id.*

9. See Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works*, N.Y. TIMES (Apr. 13, 2019), <https://perma.cc/FPL9-KRX6>; Declaration of Marlo McGriff ¶ 26, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-1. For example, if a cell phone owner is walking toward a Starbucks, she might see a Starbucks coupon appear on her device (because her device sensed that she was near the store). Once she goes into the Starbucks and uses her coupon, her device registers that information. Google tracks and stores such advertisement-servicing and usage data.

10. Declaration of Sarah Rodriguez ¶ 5, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-2.

11. Google, Supplemental Information on Geofence Warrants in the United States 1 (n.d.), <https://perma.cc/6B34-PPCX>. A TechCrunch article notes that Google released this data in August 2021. See Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021, 2:54 PM PDT), <https://perma.cc/V95P-2MMD>.

2018.<sup>12</sup> This figure, Google explained in a court document, represented “over a 1,500% increase in the number of geofence requests . . . [as] compared to 2017.”<sup>13</sup> In 2019, the number of geofence warrants received by Google increased by a further 755% over the previous year to 8,396.<sup>14</sup> In 2020, the last year for which specific statistics are publicly available at the time of writing, Google received 11,554 geofence warrants.<sup>15</sup> California law enforcement represents the most frequent geofence-warrant requester, having submitted 3,655 of the 20,932 requests logged by Google over the three-year period.<sup>16</sup> Texas law enforcement came in second with 1,825 geofence warrants submitted to Google.<sup>17</sup> By contrast, federal law enforcement submitted only 928 requests from 2018 to 2020.<sup>18</sup>

As geofences become more well-known, at least one crime victim’s family has specifically urged investigators to request a geofence warrant.<sup>19</sup> The Department of Justice’s Computer Crimes and Intellectual Property Section has held discussions with Google about geofences and, in at least one instance, provided a boilerplate geofence-warrant request form to an FBI agent.<sup>20</sup> Hawk Analytics, which frequently assists law-enforcement investigations across the country,<sup>21</sup> hosted a webinar for law enforcement called “Working with Google Geofence Reverse Location Search Records” and previously offered an online tool allowing investigators to obtain a “Google geofence warrant in a few

---

12. Google, *supra* note 11, at 2 (to locate, select “View the live page,” and then select “Download supplemental data as a CSV”).

13. Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant’s Motion to Suppress Evidence from a “Geofence” General Warrant (ECF No. 29) at 3, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 20, 2019), 2019 WL 8227162, ECF No. 59-1 [hereinafter Google Amicus Brief].

14. Google, *supra* note 11, at 2 (to locate, select “View the live page,” and then select “Download supplemental data as a CSV”).

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.*

19. Shannon Ryan, *Family, Investigators Push for Geofence Warrant in Jason Landry Case*, FOX 7 AUSTIN (May 11, 2021), <https://perma.cc/NX7G-4FLK>.

20. Mr. Chatrie’s Post-hearing Brief on “Geofence” General Warrant at 3-4, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. May 3, 2021), ECF No. 205 [hereinafter *Chatrie* Post-hearing Brief].

21. Sam Richards, *Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country*, INTERCEPT (Dec. 23, 2020, 6:31 AM), <https://perma.cc/57XS-WX2X>.

‘clicks.’”<sup>22</sup> Reports of wrongful arrests due to geofence warrants have already emerged.<sup>23</sup>

Courts and legislatures have paid little attention to how the Fourth Amendment applies to geofence warrants.<sup>24</sup> This is largely due to the novelty of the tool: As of this writing, most litigation has been *ex parte*, only five magistrate opinions considering the issue have been unsealed, and some of the first state and federal challenges by criminal defendants are underway.<sup>25</sup> But the lack of attention may also be due to Google’s unique role. Since the Supreme Court’s landmark decision in *Carpenter v. United States*—holding that the production of seven days’ worth of cell phone location information constitutes a Fourth Amendment search requiring a warrant<sup>26</sup>—litigation and scholarship have focused on whether non-*Carpenter* technologies also lead to

---

22. *Working with Google Geofence Reverse Location Search Records*, HAWK ANALYTICS (Jan. 23, 2020), <https://perma.cc/3QQ4-HAXM>; Hawk Analytics (@hawkanalytics), FACEBOOK (June 17, 2019) (capitalization altered), <https://perma.cc/LD5J-QDNY> (to locate, select “View the live page”); Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, GUARDIAN (Sept. 16, 2021, 6:00 AM EDT), <https://perma.cc/94H4-ERPF>.

23. See *infra* notes 57–67 and accompanying text.

24. See *infra* Parts III, VI.A. And the literature has only begun to explore the many questions raised by this new tool. See Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2515–20 (2021) (considering the question of when a geofence search occurs and arguing that it occurs when the provider searches its database, not when law enforcement receives the requested data); Tim O’Brien, *Suspicionless Search: Geofence Warrants and the Fourth Amendment* 19–31 (Aug. 6, 2021) (unpublished manuscript), <https://perma.cc/L7C3-SYZ3> (highlighting the shortcomings of anonymization in the geofence-warrant process and arguing that Fourth Amendment case law and statutory protections are insufficient to protect users’ privacy); Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, CRIM. JUST., Summer 2020, at 7, 12–13 (recommending limitations on the use of geofence warrants, such as allowing these warrants only for violent offenses and only after exhausting traditional investigation methods). See generally John C. Ellis, Jr., *Google Data and Geofence Warrant Process*, NLSBLOG.ORG (Jan. 8, 2021), <https://perma.cc/E7CW-7NZJ> (explaining geofence-warrant technology and execution); Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment?*, LAWFARE (Feb. 24, 2020, 1:03 PM), <https://perma.cc/Y4MV-FTVR> (detailing the motion to suppress filed in *United States v. Chatrue*, a case discussed below). This Note breaks new ground by focusing on how to properly conduct the probable-cause inquiry, explaining that courts must focus the inquiry on each device swept up in the geofence search. This Note also makes a novel contribution by introducing analogies to checkpoints, area warrants, and searches of many people in a commercial location. Finally, this Note is the first to highlight the broader impacts of Google’s role in this emerging issue, arguing that the corporation’s policies have played an outsized role in shaping law-enforcement norms and practices.

25. See *infra* Part III.

26. 138 S. Ct. 2206, 2212, 2217 n.3, 2220–21 (2018).

Fourth Amendment searches.<sup>27</sup> For geofences specifically, however, Google's policy of objecting to any request not derived from a probable-cause warrant has deferred the familiar "is this a Fourth Amendment search" question.<sup>28</sup> Questions surrounding geofence warrants' legality thus occupy less explored regions at the intersection of new technology and the Fourth Amendment: probable cause, particularity, and proper warrant execution.

This Note fills an analytical void by providing a comprehensive examination of these underexplored Fourth Amendment warrant requirements. It proceeds in six parts. Part I is a technology primer, detailing the three steps involved in geofence warrants: the initial data dump, selective expansion, and unmasking. Part II provides a background of relevant Fourth Amendment doctrine, including a discussion of how *Carpenter* intersects with geofence warrants. Part III catalogs burgeoning geofence litigation, with a special focus on the first few federal magistrate opinions on the issue. Part IV considers the initial data dump, identifying the difficulty of meeting probable-

---

27. See *id.* at 2220 (noting the decision's narrow scope). For post-*Carpenter* litigation, see generally *United States v. Moore-Bush*, 963 F.3d 29 (1st Cir.) (holding that *Carpenter* does not extend to eight months of video surveillance conducted using a pole camera), *vacated and reh'g en banc granted*, 982 F.3d 50 (1st Cir. 2020); *State v. Sylvestre*, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018) (holding that *Carpenter* extends to cell-site simulator location data); and *United States v. Diggs*, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (holding that *Carpenter* extends to the acquisition of a vehicle's long-term GPS data). For post-*Carpenter* scholarship applying the decision in a variety of contexts, see, for example, Orin S. Kerr, *Implementing Carpenter* (USC L. Legal Stud. Working Paper, Paper No. 18-29, 2018), <https://perma.cc/XG96-NMTR> (arguing that *Carpenter* should apply to non-content internet records if those records are collected by new digital technologies, are collected without a user's meaningful consent, and reveal intimate personal details); Susan Freiwald & Stephen Wm. Smith, *The Supreme Court, 2017 Term—Comment: The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 227-31 (2018) (suggesting *Carpenter* may extend to real-time location information, fewer than seven days of historical location information, and other technologies); Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), <https://perma.cc/A2SX-Z9GP> ("[A]lmost everything we do in the digital age—social media, internet searches, the Internet of Things—has locational privacy implications because they track location, and *Carpenter* suggests that they might also have Fourth Amendment implications."); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 375-76 (2019) (suggesting that *Carpenter* could extend to real-time location information); Lara M. McMahon, Note, *Limited Privacy in "Pings": Why Law Enforcement's Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment*, 77 WASH. & LEE L. REV. 981, 1027 (2020) (arguing that *Carpenter* does not extend to all cell phone pings); Emma Lux, Student Contribution, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. ONLINE 109, 113-18 (2020) (analyzing whether *Carpenter* extends to tower dumps); and Stephanie Foster, Note, *Should the Use of Automated License Plate Readers Constitute a Search After Carpenter v. United States?*, 97 WASH. U. L. REV. 221, 238-39 (2019) (asserting that *Carpenter* extends to aggregated data from automated license-plate readers).

28. See *infra* Part II.A.

cause and particularity requirements due to the inherent breadth of the search. Here the Note analogizes to the search of many people located at the scene of a crime in *Ybarra v. Illinois*,<sup>29</sup> the use of digital checkpoints, and the use of area warrants. It then explores the difficulty of tailoring by (1) examining digital searches of multi-occupancy buildings; (2) surveying scholarship and litigation regarding tower dumps; and (3) suggesting particularized search protocols that could meet constitutional requirements. Part V examines the selective expansion and unmasking steps, arguing that geofence warrants are unconstitutional general warrants because of the discretion given to law-enforcement officials in warrant execution. Part V also argues that the selective-expansion and unmasking steps may impermissibly increase a warrant's scope or constitute multiple searches under one warrant. Finally, Part VI considers the broader implications of corporate policy driving Fourth Amendment guardrails.

## I. The Technology Behind a Geofence Request

A geofence warrant compels Google to produce data from its SensorVault location-history database.<sup>30</sup> Under Google's threat of noncompliance, most geofence warrants proceed in three steps: the initial data dump, selective expansion, and unmasking. This Part first explains the SensorVault and then elaborates on each of the three execution steps, drawing on unsealed search warrants from federal and state investigations as examples.

---

29. 444 U.S. 85, 87-88 (1979).

30. See Valentino-DeVries, *supra* note 3 ("Investigators who spoke with The New York Times said they had not sent geofence warrants to companies other than Google, and Apple said it did not have the ability to perform those searches."). Google is the only company known to release location-history data in this manner. Leila Barghouty, *What Are Geofence Warrants?*, MARKUP (Sept. 1, 2020, 8:00 AM ET), <https://perma.cc/XQ3Z-K88H>. Microsoft recently stated that it "does not and would not be in a position to comply with any warrants seeking such [location] information." *Id.* (quoting Microsoft Assistant General Counsel Hasan Ali). Facebook stated that it does not fulfill geofence warrants because of its less precise location information and limitations on data storage. David Uberti, *Police Requests for Google Users' Location Histories Face New Scrutiny*, WALL ST. J. (July 27, 2020, 5:30 AM ET), <https://perma.cc/C9DM-SS9E>. Lyft has signaled a potential willingness to fulfill geofence warrants if undefined specificity conditions are met. *Id.* Garmin has stated that it would not fulfill geofence warrants if served because of a belief that such requests are "invasive of our users' privacy rights." *Id.* (quoting a Garmin representative). Amazon Web Services recently announced that it will add "Amazon Location" geofence capabilities for companies hosted on its platform. Renato Losio, *AWS Introduces Location Service in Preview*, INFOQ (Jan. 3, 2021), <https://perma.cc/S2K6-5PU4>.

A. The Sensor Vault

Google's SensorVault is a prodigious pool of consumer location information, pioneered in part to target advertisements but now routinely used by law enforcement for geofence warrants.<sup>31</sup> Cell-service providers and other corporations also collect cell-site location information for various purposes.<sup>32</sup> Yet the SensorVault and linked internal Google databases are more expansive, storing user location information generated from "search queries," "users' IP addresses, device sensors," and "device signals including GPS, information cellular networks provide to a device, information from nearby Wi-Fi networks, and information from nearby Bluetooth devices."<sup>33</sup> Multiple inputs can be combined to estimate a user's location "to a high degree of precision."<sup>34</sup> Google refers collectively to this data, regardless of its source, as location history (LH). Absent a user request or account closure, LH is stored within Google's databases for at least eighteen months.<sup>35</sup>

Google's LH practices affect the vast majority of people living in the United States. Eighty-five percent of Americans currently own a smartphone

- 
31. See *supra* note 9 and accompanying text. For examples of commercial uses of location data, see *Geofencing Advertising Platform*, GROUNDTRUTH, <https://perma.cc/MWE6-DUCL> (archived Oct. 22, 2021); Sarah Berry, *Geofencing Marketing: The New Way to Market Your Business*, WEBFX (Apr. 20, 2021), <https://perma.cc/4MKB-RYK8>; and Justin Croxton, *Geofencing Advertising: What Is Geo Fencing & How Does It Work*, PROPELLANT MEDIA (Jan. 5, 2021), <https://perma.cc/CDP6-NTAM>. The use of location data and geofences to target advertisements raises privacy and ethics questions beyond the scope of this Note. See, e.g., Kearston L. Wesner, *Is the Grass Greener on the Other Side of the Geofence? The First Amendment and Privacy Implications of Unauthorized Smartphone Messages*, 10 CASE W. RES. J.L. TECH. & INTERNET, no. 1, 2019, at 1, 1-3 (describing a settlement regarding geofence-based advertisements that targeted women in the vicinity of abortion clinics and encouraged them not to terminate their pregnancies); John G. Browning, *Geo-Fencing: Free Speech or Tainting the Jury Pool?*, J.L. & TECH. TEX. (Nov. 15, 2019), <https://perma.cc/9EVH-F7RK> (describing Monsanto's use of geofences to target ads highlighting its herbicide's safety in the lead-up to a California trial on the issue).
32. See *supra* note 31; see also, e.g., AT&T, AT&T Location Information Services 1-2 (2012), <https://perma.cc/8E5N-FV4C>.
33. Exhibit 202 at 4, State v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. July 17, 2020); see also Google Amicus Brief, *supra* note 13, at 10 ("[I]nputs include not only information related to the locations of nearby cell sites, but also GPS signals . . . or signals from nearby Wi-Fi networks or Bluetooth devices.").
34. Google Amicus Brief, *supra* note 13, at 10. Google's geofence-warrant results normally include an indication of location precision, shown via a radius in which Google's algorithm has calculated the user is likely located. A smaller radius, resulting from more location inputs or better quality, indicates a more precise location. See *infra* Figure 3; *infra* notes 73-74 and accompanying text.
35. See Jessica Bursztynsky, *Google Just Announced It Will Automatically Delete Your Location History by Default*, CNBC (updated June 24, 2020, 12:11 PM EDT), <https://perma.cc/RN7M-6XQF>.

with mobile internet capabilities.<sup>36</sup> Approximately 46.8% of these U.S. smartphones operate on Google's Android operating system.<sup>37</sup> Across platforms, three of the five most popular smartphone applications in the United States—Gmail, Google Maps, and Google Search, each accessed on over 50% of U.S. smartphones—belong to Google.<sup>38</sup> And for the over 220 million estimated U.S. mobile search users,<sup>39</sup> 96% of searches were conducted via Google as of the first quarter of 2020.<sup>40</sup> Google's servers capture location data from all of these services: the Android operating system, Google-owned mobile applications, and in-browser mobile searches via Google.<sup>41</sup>

Presumably because of its vast information troves, Google is receiving geofence-warrant requests at an alarming rate. Google publishes the aggregate figures for subpoenas, court orders, warrants, and other requests that it receives from U.S. law enforcement, but until recently it did not release specific geofence-warrant tallies.<sup>42</sup> In 2019, an anonymous Google employee told the *New York Times* that the corporation received upwards of 180 geofence warrants in one week.<sup>43</sup> In January 2020, in what experts speculated could be a tactic to deter law-enforcement requests, Google began charging \$245 for

---

36. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), <https://perma.cc/5UX9-P7PU>.

37. S. O'Dea, *U.S. Smartphone Subscriber Share by Operating Platform 2012-2021, by Month*, STATISTA (Aug. 11, 2021), <https://perma.cc/3KRQ-TS53> (to locate, select "View the live page").

38. See Statista Rsch. Dep't, *Reach of Most Popular U.S. Smartphone Apps 2021*, STATISTA (July 26, 2021), <https://perma.cc/9MVQ-K8QC> (to locate, select "View the live page"). A fourth, YouTube, is owned by Google's parent company, Alphabet. See *id.*

39. Statista Rsch. Dep't, *Number of Mobile Search Users in the United States 2014-2020*, STATISTA, <https://perma.cc/PV5B-3VWZ> (archived Oct. 22, 2021) (to locate, select "View the live page").

40. Joseph Johnson, *U.S. Total & Mobile Organic Search Visits 2020, by Engine*, STATISTA (Feb. 22, 2021), <https://perma.cc/43LF-PNRW>.

41. See *How Google Uses Location Information*, GOOGLE, <https://perma.cc/D4ZX-C9A3> (archived Oct. 22, 2021). The government has explained the ubiquity of Google products in court filings. "In its affidavit, the government asserts that approximately 97% of smartphones in the world use Google applications or Google's operating system," which would allow those smartphones to appear in a geofence if present within its boundaries. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at \*3 (N.D. Ill. July 8, 2020). "[T]he government asserts a likelihood 'that at any given time, a mobile telephone, regardless of make, is interfacing in some manner with a Google application, service, and/or platform[.]'" *Id.* at \*3 n.3 (alteration in original) (quoting the government's filing). "We assume this reasonable conclusion to be true, and thus reasonably conclude that likely hundreds of cellphones other than the suspect's cellphone would be included in the requested geofences." *Id.*

42. See *Global Requests for User Information*, GOOGLE, <https://perma.cc/2YTD-ZMEV> (archived Oct. 23, 2021); Ng, *supra* note 4; *supra* note 11.

43. Valentino-DeVries, *supra* note 3.

compliance with a search warrant.<sup>44</sup> Tallies have continued to grow, however, and Google received an average of more than thirty geofence warrants per day in 2020.<sup>45</sup>

Police have not limited the use of the SensorVault to egregious or violent crimes.<sup>46</sup> According to an early geofence-warrant exposé by Minnesota Public Radio, police obtained geofence warrants for an investigation into who had stolen a pickup truck and, separately, \$650 worth of tires.<sup>47</sup> Separately, Minneapolis investigators used a geofence warrant to identify individuals near an AutoZone where a man had smashed windows during protests over the murder of George Floyd.<sup>48</sup>

It remains unclear if a user can choose to withhold all of her location history from Google, which has asserted that LH sharing is optional for its users.<sup>49</sup> But manually deactivating all LH sharing remains difficult and discouraged.<sup>50</sup> A consumer-fraud lawsuit brought by Arizona's Attorney General alleged that while "Google told users [that] . . . '[w]ith Location History off, the places you go are no longer stored,'" Google "would surreptitiously collect location information through other settings such as Web & App Activity and use that information to sell ads."<sup>51</sup> The Associated Press "found that many Google services on Android devices and iPhones store your location data even if you've used a privacy setting that says it will prevent Google from

---

44. See Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), <https://perma.cc/NZP5-5924>.

45. See *supra* notes 11-18 and accompanying text.

46. Magistrate Judge M. David Weisman has lamented the government's "undisciplined . . . overuse" of geofence warrants in "run-of-the-mill cases that present no urgency or imminent danger." *In re the Search*, 2020 WL 5491763, at \*8.

47. Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPR NEWS (Feb. 8, 2019, 1:10 PM), <https://perma.cc/HF3G-BP2V>.

48. Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protestors*, TECHCRUNCH (Feb. 6, 2021, 8:00 AM PST), <https://perma.cc/Y6BX-GHLL>.

49. Google Amicus Brief, *supra* note 13, at 5. ("Holders of Google accounts can control various account-level and service-level settings and preferences. 'Location History' . . . is an optional account-level Google service. It does not function automatically for Google users."); *Manage Your Location History*, GOOGLE ACCT. HELP, <https://perma.cc/GP93-XARG> (archived Oct. 23, 2021) ("Location History is turned off by default for your Google Account and can only be turned on if you opt in.").

50. See Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, VERGE (Aug. 25, 2020, 3:04 PM EDT), <https://perma.cc/X6EQ-5XQ5> (describing the difficult process to deactivate Google location history); Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, AP NEWS (Aug. 13, 2018), <https://perma.cc/CB84-X5KE> (same).

51. Complaint for Injunctive and Other Relief ¶ 8, *State ex rel. Brnovich v. Google LLC*, No. CV2020-006219 (Ariz. Super. Ct. May 27, 2020) (quoting Nakashima, *supra* note 50).

doing so,” and researchers at Princeton University confirmed these findings.<sup>52</sup> In 2018, an internal Google email explained that “[t]he current [user interface] feels like it is designed to make [limiting LH collection] possible, yet [it is] difficult enough that people won’t figure it out.”<sup>53</sup> Another internal email in 2019 expressed similar frustration: “Speaking as a user . . . I *thought* I had location tracking turned off on my phone. However the location toggle in the quick settings was on.”<sup>54</sup> The email’s author continued: “[O]ur messaging around this is enough to confuse a privacy focused [software engineer]. That’s not good.”<sup>55</sup> As one Google employee wrote, “I’d want to know which of these [location-sharing] options (some? all? none?) enter me into the wrongful-arrest lottery.”<sup>56</sup>

And the wrongful-arrest lottery has already begun. In 2018, Arizona police officers jailed Jorge Molina for six days on suspicion of murder.<sup>57</sup> Officers told Molina that they knew “one hundred percent, without a doubt” that his phone was at the scene of the crime based on a Google geofence warrant.<sup>58</sup> In reality, Molina had lent an old phone, inadvertently still signed into his Google account, to the man police later arrested for the murder.<sup>59</sup> In addition to the six days he spent behind bars, Molina lost his job, and “[w]hen he started looking for a new job, he couldn’t get an interview or pass a background check, since a quick Google search showed he had been accused of murder.”<sup>60</sup> The state impounded Molina’s car during the investigation; eventually, without any income to support himself, Molina lost title to the vehicle.<sup>61</sup>

In another nightmarish scenario, Florida police using a geofence warrant to investigate a burglary turned to Google to obtain “more information” on

---

52. Nakashima, *supra* note 50; *see also* Mark Brnovich (@GeneralBrnovich), TWITTER (May 27, 2020, 3:29 PM), <https://perma.cc/9WYV-QSMB> (“We began our investigation of Google following a 2018 @AP article that detailed how users are lulled into a false sense of security, believing Google provides users the ability to actually disable their Location History.”).

53. Exhibit 18 at 6, State *ex rel.* Brnovich v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. Aug. 21, 2020).

54. Exhibit 215 at 6, State *ex rel.* Brnovich v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. Aug. 21, 2020).

55. *Id.*

56. *Id.* at 4-5.

57. Fussell, *supra* note 6; *see also* Meg O’Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), <https://perma.cc/63PT-K2JM>.

58. Fussell, *supra* note 6 (quoting the police report).

59. *See id.*

60. O’Connor, *supra* note 57.

61. *Id.*

Zachary McCoy.<sup>62</sup> Google's legal investigations support team notified McCoy that Google would release his data absent court intervention.<sup>63</sup> With the help of an attorney, McCoy realized that he was swept into the geofence because, on the day of the burglary, he biked past "the victim's house three times within an hour, part of his frequent loops through his neighborhood."<sup>64</sup> An avid biker, McCoy used an application called Runkeeper to record his bike rides; Runkeeper "relied on his phone's location services, which fed his movements to Google."<sup>65</sup> After police withdrew the warrant, McCoy speculated that his entanglement may have ended differently "if his parents hadn't given him several thousand dollars to hire [a lawyer]."<sup>66</sup>

These are but two egregious cases highlighted by news outlets. With hundreds of new geofence warrants filed each week, many similar cases presumably lie unreported.<sup>67</sup> We now turn to what makes the entanglement of innocents possible by examining the breadth of geofence warrants' reach and the typical geofence-warrant execution process.

## B. Warrant Execution

Google has crafted a three-step warrant execution process to handle geofence requests.<sup>68</sup> As a Google employee stated in a court declaration, "[e]arly 'geofence' legal requests sought LH data that would identify all Google users who were in a geographical area in a given time frame"—essentially an unmasked data dump.<sup>69</sup> To "ensure privacy protections for Google users and to protect against overbroad disclosures . . . Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures."<sup>70</sup> This has led to the now "typical[]" three-step protocol.<sup>71</sup>

---

62. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 3:22 AM PST), <https://perma.cc/84NC-K8QQ>.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. Captain John Sherwin of the Rochester Police Department in Minnesota put it colorfully, telling reporters: "When you sit down and think about it, it makes you want to destroy all your devices" and "move to a cabin in Montana." Thomas Brewster, *Feds Order Google to Hand Over a Load of Innocent Americans' Locations*, FORBES (Oct. 23, 2018, 9:00 AM EDT) (quoting Sherwin), <https://perma.cc/5QSU-Y74P>.

68. Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

69. *Id.*

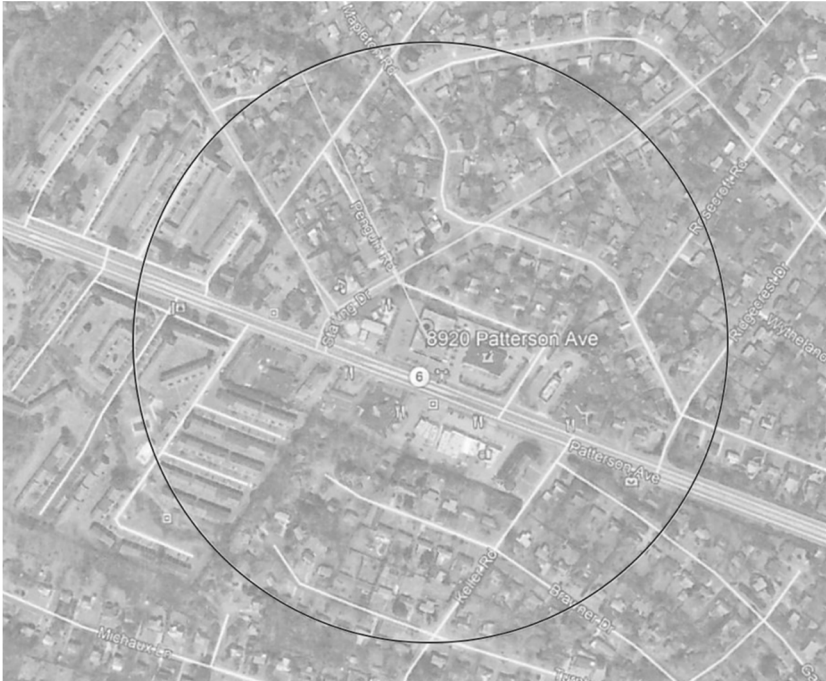
70. *Id.*

71. *See id.* ¶¶ 5-12.

1. Initial data dump

In the initial data dump, law enforcement requests from Google the location information of all devices within a specified geographic zone during a defined time frame. The following Figure illustrates one such request.

**Figure 1**

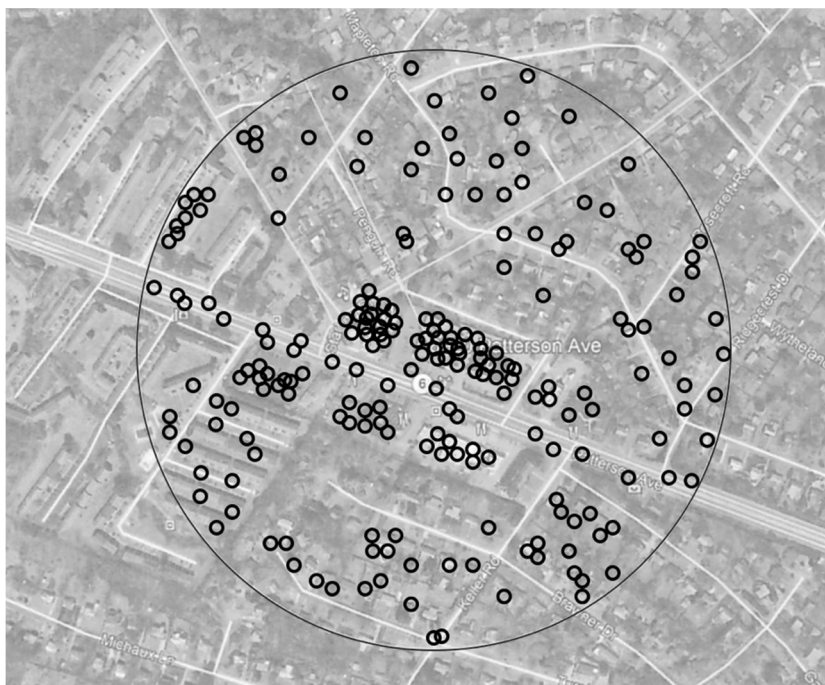


This was one of the geofences requested as part of a Dollar Tree robbery investigation by the FBI in Henrico, Virginia. A significant number of residences and commercial businesses other than the targeted Dollar Tree were within the geofence's geographic zone.

*Source:* Brewster, *supra* note 67.

In response, Google discloses an anonymized list of devices, each with a unique device ID, timestamps and coordinates, and the data source.<sup>72</sup>

**Figure 2**



We created this visual aid to represent what the initial data dump may have looked like to law enforcement, with each circle representing a location ping from a device caught within the boundaries of the geofence.

72. See Brewster, *supra* note 7. Notably, users' supposedly anonymous IDs may not actually be anonymous. A recent exposé on mobile advertising identifiers revealed that these identifiers can be used to piece together personal information about even "masked" users. Charlie Warzel & Stuart A. Thompson, Opinion, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. TIMES (Feb. 5, 2021), <https://perma.cc/2J5T-VUHL> (to locate, select "View the live page"). It is not clear whether Google uses mobile advertising identifiers in its data returns.

**Figure 3**

---

Device ID	Date	Time (America/Chicago -05:00)	Latitude	Longitude	Source	Maps Display Radius (m)
-1025956090	4/8/2019	11:07:00 (-05:00)	43.4214456	-88.3507382	GPS	9
-1361086191	4/8/2019	10:52:33 (-05:00)	43.4211171	-88.3508743	GPS	16
-1638700124	4/8/2019	10:54:57 (-05:00)	43.421202	-88.3503325	WiFi	58
1565184502	4/8/2019	10:55:12 (-05:00)	43.4313883	-88.35045	GPS	3
1830501424	4/8/2019	11:05:24 (-05:00)	43.4211382	-88.3500203	WiFi	50
647939400	4/8/2019	10:56:03 (-05:00)	43.421015	-88.350123	WiFi	59

---

This is what the initial data dump looks like on paper. This particular list was the location history returned to law-enforcement officials investigating a bank robbery in Allenton, Wisconsin.

*Source:* Brewster, *supra* note 7.

---

The precision of the latitude and longitude coordinates varies depending on source, as demonstrated by Figure 3’s rightmost column, “Maps Display Radius (m).”<sup>73</sup> For GPS-derived latitude and longitude coordinates, Google provides maps display radii (i.e., certainty of a user’s location) ranging from three to sixteen meters. For coordinates derived via Wi-Fi, however, Google provides radii ranging from fifty to fifty-nine meters. As shown in Figure 3, Google was able to approximate the coordinates derived using GPS more precisely than those derived via Wi-Fi. As a Google product manager noted, “[I]f a user opens Google Maps and looks at the blue dot indicating Google’s estimate of his or her location, Google’s goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.”<sup>74</sup>

---

73. This is the circle that a user sees when they open up a map-based application on their mobile device: The larger the radius of the circle, the less precise the reported location of the user. See *Find & Improve Your Location’s Accuracy*, GOOGLE MAPS HELP, <https://perma.cc/C4MC-QXR7> (archived Jan. 28, 2022); Ellis, *supra* note 24. See generally Krista Merry & Pete Bettinger, *Smartphone GPS Accuracy Study in an Urban Environment*, 14 PLOS ONE, no. 7, July 2019, at 1, 2-3, 17 (noting that the accuracy of a smartphone’s reported location data can vary widely depending on a number of variables).

74. Declaration of Marlo McGriff, *supra* note 9, ¶ 24. Geofence warrants do not necessarily limit the data searched to the subset of users actually present in the geofence. Depending on how a corporation indexes data, all accounts may need to be queried to identify records that match the warrant’s specified place and time. This is the case for Google, which has stated that its database is structured such that it requires a search of all users to produce the initial data dump. See Google Amicus Brief, *supra* note 13, at 12-13.

Accordingly, law enforcement may obtain data for users outside of the warrant's geographic parameters who, due to imprecision, logged a location radius that fell within the geofence.<sup>75</sup> The following example illustrates such a possibility. Focusing on two devices in our geofence, Device 1 and Device 2, let us assume (1) that Device 1 has location coordinates derived from Wi-Fi with a radius of fifty-five meters; and (2) that Device 2 has location coordinates derived from a cell site with a radius of 1,000 meters (a radius that can be typical for locations based on cell sites<sup>76</sup>).

The radius of Device 1 would look like this:

**Figure 4**

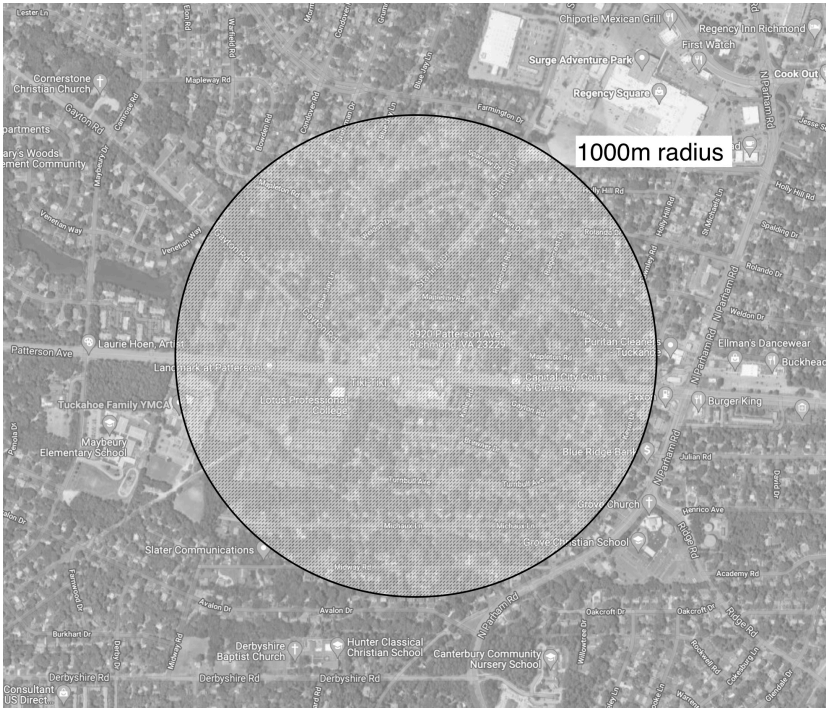


75. See Declaration of Marlo McGriff, *supra* note 9, ¶ 25.

76. Ellis, *supra* note 24.

The radius of Device 2 would look like this:

Figure 5



Therefore, as illustrated in particular for Device 2 (because of its large radius), it is possible that an individual can end up in a geofence for an area in which they were never present. This issue may not be a concern for targeted advertisements: Accidentally serving ads to people outside of the intended geographic area carries little harm beyond wasted effort and money.<sup>77</sup> But the same flaw in precision carries far more serious consequences when the SensorVault is used for criminal liability.

77. Indeed, a Google product manager explained that Google's ability to approximate device location "is sufficiently precise and reliable for [the] purposes for which Google designed LH." Declaration of Marlo McGriff, *supra* note 9, ¶ 26.

## 2. Selective expansion

After law-enforcement officials review the data in the initial dump, the next step is selective expansion. Without the oversight of a magistrate judge, law enforcement requests additional location history for certain devices in the geofence.<sup>78</sup> The expanded location history reaches beyond the geographic and temporal ranges specified in the initial data dump, enabling law enforcement to track the path of devices before and after the window in which the crime allegedly occurred.<sup>79</sup> This information can lead officials to discard some devices from the investigation and focus more deeply on others (if, for example, a device's trajectory aligns with the known escape route of an unidentified person of interest).<sup>80</sup>

The original warrant typically governs the time frame beyond the original window for which law enforcement can request geographically unbounded LH. For example, one geofence warrant told Google to "provide additional location history outside of the predefined area for . . . relevant accounts to determine path of travel" for up to forty-five minutes before or after the originally enumerated time windows.<sup>81</sup> Another geofence warrant permitted investigators to request additional data from "30 minutes before AND 30 minutes after the initial search time periods."<sup>82</sup>

---

78. See, e.g., Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 6, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Oct. 29, 2019), 2019 WL 7660969, ECF No. 29 [hereinafter *Chatrie Motion to Suppress*]; see also Valentino-DeVries, *supra* note 3.

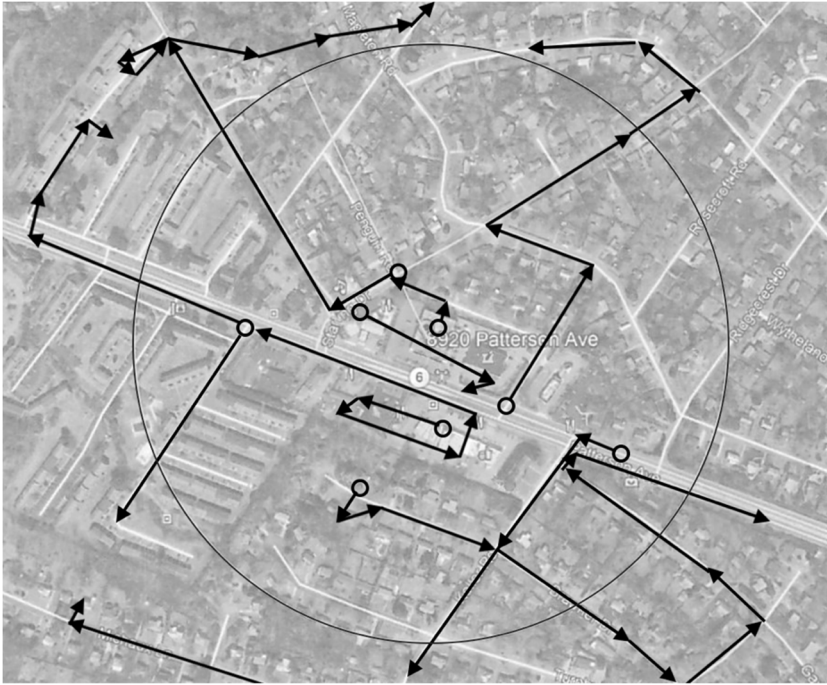
79. See, e.g., *Chatrie Motion to Suppress*, *supra* note 78, at 6 (describing how investigators, without judicial scrutiny, gained access to the unbounded location data of nine users for thirty minutes before and after the initial geofence time period).

80. The selective-expansion step is sometimes omitted for geofence warrants that examine multiple time frames. See, e.g., Application for a Search Warrant at 16-17, *In re the Search of: Location & Identifying Info. Maintained by Google LLC*, No. 19-mj-00918 (E.D. Wis. Dec. 31, 2019), ECF No. 1 [hereinafter Dec. 31, 2019 Application]; Application for a Search Warrant at 20-22, *In re the Search of: Location Hist. Data from Google LLC Generated from Mobile Devices*, No. 19-mj-00104 (E.D. Wis. Dec. 4, 2019), ECF No. 1; Application for a Search Warrant at 14-16, 19, *In re the Search of: Location Hist. Data from Google LLC Generated from Mobile Devices*, No. 19-mj-00846 (E.D. Wis. May 1, 2019), ECF No. 1; Application for a Search Warrant at 9, 11, 13-14, *In re the Search of: Info. That Is Stored at Premises Controlled by Google*, No. 18-mj-01307 (E.D. Wis. Nov. 20, 2018), ECF No. 1. This may be because investigators are able to identify devices of interest based on multiple appearances.

81. Motion to Quash & Suppress Evidence Under Penal Code §§ 1538.5 & 1546 at 8, *People v. Dawes*, No. 19002022 (Cal. Super. Ct. June 9, 2020) [hereinafter *Dawes Motion to Quash & Suppress*] (emphasis omitted) (quoting the warrant).

82. *Chatrie Motion to Suppress*, *supra* note 78, at 6 (quoting the warrant).

Figure 6



A visual representation of the selective-expansion step, showing location history outside of the originally specified time and radius for devices identified for additional data production.

### 3. Unmasking

Lastly, and again without judicial oversight, law enforcement requires Google to provide subscriber information for any device selected by investigators.<sup>83</sup> This unmasking divulges information including the account's registered name, address, start date of service, services utilized, telephone

83. See, e.g., *Chatrle Motion to Suppress*, *supra* note 78, at 6-7; see also Valentino-DeVries, *supra* note 3. Note that Minnesota police officers follow a different practice: After they receive the initial data dump, they request another warrant from the court to retrieve identifying information. Aaron Mak, *Close Enough*, SLATE (Feb. 19, 2019, 5:55 AM), <https://perma.cc/72YG-393W>.

numbers, email addresses, and means and sources of payment for services.<sup>84</sup> In at least one instance, law enforcement has sought personal identifying information from all devices included in the initial data dump.<sup>85</sup>

## II. Geofences and the Fourth Amendment

Geofence warrants raise a series of Fourth Amendment questions, some more explored than others in the context of new technologies.

### A. Is a Geofence a Fourth Amendment “Search”?

The threshold question is, of course, whether a geofence is a search—that is, whether it invades a “reasonable expectation of privacy” per the test formulated by Justice Harlan’s concurrence in *Katz v. United States*.<sup>86</sup> In perhaps the most relevant precedent addressing law enforcement’s investigatory use of consumer data, *Carpenter v. United States*, the Court grappled with this question in the context of cell-site location information used to catalog a suspect’s whereabouts over the course of several days.<sup>87</sup> Rejecting an application of the third-party doctrine (given that the data was in the possession of the suspect’s cell-service provider),<sup>88</sup> the Court held that the government’s acquisition of this data was a search and that the government should have obtained a probable-cause warrant in order to access it.<sup>89</sup> However, the Court ended its opinion with a caveat, explaining that the decision was narrow and cabined to its facts.<sup>90</sup>

The *Carpenter* caveat opened the door to a cottage industry of litigation over whether, under *Carpenter*’s reasoning, the use of other technologies can also amount to a Fourth Amendment search.<sup>91</sup> One prominent unanswered question in this inquiry is whether the government can avoid *Carpenter*’s warrant requirement by using many small intrusions over a large population

---

84. See, e.g., Dec. 31, 2019 Application, *supra* note 80, at 17; cf. 18 U.S.C. § 2703(c)(2) (describing the required disclosures in response to a Stored Communications Act subpoena for subscriber information).

85. Brewster, *supra* note 7.

86. See 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

87. 138 S. Ct. 2206, 2212–13, 2216–17 (2018).

88. Traditionally, under the third-party doctrine, “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

89. *Carpenter*, 138 S. Ct. at 2221, 2223.

90. *Id.* at 2220.

91. See *supra* note 27.

(as it does with geofence warrants) rather than a few large intrusions over a small population (as it did in *Carpenter*).<sup>92</sup>

In addition to its unclear scope, *Carpenter*'s longevity is uncertain. The recent change in Supreme Court membership (with the passing of Justice Ginsburg and the confirmation of Justice Barrett) means that the five-vote *Carpenter* majority is no longer intact. Attention has now turned to Justice Gorsuch's *Carpenter* dissent as a possible path forward.<sup>93</sup> Justice Gorsuch's theory employs a positive-law approach, suggesting that a user may retain a property interest in his or her data held by a third-party provider.<sup>94</sup>

Accordingly, an in-depth analysis of the *Carpenter* question—whether a geofence warrant constitutes a Fourth Amendment search—is not the main focus of this Note. Google's policy of objecting to anything less than a probable-cause warrant has seemingly pressured the government to file only warrant applications, punting the resolution of the *Carpenter* question further down the line.<sup>95</sup> And at least one court to consider the *Carpenter* question in the geofence context has noted that *Carpenter* is not dispositive. In a 2020 opinion denying a geofence warrant, Magistrate Judge M. David Weisman wrote that a citation to *Carpenter* was "not intended to suggest that *Carpenter* pre-ordains the outcome here."<sup>96</sup> Instead, Judge Weisman's opinion was "premised on much longer established Fourth Amendment principles that a search warrant must establish probable cause to justify the scope of the search requested, and the type of evidence to be seized must be particularly described, not left to the agents' complete discretion."<sup>97</sup> The court thus found that the only dispositive question was whether the geofence warrant could be properly issued under the magistrate's authority, bound to the probable-cause and particularity issues we discuss in Parts IV and V below.

---

92. This question raises a related issue: If there is a search, when does the search occur? Is it at the time Google queries the database, or is it when law enforcement gains access to the data? See generally Note, *supra* note 24, at 2515-20 (arguing that a search occurs "when a private company first searches through its entire database"). For the purposes of this Note, the distinction makes no difference. Even if the search occurs when data is returned to law enforcement, the search still cannot satisfy probable-cause and particularity requirements. See *infra* Part IV.

93. See, e.g., Chris Machold, Note, *Could Justice Gorsuch's Libertarian Fourth Amendment Be the Future of Digital Privacy? A "Moderate" Contracts Approach to Protecting Defendants After Carpenter*, 53 U.C. DAVIS L. REV. 1643, 1648-49 (2020) (noting that Justice Gorsuch's *Carpenter* dissent offers a promising path to a majority that can protect the digital privacy interests of defendants).

94. See *Carpenter*, 138 S. Ct. at 2267-72 (Gorsuch, J., dissenting).

95. See *infra* Parts III.A-C.

96. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at \*7 n.10 (N.D. Ill. July 8, 2020).

97. *Id.*

But to briefly indicate our intuitions on the *Carpenter* question: We agree with the court decisions and commentators arguing that *Carpenter*'s holding extends beyond its factual boundaries.<sup>98</sup> And we believe that *Carpenter* extends to geofence technology. Whether a geofence request is viewed as a search of many individuals, a search of many individual devices, or a search of many homes, a geofence violates the reasonable expectation of privacy of each user swept up in its bounds. It is near axiomatic to say that users today have, or should have, a reasonable expectation of privacy in their sensitive location data. Location data is qualitatively different than other kinds of data: It is precise and revealing,<sup>99</sup> and it is in many ways the currency of the modern era. Some companies compete by limiting third-party access to location data; others use dubious means to mine it.<sup>100</sup> And cell-site location information—the kind of data that the *Carpenter* Court found precise enough to warrant Fourth Amendment protection—is the least precise form of location input.<sup>101</sup>

Any argument that a geofence search is less privacy invasive because it gathers data only in a short time window is misguided. Mere minutes of the SensorVault's pinpointed LH can be incredibly revealing.<sup>102</sup> In fact, this is often the precise reason that law-enforcement officials seek LH: As a Minnesota deputy police chief admitted, SensorVault's constant, precise tracking "shows the whole pattern of life," a "game changer for law enforcement."<sup>103</sup> And even a brief snapshot can expose highly sensitive information—think a visit to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar,"<sup>104</sup> or a location other than home during a COVID-19 shelter-in-place order.

---

98. See, e.g., *State v. Sylvestre*, 254 So. 3d 986, 991-92 (Fla. Dist. Ct. App. 2018) (holding that *Carpenter* extends to cell-site simulator location data); Freiwald & Smith, *supra* note 27, at 227-31.

99. See *Carpenter*, 138 S. Ct. at 2212 (noting that "modern cell phones generate increasingly vast amounts of increasingly precise" cell-site location information).

100. See, e.g., Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolick, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), <https://perma.cc/R8QW-XWCF> (to locate, select "View the live page"); Chaim Gartenberg, *Why Apple's New Privacy Feature Is Such a Big Deal*, VERGE (Apr. 27, 2021, 10:30 AM EDT), <https://perma.cc/H8LT-24GC>; Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice*, N.Y. TIMES (updated Sept. 29, 2021), <https://perma.cc/PJN5-RB6N>.

101. *Carpenter*, 138 S. Ct. at 2220; Ellis, *supra* note 24.

102. See *supra* Part I.A.

103. Valentino-DeVries, *supra* note 3 (quoting Brooklyn Park Deputy Police Chief Mark Bruley).

104. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

There are also real doubts as to whether anonymization actually protects the privacy of users whose data is revealed in a geofence. As researchers have repeatedly proven, cross-referencing datasets can reveal the identifying information of nearly every “anonymized” user.<sup>105</sup> There are many opportunities to cross-reference an anonymized data dump received from Google, invading the privacy of all users caught up in the geofence.

Regarding an application of the third-party doctrine, there is real doubt as to whether users voluntarily share their location data with Google.<sup>106</sup> As detailed above, even sophisticated Google employees struggle to understand how, if at all, they can turn off LH collection.<sup>107</sup> And even if it is theoretically possible to stop Google’s location tracking, the briefing for *United States v. Chatrie* has documented the lack of voluntariness of the initial consent:

Following the standard setup of an Android phone like the one used by Mr. Chatrie, a user encounters a pop-up screen . . . when opening the Google Maps application for the first time. It says, “Get the most from Google Maps” and then it gives the user two options: “YES I’M IN” or “SKIP.” There is also a statement that reads “Google needs to periodically store your location to improve route recommendations, search suggestions, and more” and a button to “LEARN MORE.” The pop-up does not use the phrase [sic] “Location History,” but clicking on “YES I’M IN” enables the function. Clicking on “LEARN MORE” takes the user to a webpage with Google’s complete Privacy Policy and Terms of Service; it does not direct the user to any specific language concerning location data or Location History specifically.

In fact, Google’s Terms of Service do not mention Location History at all. And Google’s Privacy Policy, which is 27 pages long, mentions Location History only twice. In the first instance, it says, in full: “You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.” If anything, the phrase “private map” is misleading and suggests that Google does not have access to the data. In the second instance, the policy says, in full: “Decide what types of activity you’d like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions.” Of course, “traffic predictions” do not begin to suggest that Google will keep a 24/7 “journal” of a user’s whereabouts. But even if it did, a user would have no way of knowing that the pop-up “opt-in” screen relates to the Location History feature.

---

105. The inability of users to stop sharing location data with cell-service providers helped motivate the holding in *Carpenter*. See *Carpenter*, 138 S. Ct. at 2220 (“[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.”).

106. Warzel & Thompson, *supra* note 72; Gina Kolata, *Your Data Were “Anonymized”? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), <https://perma.cc/73J2-PXUQ>.

107. See *supra* notes 53-56 and accompanying text.

The pop-up does not reference “Location History” by name. As a result, a typical user would not know to scour Google’s policies for references to Location History, much less understand the implications of the choice Google is asking them to make. In short, it is strikingly easy for a user to “opt-in” to Location History without ever being aware of doing so.<sup>108</sup>

Another *Chatrie* defense brief details the similarly confusing maze a user must navigate to pause and delete LH data.<sup>109</sup>

Even if the Supreme Court adopts Justice Gorsuch’s theory that a provider may serve as a bailee of data,<sup>110</sup> we believe that the Fourth Amendment still applies to geofence searches. Users likely have a property interest in their SensorVault information, and those individuals who knowingly opt into LH collection affirmatively designate Google as a bailee.

### B. Probable Cause, Particularity, and Warrant Execution

Because of Google’s policies and the uncertainty surrounding *Carpenter*,<sup>111</sup> geofence issues have primarily been situated in less explored Fourth Amendment questions: (1) when a search warrant is properly issued per the requirements of probable cause and particularity; and (2) how a warrant is properly executed. A brief primer on the relevant case law: A valid search warrant can only issue upon a showing of probable cause to the issuing neutral magistrate.<sup>112</sup> In rare circumstances—primarily in administrative or regulatory searches, where a public need and the lack of an ordinary criminal investigation justify an intrusion—investigative techniques are subjected to a relaxed probable-cause requirement.<sup>113</sup>

The Fourth Amendment also instructs that no warrants shall issue except those “particularly describing the place to be searched, and the persons or things to be seized.”<sup>114</sup> The Supreme Court has explained that this requirement “makes general searches under [warrants] impossible and prevents the seizure

---

108. Defendant Okello Chatrie’s Supplemental Motion to Suppress Evidence Obtained from a “Geofence” General Warrant at 15-17, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. May 22, 2020), 2020 WL 4551093, ECF No. 104 [hereinafter *Chatrie* Supplemental Motion to Suppress] (footnotes omitted) (citations omitted).

109. *Chatrie* Post-hearing Brief, *supra* note 20, at 14-15.

110. *See Carpenter*, 138 S. Ct. at 2268-69 (Gorsuch, J., dissenting); *supra* notes 93-94 and accompanying text.

111. *See supra* notes 92-97 and accompanying text.

112. *See* U.S. CONST. amend. IV; *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971), *overruled in part on other grounds by Horton v. California*, 496 U.S. 128 (1990); *Johnson v. United States*, 333 U.S. 10, 13-15 (1948).

113. *See infra* Part IV.A.3.

114. U.S. CONST. amend. IV.

of one thing under a warrant describing another.”<sup>115</sup> The particularity requirement also limits the discretion of an officer executing a warrant and “determines the permissible intensity” and scope of the search.<sup>116</sup> For example, a search warrant describing an entire apartment building will usually be held invalid without a probable-cause showing as to all the units in the building.<sup>117</sup> Similarly, a warrant authorizing the search of a specified area and “any and all persons found therein” is likely defective if it does not establish that (1) someone present during the warrant execution is likely involved in the criminal activity; and (2) the individual likely has evidence of the crime on his or her person.<sup>118</sup> And once the original warrant is executed, the place cannot be searched a second time unless a second warrant is obtained from the court, coupled with an affidavit detailing why there is probable cause to search again notwithstanding the first warrant.<sup>119</sup>

### III. How Courts Are Handling Geofence Warrants

Amid a lack of binding state and federal jurisprudence, magistrate judges in the U.S. District Court for the Northern District of Illinois and the U.S. District Court for the District of Kansas have collectively produced five opinions on geofence warrants. Three of the Illinois opinions reject geofence-warrant applications but leave open the possibility of a constitutionally permissible geofence request. Similarly, the Kansas opinion rejects a geofence-warrant application based on its lack of probable cause and particularity without categorically ruling geofence warrants unconstitutional. The fourth Illinois opinion approves a geofence-warrant application.

The first geofence-warrant challenge before an Article III federal judge is underway in *United States v. Chatrie*, with the issue briefed and argument pending at the time of writing.<sup>120</sup> Similarly, a state court opinion examining

---

115. *Marron v. United States*, 275 U.S. 192, 196 (1927).

116. 2 WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, *CRIMINAL PROCEDURE* § 3.4(f) (West 2021).

117. *Id.* § 3.4(e).

118. *Id.* (collecting cases).

119. *Id.* § 3.4(j); see *United States v. Baldyga*, 233 F.3d 674, 682-83 (1st Cir. 2000).

120. See Defendant’s Response to the Government’s Supplemental Memorandum in Opposition to Defendant’s Discovery of SensorVault Data at 12, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Feb. 25, 2020), ECF No. 92 (“The Court has recognized that this is ‘a case of first impression . . .’” (quoting Complete Transcript of Discovery Motion Before the Honorable M. Hannah Lauck at 179, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Jan. 30, 2020), ECF No. 81)); Andrea Vittorio, *Robbery Poses Legal Test for Police Use of Google Location Data*, BLOOMBERG L. (Sept. 14, 2021, 2:01 AM), <https://perma.cc/Z38W-F8YB> (noting that *Chatrie* “is considered the first federal example of a criminal defendant challenging the use of a [geofence] data as

*footnote continued on next page*

the constitutionality of geofence warrants could emerge from a challenge currently underway in California's San Francisco County Superior Court in *People v. Dawes*.<sup>121</sup>

This Part walks through the Northern District of Illinois and District of Kansas cases and examines both *Chatrie* and *Dawes*. It then concludes with preliminary takeaways from the nascent geofence litigation.

#### A. Northern District of Illinois Magistrate Opinions

Northern District of Illinois magistrate judges have taken the lead in considering the constitutional questions surrounding geofence warrants. They have done so in four opinions across two investigations. In the first investigation, regarding the theft and sale of pharmaceuticals, law enforcement requested a geofence warrant three separate times.<sup>122</sup> Magistrate judges denied all three requests.<sup>123</sup>

A second investigation, regarding a series of arsons, involved one geofence-warrant request and yielded an unsealed opinion granting the warrant.<sup>124</sup> This opinion, while far from the first grant of a geofence warrant, represents the first published opinion approving a geofence warrant and asserting the warrant's constitutionality.<sup>125</sup>

In the first investigation, the government sought a geofence warrant to investigate "the theft and resale of certain pharmaceuticals."<sup>126</sup> The government requested three specific geofences, all for forty-five-minute periods, across three different days.<sup>127</sup> The first covered a 100-meter radius

---

evidence in his indictment"); Sobel, *supra* note 24 (identifying *Chatrie* as "the first known federal Fourth Amendment challenge against a geofence warrant in a federal district court").

121. See *Dawes* Motion to Quash & Suppress, *supra* note 81, at 1-2. One of the authors of this Note was an author of the motion to quash and suppress in *Dawes*.

122. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 732-33 (N.D. Ill. 2020).

123. *Id.* at 732-33, 757; see also Sealed Memorandum Opinion & Order at 1, 25, *In re the Search of: Info. Stored at Premises Controlled by Google*, as Further Described in Attachment A, No. 20-mc-00392 (N.D. Ill. July 24, 2020), ECF No. 5; *In re the Search of: Info. Stored at Premises Controlled by Google*, as Further Described in Attachment A, No. 20-mc-00297, 2020 WL 5491763, at \*1 (N.D. Ill. July 8, 2020), ECF No. 4.

124. *In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 349, 351 (N.D. Ill. 2020).

125. See *In re the Search*, 481 F. Supp. 3d at 748 ("The Court is not aware of any federal decision addressing [probable-cause and particularity] issues with respect to a geofence warrant, and the Court has reason to believe that geofence warrants are facing their first round of judicial scrutiny.").

126. *In re the Search*, 2020 WL 5491763, at \*1.

127. *Id.*

(over 7.7 acres of land) during the afternoon in “a densely populated” area containing “restaurants, various commercial establishments, and at least one large residential complex.”<sup>128</sup> The second and third, both of which also covered 100-meter radii during the afternoon, included “medical offices and other single and multi-floor commercial establishments that are likely to have multiple patrons.”<sup>129</sup>

1. Pharmaceutical sale investigation: first denial

The first warrant application requested only the initial data dump and unmasking steps.<sup>130</sup> Magistrate Judge M. David Weisman’s opinion roundly rejected the government’s application. Judge Weisman indicated his “only point of agreement” with the government’s argument was probable cause for the suspect: “There is probable cause to believe that among all the other data this warrant application seeks from Google, there is a likelihood that the suspect’s phone data would be included.”<sup>131</sup> But the warrant, he wrote, “suffers from two obvious constitutional infirmities.”<sup>132</sup> “First, the scope of the search is overbroad, and second, the items to be seized are not particularly described.”<sup>133</sup>

Judge Weisman explained that it “strains credibility” in a probable-cause inquiry to assert that individuals within the entire geofence bore witness to the illegal pharmaceutical transaction, which involved receipt indoors of a mailed package.<sup>134</sup> Witnessing such an act, he colorfully speculated, would have required the individuals to “possess extremely keen eyesight and perhaps x-ray vision to see through . . . many walls.”<sup>135</sup> Judge Weisman also noted that “the majority of the area sought encompasses structures and businesses that would necessarily have cell phone users who are not involved in [the underlying] offenses.”<sup>136</sup>

In explaining why the government’s request was not narrowly tailored, the opinion noted that “the geographic scope of this request [is] a congested urban area encompassing individuals’ residences, businesses, and healthcare providers,” meaning that the “vast majority of cellular telephones likely to be

---

128. *Id.* at \*1, \*3.

129. *Id.* at \*1.

130. *See id.*; *supra* Part I.B.

131. *In re the Search*, 2020 WL 5491763, at \*4.

132. *Id.* at \*3.

133. *Id.*

134. *Id.* at \*5 & n.6.

135. *Id.*

136. *Id.* at \*3.

identified in this geofence will have nothing whatsoever to do with the offenses under investigation.”<sup>137</sup> Judge Weisman rejected the government’s assertion that the warrant’s multistep process would protect people’s privacy, finding that “the warrant does not limit agents to only seeking identifying information as to the ‘five phones located closest to the center point of the geofence,’ or some similar objective measure of particularity.”<sup>138</sup>

## 2. Pharmaceutical sale investigation: second denial

After the denial by Judge Weisman, the government submitted two additional warrant applications, both of which were denied.

In its second application, the government added a request that the areas to be searched include “the location history for such devices that ‘could have been (as indicated by margin of error, i.e. “maps display radius”) located within’ the geographical area of the geofences . . . within the time and date parameters of the geofences.”<sup>139</sup> The court explained that the “purpose of including this ‘margin of error’ . . . appears to be directed at ensuring that the proposed warrant captures the location histories for Google-connected devices within the margin of error, i.e., to minimize the possibility that the geofences would miss or overlook a device that may have been inside” the relevant locations.<sup>140</sup> Magistrate Judge Gabriel Fuentes objected to this inclusion, noting that “even a small-scale expansion of the boundaries” of the geofences in question would increase “the chances that the information of uninvolved users would fall within the reach of the government at its discretion.”<sup>141</sup>

The government’s second application also narrowed the geographic scope of the three proposed geofences, keeping the searches closer to the two physical locations at issue.<sup>142</sup> Judge Fuentes found that the narrowing of the geofence boundaries did not “solve the constitutional problem,” however, because “the Court still has no idea how many . . . devices and their users will be identified under the warrant’s authority.”<sup>143</sup> In other words, “the information of an undetermined number of uninvolved persons is authorized to be seized.”<sup>144</sup>

---

137. *Id.* at \*5 (footnote omitted).

138. *Id.* at \*5-6.

139. Sealed Memorandum Opinion & Order, *supra* note 123, at 15 (quoting the application); *see supra* notes 73-75 and accompanying text.

140. Sealed Memorandum Opinion & Order, *supra* note 123, at 16.

141. *Id.* at 16-17.

142. *Id.* at 11-12, 14-15.

143. *Id.* at 22.

144. *Id.* The government also argued that a stay-at-home order reduced the number of innocent people at one of the geofence locations, but the court responded that it “still has no way of knowing how many Google-connected devices traversed the busy urban  
*footnote continued on next page*

3. Pharmaceutical sale investigation: third denial

In the government's third geofence application, the requested geographic and temporal scope remained unchanged from the second application.<sup>145</sup> Although the third application eliminated the unmasking step requested in the initial warrant, the government subsequently clarified that it "retain[ed] the power to obtain by subpoena the identifying subscriber information for any of the device IDs on the anonymized list."<sup>146</sup> The government also "limit[ed] the 'anonymized' information [sought] to that which 'identifies individuals who committed or witnessed the offense,'" yet it provided "[n]o further methodology or protocol" explaining "how Google would know which of the sought-after anonymized information identifies suspects or witnesses."<sup>147</sup>

According to Judge Fuentes, elimination of the unmasking step neither altered the analysis nor cured any constitutional infirmity.<sup>148</sup> The government's ability to obtain personal information from Google's list via subpoena, he reasoned, implicated "the principle that the government may not accomplish indirectly what it may not do directly."<sup>149</sup> Judge Fuentes also held that a "too-vague, eight-word caveat that the information is limited to that which 'identifies the individuals who committed or witnessed the [offense]'" could not cure the application's constitutional infirmity.<sup>150</sup> More specific protocols for Google to determine which devices belonged to relevant persons, he wrote, were necessary.<sup>151</sup> Judge Fuentes reiterated that the proposed warrant's "harness[ing of] geofence technology to cause the disclosure of the identities of various persons" meant that "the government must satisfy probable cause as to those persons," which it had still failed to do.<sup>152</sup>

---

area of [that geofence], and to assume the number of persons was reduced by the stay-at-home order based on the statistics the government presented would be pure speculation." *Id.* at 23.

145. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 732-33 (N.D. Ill. 2020) (stating that the three forty-five-minute geofences contained in the third application were unchanged in geographic scope from the second application).

146. *Id.* at 733.

147. *Id.* (quoting the application).

148. *Id.* at 749.

149. *Id.*

150. *Id.* at 750 (quoting the application).

151. *See id.*

152. *Id.* at 750-51.

#### 4. Arson investigation

In the second investigation that produced an unsealed federal magistrate's opinion, the government presented a geofence warrant application in connection with "a series of approximately 10 arsons in the Chicago area."<sup>153</sup> Law enforcement believed that the fires, most of which burned vehicles, were connected, and that the geofences would "contain evidence pertaining to the identity of the arson suspects and their co-conspirators."<sup>154</sup> The government requested six geofences, four located in commercial lots where the vehicle fires had occurred and two along areas of roadway where the unknown arsonists were alleged to have traveled.<sup>155</sup> Each spanned between fifteen and thirty-seven minutes in length during early morning hours.<sup>156</sup> All but one covered less than a city block, with the fourth proposed geofence covering an elongated roadway area "approximately the length of 1.25 city blocks."<sup>157</sup> Similar to the first investigation, the second investigation's warrant application requested a two-step execution: the initial data dump followed by unmasking.<sup>158</sup>

Magistrate Judge Sunil Harjani approved the application, explaining that, "[o]nce novel," geofence warrants are "now more frequent in criminal investigations" and finding that the application "satisfies the probable cause and particularity requirements of the Fourth Amendment."<sup>159</sup> Judge Harjani held that there was "probable cause that evidence of the crime will be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, can provide evidence on the identity of the perpetrators and witnesses to the crime."<sup>160</sup> Based on the government's assertions that (1) the alleged arsonists likely "use[d] cell phones to plan and commit criminal offenses"; and (2) "there was a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform," the court concluded that "there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime."<sup>161</sup>

The court also held that the geofences were sufficiently limited in scope: They were "specific to the time of the arson incidents only" and "narrowly

---

153. *In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020).

154. *Id.*

155. *Id.* at 351-53.

156. *Id.*

157. *Id.*

158. *See id.* at 353; *supra* note 130 and accompanying text.

159. *In re the Search Warrant Application*, 497 F. Supp. 3d at 349.

160. *Id.* at 355.

161. *Id.* at 356.

crafted to ensure that location data, with a fair probability, will capture evidence of the crime only.”<sup>162</sup> The court noted that the warrant request was appropriately narrow because the buildings and streets contained in the geofences were unlikely to be occupied during the early-morning times requested.<sup>163</sup> The court also explained that a margin of error for location-history data, the “exact scope” of which “is unknown,” did not render the warrant unconstitutional.<sup>164</sup> In the court’s eyes, “the fact that warrants for location data have margins of error does not invalidate them—only reasonableness is required, not surgical precision.”<sup>165</sup> Because the margin of error was “reasonable given the nature of the evidence being sought and what is possible with the technology at issue,” the court found that the warrant met the particularity requirement.<sup>166</sup>

#### B. District of Kansas Magistrate Opinion

In June 2021, Magistrate Judge Angel Mitchell of the U.S. Court for the District of Kansas denied a federal geofence-warrant application on Fourth Amendment grounds.<sup>167</sup> The opinion did not provide much detail regarding the nature of the geofence sought, stating only that the requested data would have covered an area surrounding “a sizeable business establishment” during a one-hour period.<sup>168</sup> Judge Mitchell paid significant attention to the Northern District of Illinois opinions surveyed in Part III.A above.<sup>169</sup> Guided by the analysis in those cases, Judge Mitchell held that the submitted application and affidavit were “not sufficiently specific or narrowly tailored to establish probable cause or particularity.”<sup>170</sup>

Judge Mitchell’s opinion emphasized that probable cause relates to both (1) whether a crime has been committed; and (2) whether evidence of the crime will be located at the place to be searched.<sup>171</sup> In surveying the evidence, Judge Mitchell concluded there was “probable cause that a crime was committed at

---

162. *Id.* at 357.

163. *Id.* at 358.

164. *Id.* at 360-61.

165. *Id.* at 361.

166. *Id.*

167. *In re the Search of Info. That Is Stored at the Premises Controlled by Google, LLC*, No. 21-mj-05064, 2021 WL 2401925, at \*1 (D. Kan. June 4, 2021).

168. *Id.* at \*2; *see also id.* at \*4 (noting that the geofence boundary “encompasses two public streets,” that “the subject building contains another business,” and that “the area just outside of the perimeter . . . includes residences and other businesses”).

169. *See id.* at \*1-4.

170. *Id.* at \*1.

171. *Id.* at \*2.

the [geofence location] during the relevant one-hour time period.”<sup>172</sup> She found that the government had failed, however, to “establish probable cause that evidence of the crime will be located at the place searched—that is, Google’s records showing the location data of cell phone users within the geofence boundaries.”<sup>173</sup> In her judgment, Google’s stored location data “would undoubtedly show” where certain devices were located at a given point in time.<sup>174</sup> But the government’s statements were “too vague and generic to establish a fair probability—or any probability—that the identity of the perpetrator or witnesses would be encompassed within the search.”<sup>175</sup> Even if the court assumed that most individuals, including those committing crimes, used mobile devices, the government’s affidavit still failed to establish “a fair probability that any pertinent individual would have been using a device that feeds into Google’s location-tracking technology.”<sup>176</sup> Judge Mitchell contrasted the government’s conclusory statements about phones linked to Google’s location-tracking services with the more detailed explanations offered by the government in the Northern District of Illinois warrant applications.<sup>177</sup>

Finally, with regard to probable cause, Judge Mitchell found fault with the application’s failure to anticipate the number of individuals likely to be included within the geofence.<sup>178</sup> In her view, the probable-cause inquiry is one of relative scale, in which a large amount of information on innocent individuals “lessens the likelihood that the data would reveal a criminal suspect’s identity, thereby weakening the showing of probable cause.”<sup>179</sup>

The opinion similarly emphasized a proportionality requirement for particularity,<sup>180</sup> with the court writing that “[t]he particularity requirement is more stringent if the privacy interest is greater.”<sup>181</sup> The court found that the government’s application was “missing key information to determine whether the proposed warrant is sufficiently particularized”: The government did not address the public streets and second business contained within the geofence, nor did it “explain the extent to which the geofence, combined with the margin of error, is likely to capture uninvolved individuals from . . . surrounding

---

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.* at \*3.

176. *Id.*

177. *Id.*

178. *Id.* Judge Mitchell noted that this failure “also goes to the particularity requirement, which is intertwined with probable cause.” *Id.*

179. *Id.*

180. *Id.* (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

181. *Id.* (citing *Berger v. New York*, 388 U.S. 41, 56 (1967)).

properties.”<sup>182</sup> Based on these shortcomings, the court held that the government failed to meet its particularity burden.<sup>183</sup> The opinion also questioned why the government asked for a whole hour of data, especially given that this period was longer than any period requested in the Northern District of Illinois cases.<sup>184</sup> Although the government’s affidavit mentioned three specific times that the suspect was shown on video surveillance, “[t]he proposed geofence’s temporal scope ranges from just before the second [video] sighting to approximately 10 minutes after the suspect fled the scene.”<sup>185</sup> The government’s failure to explain its timing request in relation to these facts, along with the geofence’s broad geographic boundaries, ultimately rendered the request insufficiently particular.<sup>186</sup>

The court denied the government’s application without prejudice, and it did not foreclose “the possibility that the government may be able to adequately demonstrate probable cause to support the warrant and articulate that the proposed geofence is sufficiently particular.”<sup>187</sup> But the court firmly stated its demands and the underlying policy considerations, noting that it is “not enough to submit an affidavit stating that probable cause exists for a geofence warrant because, given broad cell phone usage, it is likely the criminal suspect had a cell phone.”<sup>188</sup> “If this were the standard, a geofence warrant could issue in almost any criminal investigation where a suspect is unidentified.”<sup>189</sup>

### C. Ongoing State and Federal Litigation

The magistrate opinions discussed in the previous Subparts all emerged from *ex parte* proceedings without a defendant. The first geofence-warrant challenges brought by criminal defendants have emerged in the past year. One such challenge is in the U.S. District Court for the Eastern District of Virginia; another is in the San Francisco County Superior Court, a California trial-level state court. In *United States v. Chatrie*, a federal defendant is challenging a geofence warrant that allegedly identified him as an armed bank robber.<sup>190</sup> The

---

182. *Id.* at \*4.

183. *Id.*

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. Indictment at 1-2, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Sept. 17, 2019), 2019 WL 7660960, ECF No. 1; *Chatrie* Motion to Suppress, *supra* note 78, at 1.

geofence warrant covered a mixed residential–commercial area alongside a busy regional highway.<sup>191</sup> In addition to the bank that was robbed, the geofence encompassed the entirety of a megachurch housed inside of a converted Costco superstore.<sup>192</sup> Just outside of the geofenced region is a hotel with sixty-eight guest rooms, the occupants of which would have been included in the Google returns if their maps display radii extended beyond a few yards.<sup>193</sup> The area covered by the geofence was “78,000 square meters, or about 17 acres,” but with the approximate margin of error added, “the effective range was 470,000 square meters, or about 116 acres.”<sup>194</sup>

The execution of the *Chatrie* warrant followed the three-step process described in Part I.B above.<sup>195</sup> After the initial data dump, law enforcement repeatedly sought expanded location history “for one hour on either side of the robbery . . . without geographic restriction” for *all* of the devices that Google identified.<sup>196</sup> Recognizing the overbreadth of this request, “Google did not comply until investigators identified a subset of nine users for further scrutiny.”<sup>197</sup> Law enforcement then narrowed the list and requested that Google unmask the owners of three devices.<sup>198</sup>

After the defendant sought to suppress the evidence obtained from the geofence warrant, Google filed an amicus curiae brief in support of neither party.<sup>199</sup> The amicus brief revealed previously unknown information about Google’s use of LH (location history) and defended the corporation’s position that law enforcement must obtain a warrant supported by probable cause in order to access LH records.<sup>200</sup> Google did not take a position on the validity of the warrant at issue.<sup>201</sup>

---

191. *Chatrie* Motion to Suppress, *supra* note 78, at 5-6.

192. *Id.* at 6; Jim McConnell, *A Church Is Born Again Inside an Old Costco*, CHESTERFIELD OBSERVER (Feb. 15, 2017), <https://perma.cc/V4GX-ZU2B>.

193. *Chatrie* Motion to Suppress, *supra* note 78, at 6; *Hampton Inn Richmond-Southwest-Hull Street*, HAMPTON, <https://perma.cc/43BQ-FGLG> (archived Oct. 23, 2021); see Affidavit & Search Warrant at 5, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 18, 2019), ECF No. 54-1.

194. *Chatrie* Supplemental Motion to Suppress, *supra* note 108, at 8-9.

195. *Id.* at 1-2.

196. *Id.* at 2.

197. *Id.*

198. *Id.*

199. See *id.*; Motion for Leave to File Amicus Curiae Brief in Support of Neither Party at 1, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Dec. 20, 2019), ECF No. 59; Google Amicus Brief, *supra* note 13, at 1-2.

200. See Google Amicus Brief, *supra* note 13, at 2, 5-14.

201. *Id.* at 2.

In *Chatrie*, the probable-cause statement for the geofence warrant emphasized that the unidentified bank robber appeared to use a cell phone prior to the robbery.<sup>202</sup> Based on this crime-specific information and generic recitations regarding cell phone use and Google's LH collection, the Chesterfield Circuit Court approved the warrant.<sup>203</sup>

In the San Francisco County Superior Court, the criminal defendant in *People v. Dawes* is similarly challenging a geofence warrant that led to his alleged identification as one of four suspects in a home burglary.<sup>204</sup> Before a San Francisco magistrate, officials in *Dawes* presented a statement of probable cause that included even less detail than the *Chatrie* affidavit.<sup>205</sup> Law enforcement did not even indicate that a cell phone was used during the crime.<sup>206</sup> The investigating officer instead asserted, using boilerplate language, that "[b]ased on my training, experience and consulting with other investigators, I know that subjects who commit crimes, including residential burglaries, often uses [sic] their cell phones as a means of communication during the commission of the crime."<sup>207</sup> The statement then summarized how cell phones collect users' LH data for storage on Google's servers.<sup>208</sup> While litigants await the district court's ruling in *Chatrie* and the evidentiary hearing in *Dawes*, the law governing geofences remains unsettled.

#### D. Preliminary Takeaways from the Early Litigation

Early litigation surrounding geofence warrants has revealed emerging judicial views, government attitudes toward geofences, and potential arguments for defendants. For example, the government has shown that it is willing to narrow requests or forgo selective expansion and unmasking when pressured by Google or magistrate judges.<sup>209</sup>

Although it is early to draw conclusions from five magistrate opinions across two federal districts, we briefly note emerging areas of agreement and disagreement. None of the magistrate judges in the Northern District of Illinois or the District of Kansas held that geofences were categorically

---

202. Affidavit & Search Warrant, *supra* note 193, at 6.

203. *See id.* at 6-8.

204. *Dawes* Motion to Quash & Suppress, *supra* note 81, at 1-2, 6-8.

205. Statement of Probable Cause at 10-11, *People v. Dawes*, No. 19002022 (Cal. Super. Ct. Dec. 4, 2018) (on file with authors). By our calculation, the geofence in *Dawes* covered roughly 14,000 square feet. *See id.* at 11.

206. *See id.* at 8-10.

207. *Id.* at 10.

208. *Id.*

209. *See supra* Parts III.A.2-.3; *see also supra* notes 196-97 and accompanying text.

unconstitutional.<sup>210</sup> Rather, the magistrates differed as to when and how a geofence can conform to the constitutional requirements of a warrant.<sup>211</sup> A large part of this disagreement concerned whether probable cause must be shown for each device searched or merely for Google’s SensorVault as a whole.<sup>212</sup>

Views regarding geofence issues will continue to diverge as the above cases progress—and as new ones arise. We turn now to how Supreme Court precedent on probable-cause and particularity requirements might apply to geofence warrants.

#### IV. Constitutionality of the Initial Data Dump

Our constitutional analysis begins with an evaluation of the first step of geofence-warrant execution: the initial data dump. This Part shows that the government faces difficulty in satisfying probable-cause and particularity requirements at this step because it generally lacks specific knowledge about the crime when it applies for a geofence warrant. We first consider probable cause for geofence warrants in the context of the Supreme Court’s case law regarding checkpoints, area warrants, and searches of people near a crime scene. We then discuss particularity, first examining geofences that include multi-occupancy buildings and then suggesting particularized search protocols for geofence warrants.

##### A. Probable Cause

When applying for geofence warrants, law enforcement’s support for probable cause often resembles that proffered in the Northern District of Illinois arson investigation, as described in Part III.A.4 above. An unknown suspect committed a crime at a certain location at a certain time; investigators assumed—with no proof—that the perpetrator had a smartphone with him

---

210. *See supra* Parts III.A–B.

211. *See supra* Parts III.A–B.

212. *Compare In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 750–51 (N.D. Ill. 2020) (noting that where a geofence warrant “cause[s] the disclosure of the identities of various persons,” the government “must satisfy probable cause as to [each of] those persons”), *with In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 355 (N.D. Ill. 2020) (examining whether there is “probable cause that evidence of the crime will be located at Google”), *and In re the Search of Info. That Is Stored at the Premises Controlled by Google, LLC*, No. 21-mj-05064, 2021 WL 2401925, at \*2 (D. Kan. June 4, 2021) (stating that the government must “establish probable cause that evidence of the crime will be located at the place searched—that is, Google’s records”). We address this topic further in Part IV.A below.

during the offense; and investigators noted “a reasonable probability that a cell phone, regardless of its make, is interfacing in some manner with a Google application, service, or platform.”<sup>213</sup>

Geofence warrants are not the first instance of the government selecting a geographic region and searching everything within it. Sometimes, law enforcement has selected an area and searched every person within it.<sup>214</sup> At other times, it has selected an area and searched every home within it.<sup>215</sup> Now, law enforcement selects an area and searches every device within it. Fourth Amendment jurisprudence has long grappled with the probable-cause and particularity requirements of these inherently broad searches.

### 1. Geofences as *Ybarra* searches

The Supreme Court has made clear that an individual’s mere presence near a crime is insufficient to establish probable cause. In *Ybarra v. Illinois*, an informant told police that he observed a bartender in possession of (and potentially selling) heroin.<sup>216</sup> A judge issued a warrant authorizing the search of the tavern and the bartender.<sup>217</sup> When officers arrived, they searched not only the tavern but also all customers present, including Ventura Ybarra.<sup>218</sup>

The Court declared the search unconstitutional because the government’s warrant application only alleged probable cause for the bartender and did not assert proof “that any person found on the premises of the Aurora Tap Tavern, aside from [bartender] ‘Greg,’ would be violating the law.”<sup>219</sup> “Nowhere . . . did the complaint even mention the [bar’s] patrons.”<sup>220</sup> And Ybarra himself, the Court found, gave police “no reason to believe that he had committed, was committing, or was about to commit any offense under state or federal law.”<sup>221</sup> The Court noted that “the agents knew nothing in particular about Ybarra, except that he was present, along with several other customers, in a public tavern at a time when the police had reason to believe that the bartender would have heroin for sale.”<sup>222</sup> As the Court held, “a person’s mere propinquity to . . .

---

213. *In re the Search Warrant Application*, 497 F. Supp. 3d at 356.

214. *See infra* Parts IV.A.1-2.

215. *See infra* Part IV.A.3.

216. 444 U.S. 85, 87-88 (1979).

217. *Id.* at 88.

218. *Id.* at 88-89. Ybarra, as it turned out, was also in possession of heroin. *Id.* at 89.

219. *Id.* at 90.

220. *Id.*

221. *Id.* at 90-91.

222. *Id.* at 91.

criminal activity does not, without more, give rise to probable cause to search that person.”<sup>223</sup>

An individual Google user being searched via geofence is analogous to Ventura Ybarra being searched at the tavern. Like the warrant application in *Ybarra*, a standard geofence-warrant application alleges two things: (1) that someone committed a crime;<sup>224</sup> and (2) that the crime occurred in a certain location. And like a search of all persons present at the Aurora Tap Tavern, a geofence warrant searches all devices within the specified area.

Similar to the *Ybarra* warrant application, which did not “even mention” individuals other than the bartender,<sup>225</sup> a standard geofence-warrant application does not mention any details about individuals other than the fact that a suspect is likely to be present in the geofence.<sup>226</sup> To borrow from the *Ybarra* Court: The investigators know “nothing in particular about” any individual subjected to the geofence search “except that he was present” in a place “at a time when the police had reason to believe” that a crime occurred.<sup>227</sup>

The Court in *Ybarra* underscored that probable cause must be established for each individual subject to the search. The Court’s analysis contrasts with Magistrate Judge Harjani’s reasoning in the Northern District of Illinois arson case discussed above.<sup>228</sup> In granting a geofence warrant, Judge Harjani considered whether there was a fair probability that evidence of the crime would be found *in the SensorVault*, instead of asking whether there was a fair probability that evidence of the crime would be found *in each user account searched*.<sup>229</sup> In reviewing such decisions, courts must grapple with *Ybarra*’s declaration that the probable-cause requirement “cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.”<sup>230</sup>

---

223. *Id.* (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968)); *see also* *United States v. Di Re*, 332 U.S. 581, 587 (1948) (holding that an individual does not lose constitutional immunities from search by “mere presence in a suspected car”). This holding applies when presence at a crime scene is a known certainty—but presence is not a certainty with geofence returns because of the way that Google collects data. *See supra* notes 73–77 and accompanying text.

224. But in the geofence case, there is not even a named suspect like “Greg” the bartender.

225. *Ybarra*, 444 U.S. at 90.

226. *See, e.g., supra* notes 202–08 and accompanying text.

227. *Ybarra*, 444 U.S. at 91.

228. *See supra* Part III.A.4.

229. *See In re the Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 355 (N.D. Ill. 2020).

230. *Ybarra*, 444 U.S. at 91.

The analogy, of course, is imperfect. The search of a person in a bar is not the same as the search of a device's location history in a geofenced region. Individuals' privacy preferences differ. Some might feel that it is more privacy invasive for a law enforcement to rifle through pockets or a purse than it is for law enforcement to rifle through location data over the course of an hour. Nevertheless, there are good reasons to think that both physical and geofence searches fall within the same category of Fourth Amendment protection. The search of a cell phone's data generally requires a warrant,<sup>231</sup> as does the search of a home.<sup>232</sup> Similarly, the search of cell-site location information generally requires a warrant,<sup>233</sup> as does the search of a bar patron's pockets.<sup>234</sup> All told, the *Ybarra* search parallels geofence searches for purposes of Fourth Amendment jurisprudence. And *Ybarra* models the analysis a court should employ when evaluating probable cause to conduct searches of many people—or many people's devices.

## 2. Geofences as checkpoints

Geofence warrants also resemble checkpoints: Both geofences and checkpoints delineate a geographic region and search everyone within that region. The Supreme Court's checkpoint doctrine is illustrated in *Michigan Department of State Police v. Sitz*, in which law enforcement constructed a checkpoint for drunk driving:

All vehicles passing through a checkpoint would be stopped and their drivers briefly examined for signs of intoxication. In cases where a checkpoint officer detected signs of intoxication, the motorist would be directed to a location out of the traffic flow where an officer would check the motorist's driver's license and car registration and, if warranted, conduct further sobriety tests. Should the field tests and the officer's observations suggest that the driver was intoxicated, an arrest would be made.<sup>235</sup>

A geofence search is essentially a digitized version of the *Sitz* checkpoint. All devices that passed through the specified region during the relevant time window are revealed in the initial data dump, and their location history is examined by law enforcement for signs of criminal activity. When an officer sees suspicious location history, that individual is selected for further investigation via the selective-expansion step.<sup>236</sup> Should the officer's further observations suggest that the individual is a suspect, the geofence warrant

---

231. *Riley v. California*, 573 U.S. 373, 386, 401 (2014).

232. *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990).

233. *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).

234. *Ybarra*, 444 U.S. at 88-89, 90-91.

235. 496 U.S. 444, 447 (1990).

236. *See supra* Part I.B.2.

requires Google to unmask that person and produce his or her subscriber information.<sup>237</sup> In other words, all individuals in the area are preliminarily inspected and, at the officer's discretion, searched. More broadly, law-enforcement officials executing a geofence warrant develop probable cause to investigate certain individuals only *after* they have reviewed the initial data dump (and perhaps selective-expansion data).

The *Sitz* Court found the checkpoint constitutional because it “was clearly aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways, and there was an obvious connection between the imperative of highway safety and the law enforcement practice at issue.”<sup>238</sup> But in *City of Indianapolis v. Edmond*, the Court held that a checkpoint was unconstitutional because its “primary purpose . . . [was] the interdiction of narcotics” and made clear that general-purpose checkpoints are prohibited.<sup>239</sup> The *Edmond* Court declined to “suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes.”<sup>240</sup> If such checkpoints were allowed, the Court reasoned, “there would be little check on the ability of the authorities to construct roadblocks for almost any conceivable law enforcement purpose.”<sup>241</sup> Under this logic, geofence warrants used to investigate ordinary crimes (i.e., those that do not pose an immediate hazard) seem to run afoul of *Edmond* and *Sitz*.

*Illinois v. Lidster* presents an apt comparison to geofence warrants, as the case involved a criminal investigation in search of leads.<sup>242</sup> Faced with a stale investigation of a fatal hit-and-run, law enforcement created an “information-seeking” checkpoint near the accident’s location.<sup>243</sup> The checkpoint blocked a portion of the highway so that officers could approach each vehicle, ask passengers if they had witnessed the accident, and hand passengers a flyer requesting assistance in identifying the vehicle and driver involved.<sup>244</sup> The Supreme Court upheld this checkpoint as constitutional because, unlike the *Edmond* checkpoint, it was not set up primarily to detect evidence of ordinary

---

237. See *supra* Part I.B.3.

238. *City of Indianapolis v. Edmond*, 531 U.S. 32, 39 (2000) (citing *Sitz*, 496 U.S. at 451).

239. *Id.* at 41 (“We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.”).

240. *Id.* at 44.

241. *Id.* at 42.

242. See 540 U.S. 419, 422 (2004).

243. *Id.* at 422, 424.

244. *Id.* at 422. Respondent Robert Lidster swerved into the checkpoint and nearly collided with it, and was subsequently arrested for driving under the influence. *Id.*

criminal wrongdoing.<sup>245</sup> In the Court's eyes, the key distinguishing factor from *Edmond* was that law enforcement in *Lidster* sought information from third parties unlikely to have themselves committed the crime under investigation.<sup>246</sup>

Like in *Lidster*, law enforcement has no suspect and no known witnesses when requesting a geofence warrant. But a geofence warrant is more like the checkpoint in *Edmond* than the one in *Lidster*. While *Lidster*'s checkpoint was in furtherance of a criminal investigation, it did not aim to "determine whether a vehicle's occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others."<sup>247</sup> As the geofence warrants surveyed above indicate, however, the government seeks geofence warrants precisely to reveal unknown perpetrators.<sup>248</sup> Inspection of geofence data is thus equivalent to law enforcement stopping each individual leaving an area, demanding his or her digital device, and checking its location history for evidence of a crime. This is precisely what the Fourth Amendment prohibits.<sup>249</sup>

### 3. Geofences as area warrants

Geofences are also analogous to area warrants. One commentator defines area warrants as "judicial warrants that specify the location and timing of a search without specifying the persons or objects to be searched."<sup>250</sup> In contrast to typical search warrants, an area warrant, such as an administrative warrant or a suspicionless search, "generally cannot provide much detail beyond . . . an address, a stated purpose, and general parameters for a search."<sup>251</sup> When an area warrant issues, it authorizes the government to search "every person, place, or thing in a specific location . . . based only on a showing of a generalized government interest."<sup>252</sup> Such searches are not predicated on

---

245. *Id.* at 427-28.

246. *Id.* at 423.

247. *Id.*; see also *id.* at 428 (Stevens, J., concurring in part and dissenting in part) ("There is a valid and important distinction between seizing a person to determine whether she has committed a crime and seizing a person to ask whether she has any information about an unknown person who committed a crime a week earlier.").

248. See *supra* Part II; see also, e.g., *supra* notes 46-48 and accompanying text.

249. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.").

250. Christopher Lee, Comment, *The Viability of Area Warrants in a Suspicionless Search Regime*, 11 U. PA. J. CONST. L. 1015, 1019 (2009).

251. *Id.* at 1044.

252. Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 263 (2011).

probable cause for each thing searched within the specific location,<sup>253</sup> so they cannot meet the usual standard required for warrants. Instead, the Supreme Court recognizes an exception for area warrants in cases where “requiring individualized showings of probable cause would prevent the government from addressing important health or safety concerns,” such as the need to conduct “[a] health or safety inspection of every home in a given area or every business in a particular industry.”<sup>254</sup> Because of this unique government rationale, these warrants can be predicated on *sui generis* area-wide probable cause.

The Supreme Court defined the constitutional limits of area warrants in *Camara v. Municipal Court*, which concerned a municipal government’s inspection of housing “based on its appraisal of conditions in the area as a whole, not on its knowledge of conditions in each particular building.”<sup>255</sup> In *Camara*, the government expected that many homes subject to search would be in compliance with housing codes.<sup>256</sup> As a result, the government’s inspections “would burden many law-abiding homeowners who had done nothing to trigger any suspicion of wrongdoing.”<sup>257</sup> Under ordinary Fourth Amendment jurisprudence, such inspections would be prohibited. The *Camara* Court, however, recognized an exception to the usual probable-cause requirement “because the inspections are neither personal in nature nor aimed at the discovery of evidence of crime,” meaning that “they involve a relatively limited invasion of the urban citizen’s privacy.”<sup>258</sup>

But the Court emphasized that “the importance of the government’s interest” in regulating health and safety and the “minimally intrusive nature of the search” were not, by themselves, sufficient to exempt housing inspections from the requirement of individualized suspicion.<sup>259</sup> The Court included in its test an exhaustion requirement, indicating that area warrants were only to be used as a last resort<sup>260</sup> and explaining the “unanimous agreement among those most familiar with this field that the *only* effective way to seek universal compliance with the minimum standards required by municipal codes is through routine periodic inspections of all structures.”<sup>261</sup> The Court

---

253. *Id.*

254. *Id.* at 262-63.

255. *See* 387 U.S. 523, 535-36 (1967).

256. *Primus, supra* note 252, at 264.

257. *Id.*; *see Camara*, 387 U.S. at 532-33 (emphasizing various ways in which administrative inspections burden each individual whose property is searched).

258. *Camara*, 387 U.S. at 537.

259. *Primus, supra* note 252, at 264.

260. *See Camara*, 387 U.S. at 539-40.

261. *Id.* at 535-36 (emphasis added).

emphasized that no home-inspection technique based on probable cause “would achieve acceptable results,”<sup>262</sup> and in the decade after *Camara* it struck down “many proposed administrative searches—even minimally intrusive ones—because alternative regimes predicated on individualized suspicion could reasonably serve the government’s interests.”<sup>263</sup>

The *Camara* test thus guides the analysis of whether geofence warrants are permissible area warrants. Instead of inspecting each home in an area based on the probability of housing code violations, geofence warrants allow law enforcement to inspect every digital device in an area based on the likelihood of evidence being found on a device. Many, if not most, devices with information returned will be unrelated to the investigation; many law-abiding people who did nothing to trigger suspicion of wrongdoing will be burdened. The Court in *Camara* made clear that such a search is only permissible in the context of an important public health and safety issue when no other investigative method would suffice.<sup>264</sup> Given this analysis, it seems unlikely that a geofence warrant, outside of a special situation or a dire exigency, could pass the high *Camara* bar.

#### 4. Takeaways

As seen through the *Ybarra* opinion and the other examples discussed in the previous Subparts, the probable-cause requirement is likely the main barrier to the constitutionality of geofence warrants. Geofence-warrant applications in their current form assert only that individual users (1) were at or near the scene of a crime; and (2) possessed a cell phone that sends data to Google.<sup>265</sup> This falls short of probable cause.

The first allegation, that a user was near the scene of the crime, clashes with *Ybarra*. In order to obtain a geofence warrant, the government may have to show—also in line with the Supreme Court’s checkpoint and area-warrant jurisprudence—that a special need beyond general law-enforcement activity, such as the risk of harm to public health or safety, is present.

The second allegation, that the user has a cell phone which sends data to Google, also seems to fall short of the *Ybarra* hurdle. Owning an iPhone or an Android phone is not a reason to believe that the individual “had committed, was committing, or was about to commit any offense under state or federal law,” and it is not “indicative of criminal conduct.”<sup>266</sup> Rather, it is indicative of

---

262. See *id.* at 537.

263. Primus, *supra* note 252, at 265–66.

264. *Camara*, 387 U.S. at 535–40.

265. See, e.g., *supra* notes 160–61 and accompanying text.

266. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

living in the twenty-first century and having the means to afford a smartphone.

Prior to receiving geofence-warrant data, investigators have no idea which individuals to scrutinize. All are treated as suspects on the basis of their devices' proximity to the crime scene. While probable cause is merely "a fair probability that contraband or evidence of a crime will be found in a particular place,"<sup>267</sup> that place cannot be an entire geographic region. Rather, the place must be each individual device caught in the net. The Constitution requires a basis for suspicion of an individual's wrongdoing, and this basis must go beyond naming an entire population or a blanket geographic region. Indeed, the Constitution requires that probable cause be established for *every individual* whose information is ensnared in the search, and probable cause cannot be satisfied by claiming that evidence of wrongdoing will likely appear in a general pool of data.<sup>268</sup> An affidavit merely showing that a crime took place in a certain geographic region at a certain time, while apparently acceptable to some courts, is constitutionally insufficient. And to the extent that courts have found this rationale adequate to issue geofence warrants, we disagree.

This is not the first time courts have used erroneous probable-cause analysis in the context of broad database searches. In a leading opinion on tower dumps,<sup>269</sup> *United States v. James*, the court held that probable cause was met because "there was a fair probability that data from the cellular towers in the area of the crimes," rather than data from each cellular device in the area, "would include cellular data related to the individual responsible for the robberies being investigated."<sup>270</sup> Stephen Henderson has explained, however,

---

267. *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

268. See *Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996) (holding that "a warrant to search 'all persons present' for evidence of a crime may only be obtained when there is reason to believe that all those present will be participants in the suspected criminal activity," and explaining that such a warrant is only appropriate for a locale "dedicated exclusively to criminal activity"); *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) ("[A]n 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity.").

269. Tower dumps and geofences share some similarities. A tower dump occurs when law enforcement asks a cell-service provider to produce the phone numbers of every device connected to a certain cell tower during a certain time period, usually near the scene of a crime when the crime was occurring. See Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014, 11:58 AM), <https://perma.cc/GL7N-SBR5>. The main differences between tower dumps and geofences are (1) that the SensorVault produces more precise location data than cell towers; and (2) that a tower-dump database search is narrower because providers can search one cell tower only. Google Amicus Brief, *supra* note 13, at 10-12, 14.

270. No. 18-cr-00216, 2019 WL 325231, at \*3 (D. Minn. Jan. 25, 2019). Despite being an unpublished district court opinion, *James* is a leading opinion because it is one of the

*footnote continued on next page*

that focusing probable cause on the group rather than the individual “would mean that a larger database is always to be preferred” by law enforcement, because “by definition there will be evidence of crime in that larger set.”<sup>271</sup> This would lead to an “absurd” understanding of probable cause, Henderson argues: “[A] prosecutor confident that a bank customer is committing tax fraud could access the combined records of *all* customers of that bank because, somewhere in there, she is very sure is evidence of crime.”<sup>272</sup> Instead, Henderson asserts, it must be the case that probable cause is required for “each person’s obtained records” in a tower dump, “meaning here each phone number contained within the dump.”<sup>273</sup> Indeed, the Supreme Court in *Camara* explained that while “in a criminal investigation, the police may undertake to recover specific stolen or contraband goods . . . public interest would hardly justify a sweeping search of an entire city conducted in the hope that these goods might be found.”<sup>274</sup> “Consequently, a search for these goods, even with a warrant, is ‘reasonable’ only when there is ‘probable cause’ to believe that they will be uncovered in a particular dwelling.”<sup>275</sup>

#### B. Issues with the Particularity Requirement

The Fourth Amendment mandates that the description within a search warrant identify the “specific place for which there is probable cause to believe that a crime is being committed,”<sup>276</sup> to ensure that searches “will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.”<sup>277</sup> Even if there is probable cause to search some users, geofence

---

few post-*Carpenter* opinions to address the constitutionality of tower dumps. See Shane Rogers, *Two Years of Carpenter*, COVINGTON: INSIDE PRIV. (July 7, 2020), <https://perma.cc/9A8M-CXXS>. Many of our arguments in this Part also apply to tower dumps. Individuals are swept into tower dumps for the same reason they are swept into geofences: proximity to the scene of the crime around the time when it occurred. But the *Carpenter* question is more relevant to tower-dump litigation than to geofence litigation, as corporations sometimes supply cell-tower information to law enforcement without a warrant. David Kravets, *Cops and Feds Routinely “Dump” Cell Towers to Track Everyone Nearby*, WIRED (Dec. 9, 2013, 5:15 PM), <https://perma.cc/KX4W-EPQW>.

271. Stephen E. Henderson, Response, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. SEE ALSO 28, 40-41 (2016).

272. *Id.* at 41.

273. *Id.*

274. *Camara v. Mun. Ct.*, 387 U.S. 523, 535 (1967).

275. *Id.*

276. *United States v. Hinton*, 219 F.2d 324, 326 (7th Cir. 1955).

277. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

warrants—which do not target a specific user or set of users<sup>278</sup>—struggle to achieve particularity because they do not describe a place for which there is probable cause to search *all* devices present.

Imagine a housing structure for which there is an ordinary, in-person search warrant. When a single warrant covers such an area, including more than one living unit in a multi-occupancy structure (or multiple single-occupancy structures), courts require “adequate probable cause for [the] search of *each* place.”<sup>279</sup> This is not an easy showing: As Wayne LaFave explains, it generally “requires a rather special set of facts.”<sup>280</sup> For example, “a generalized statement that a person involved in criminality has ‘control’ of the entirety of a multiple-occupancy structure will not suffice.”<sup>281</sup>

As noted above, geofence searches often include multi-occupancy structures within their boundaries. Yet law enforcement has not always adhered to the particularity standard required for such searches. Magistrate Judge Weisman noted this defect in his rejection of the initial pharmaceutical geofence application, writing that the government’s “inclusion of a large apartment complex in one of its geofences raises additional concerns” because it would allow the government to “obtain location information as to an individual who may be in the privacy of their own residence without any showing of probable cause related to that individual or her residence.”<sup>282</sup> Such information is invasive: Location data can reveal which room of a person’s home she is in, who is in the home with her, and more.<sup>283</sup>

---

278. In fact, one of the most infamous national security laws, section 702 of the Foreign Intelligence Surveillance Act, *see* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881a), requires more targeting than geofences do. Under this law, the government must task a “selector” to a provider, meaning that the government must provide an “account identifier such as an email address or telephone number,” and then the provider must disclose certain communications to or from that selector. U.S. DEP’T OF COM., U.S. DEP’T OF JUST. & U.S. OFF. OF THE DIR. OF NAT’L INTEL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCs AND OTHER EU LEGAL BASES FOR EU–U.S. DATA TRANSFERS AFTER *SCHREMS II*, at 7-8 (2020), <https://perma.cc/L4NX-AQYB>.

279. *State v. Ferrari*, 460 P.2d 244, 248 (N.M. 1969) (emphasis added).

280. 2 LAFAVE ET AL., *supra* note 116, § 3.4(e) n.89.

281. *Id.*; *see* *United States v. Clark*, 638 F.3d 89, 94-96 (2d Cir. 2011).

282. *In re the Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-mc-00297, 2020 WL 5491763, at \*5 n.7 (N.D. Ill. July 8, 2020) (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

283. *See supra* notes 33-34 and accompanying text (detailing the precision of SensorVault location information). In 2020, Google released reports analyzing location data to show how COVID-19 had changed movement patterns (and whether people were complying with stay-at-home orders). Casey Newton, *Google Uses Location Data to Show Which Places Are Complying with Stay-at-Home Orders—and Which Aren’t*, VERGE (Apr. 3, 2020, 2:00 AM EDT), <https://perma.cc/QAT6-JNFX>. Such reports reveal the precision with which Google chronicles users’ movements.

It is possible for law enforcement to cleverly craft a search protocol to make it sufficiently particularized. In fact, in the third denial of the pharmaceutical geofence application, Magistrate Judge Fuentes suggested that while law enforcement might not have probable cause for everyone present at *each* geofenced crime scene, it might have probable cause for everyone present at *all* (or multiple) geofenced crime scenes.<sup>284</sup> Law enforcement could have requested that Google return only location information for devices that registered LH in two or three geofences. At least one office adopted this approach in an investigation: In August 2018, police officers in Maine asked Google to return information only on users whose data appeared in more than one of the requested locations.<sup>285</sup> When crafted in this way—with returns limited to devices recorded across multiple geofences in the case of multiple crime scenes—geofence warrants may be sufficiently particularized.

## V. Constitutionality of Selective Expansion and Unmasking

Many geofence warrants authorize a second step, selective expansion, through which law-enforcement officials identify and seek additional information on individual devices from the original data pool.<sup>286</sup> Selective expansion can include location history from outside of the geofence's initial location and time boundaries.<sup>287</sup> In the subsequent, final step, law-enforcement officials require the targeted provider (so far, primarily Google) to unmask the identity of individuals in the data pool.<sup>288</sup>

These two steps can be interpreted as violative in several ways. Both selective expansion and unmasking grant executive officers unconstitutional discretion in the execution of a warrant. Furthermore, the selective-expansion step can be viewed as allowing officers to go beyond the specified scope of the warrant. Alternatively, the selective-expansion step can be viewed as authorizing additional (and wholly invalid) separate searches under a single warrant.

### A. Geofences as General Warrants

By authorizing multiple steps that are entirely subject to the direction of law enforcement, geofence warrants may grant officers unconstitutional

---

284. *In re the Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 755-56 (N.D. Ill. 2020).

285. Brewster, *supra* note 67; Mak, *supra* note 83.

286. *See supra* Part I.B.2.

287. *See supra* Part I.B.2.

288. *See supra* Part I.B.3.

discretion in warrant execution. As the Supreme Court wrote in *Marron v. United States*, “[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible.”<sup>289</sup> “As to what is to be taken,” the Court noted, “nothing is left to the discretion of the officer executing the warrant.”<sup>290</sup>

In striking down the general warrant at issue in the foundational English case *Wilkes v. Wood*, the Court of King’s Bench held that undue discretion was left to the King’s officers when they were instructed to “apprehend[] the authors, printers and publishers” of a radical newspaper.<sup>291</sup> The warrant allowed the officers discretion to search homes of their choosing and seize anything they deemed relevant.<sup>292</sup> The *Wilkes* court condemned the warrant because of the “discretionary power” it gave officials in deciding where to search and what to take.<sup>293</sup>

The U.S. Supreme Court enshrined the lessons of *Wilkes* and a contemporaneous English case, *Entick v. Carrington*,<sup>294</sup> in its canonical Fourth Amendment decision, *Boyd v. United States*.<sup>295</sup> The Court subsequently held that particularity is required for electronic searches, finding in *Berger v. New York* that a general wiretap granted “the officer a roving commission to ‘seize’ any and all conversations.”<sup>296</sup> Without “adequate judicial supervision or protective procedures,” an electronic search lacking probable cause and particularity, “[a]s with general warrants . . . leaves too much to the discretion of the officer executing the order.”<sup>297</sup>

Like general warrants, geofence warrants grant discretion to the executing law-enforcement officials. Officers can select users of their choosing and seize (through selective expansion or unmasking) further data from those users without judicial oversight.<sup>298</sup> The officers do not name these individuals in advance, nor do they provide affidavits specifying their justifications for selecting certain individuals.<sup>299</sup>

---

289. 275 U.S. 192, 196 (1927).

290. *Id.*; see *Arizona v. Gant*, 556 U.S. 332, 345 (2009) (“[T]he central concern underlying the Fourth Amendment . . . [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”).

291. (1763) 98 Eng. Rep. 489, 496, 498; Lofft 1, 14, 18.

292. See *id.* at 498, Lofft at 18.

293. *Id.*

294. (1765) 95 Eng. Rep. 807; 2 Wils. K.B. 275.

295. 116 U.S. 616, 625-27 (1886).

296. 388 U.S. 41, 58-59 (1967).

297. *Id.* at 59-60.

298. See *supra* Parts I.B.2-.3.

299. *Cf. United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (holding that a warrant authorizing the seizure of “any and all data” from a ship’s computer was  
*footnote continued on next page*

In its *Chatrie* briefing, the government argued that geofence-warrant discretion merely enabled officers to acquire *less* information than the constitutional maximum.<sup>300</sup> The government analogized its geofence warrant to the Playpen warrant, which allowed the FBI to search the computers of everyone who logged into Playpen, a site on the dark web for child sexual-abuse material, for thirty days.<sup>301</sup> In a Playpen case before the First Circuit, the court found that the warrant was sufficiently particular and allowed law enforcement to deploy the search “more discretely against particular users.”<sup>302</sup> Geofence warrants, however, can be distinguished from the Playpen warrant: The particularity requirement is more easily satisfied for seizures of contraband.<sup>303</sup> This was the case for the Playpen warrant, as the users who accessed contraband on the website provided an adequate basis for probable cause to search their devices.<sup>304</sup> By contrast, being in the vicinity of a crime scene is neither contraband nor sufficient to support probable cause on its own.<sup>305</sup>

#### B. Selective Expansions as Increases in Scope

The selective-expansion step may also be interpreted as an increase in the warrant’s scope without magistrate approval. Once the constitutional requirements of probable cause and particularity are met, the descriptions in a warrant are critical in limiting the resulting search.<sup>306</sup> For example, under a warrant particularized to a building’s first floor, authorities cannot search higher floors.<sup>307</sup> Even if the government specifies a selective-expansion protocol, a geofence warrant still only describes the data within its original

---

an invalid general warrant, as it gave executing officers total discretion as to what they would seize (quoting the warrant)).

300. See Government’s Response in Opposition to Defendant’s Motion for Suppression of Evidence Obtained Pursuant to Google Geofence Warrant at 19-20, *United States v. Chatrie*, No. 19-cr-00130 (E.D. Va. Nov. 19, 2019), 2019 WL 8227160, ECF No. 41 [hereinafter *Chatrie* Government’s Response].

301. *Id.*

302. *United States v. Anzalone*, 208 F. Supp. 3d 358, 363, 368 (D. Mass. 2016) (quoting the warrant’s affidavit), *aff’d*, 923 F.3d 1 (1st Cir. 2019).

303. 2 LAFAYETTE ET AL., *supra* note 116, § 3.4(f); see *United States v. Jenkins*, 680 F.3d 101, 106-07 (1st Cir. 2012) (holding that probable cause to believe contraband will be found in a certain place can satisfy the particularity requirement).

304. See *Anzalone*, 208 F. Supp. 3d at 368; *Chatrie* Government’s Response, *supra* note 300, at 20.

305. See *supra* Part IV.A.1.

306. 2 WAYNE R. LAFAYETTE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.10 (West 2021).

307. *Id.* § 4.10(a).

geographic coordinates and time frame. Searching data outside of those parameters is therefore outside the scope of the warrant, like searching the second floor of an apartment building when a search has only been authorized on the first floor.

Issues with searches beyond the scope of a warrant have arisen frequently in digital Fourth Amendment cases, in part because law enforcement can easily exceed specified bounds when accessing large pools of data. For example, in *United States v. Carey*, the Tenth Circuit held that a police officer searching for evidence of drug trafficking on a computer exceeded a warrant's scope when he clicked through picture files looking for evidence of child sexual-abuse material.<sup>308</sup> The court noted that "until he opened the first JPG file," the officer stated "he did not suspect he would find child pornography."<sup>309</sup> But once he saw the first image and developed probable cause to believe he would find more like it, the officer could not go searching through the computer without returning to a magistrate for another search warrant.<sup>310</sup>

As *Carey* illustrates, law-enforcement officers do not have probable cause to search any location data beyond the initial data dump until they have surveyed the data in that dump. And like in *Carey*, even when law-enforcement officers have developed probable cause to believe they will find more incriminating evidence in a certain user's location history, they may not be allowed to search through data outside of the original parameters (by requesting expansion from Google) until they receive further judicial authorization.

### C. Multiple Searches

Going a step further, recent federal appellate opinions indicate that selective expansion could be interpreted as a violation of the Fourth Amendment maxim that several searches cannot be authorized by one warrant. In *Marron*, the Supreme Court explained that the particularity requirement "prevents the seizure of one thing under a warrant describing another."<sup>311</sup> A warrant "authorizes only one search,"<sup>312</sup> and "if a place is to be searched a second time the proper procedure is to obtain a second warrant based on an affidavit explaining why there is now probable cause notwithstanding the execution of the earlier warrant."<sup>313</sup>

---

308. 172 F.3d 1268, 1272-73 (10th Cir. 1999).

309. *Id.* at 1273.

310. *Id.*

311. *Marron v. United States*, 275 U.S. 192, 196 (1927).

312. *United States v. Keszthelyi*, 308 F.3d 557, 568-69 (6th Cir. 2002).

313. 2 LAFAVE ET AL., *supra* note 116, § 3.4(j).

The multiple steps of the geofence warrant may amount to several searches of user accounts due to the underlying technology. One SensorVault query produces the initial data dump, but once that query is complete and the data has been turned over to law enforcement, a second query is necessary in order to produce the selective-expansion data that law enforcement has requested.<sup>314</sup>

While the Supreme Court has not weighed in on the issue, some courts have held that each query of an electronic database is a search, and multiple queries amount to multiple searches. The Second Circuit recently explained that, in the context of a database containing foreign-intelligence information, each query is a separate search that may require a separate warrant.<sup>315</sup> Similarly, the Ninth Circuit has held that law enforcement cannot conduct subsequent queries of the information on a computer beyond the initial query authorized by a warrant, because the government “should not be able to comb through [the defendant’s] computers plucking out new forms of evidence that the investigating agents have decided may be useful” after it failed to find all the evidence it would have liked in the initial search.<sup>316</sup>

Geofence warrants authorize exactly what the Ninth Circuit prohibits: They allow the government to comb through Google’s database for additional evidence of wrongdoing after failing to find all of its desired evidence in the initial data dump.<sup>317</sup> When law enforcement searches data outside of the initially specified time and geographic range, officers may be undertaking multiple searches, an unconstitutional action under a single warrant.

## **VI. Corporate Policy and Fourth Amendment Protections**

Geofence warrants raise questions regarding the role that technology companies play in maintaining Fourth Amendment protections. Relative to the invasive and widespread use of geofences, state and federal legislators have taken little notice of the practice.<sup>318</sup> And geofence-warrant doctrine is virtually nonexistent in the courts, with no binding precedent as of this writing.<sup>319</sup> In this void, privacy protections are governed by corporate policy. That Google is regulating state and federal use of geofence warrants has

---

314. *See supra* Part I.B.2; Google Amicus Brief, *supra* note 13, at 12-14.

315. *United States v. Hasbajrami*, 945 F.3d 641, 669-73 (2d Cir. 2019).

316. *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013).

317. *See supra* Part I.B.2.

318. *See* Issie Lapowsky, *New York Lawmakers Want to Outlaw Geofence Warrants as Protests Grow*, PROTOCOL (June 16, 2020), <https://perma.cc/3HPW-BKT9> (noting that New York’s proposed ban on geofence warrants “would be the first in the United States”).

319. *See supra* Part III.

significant implications for (1) the way that Fourth Amendment analysis is and should be conducted; (2) how user's rights should be protected; and (3) how much deference government litigation positions are owed with regard to geofence surveillance.

This Part begins by discussing the source of the vacuum in which Google has been able to take control: legislative inaction, particularly by the federal government. It then considers (1) Google's reasons for choosing to implement its policies; (2) law enforcement's acquiescence; and (3) the implications of this arrangement on democratic accountability, consumer privacy, and the role of the courts.

### A. Absence of Legislation

Legislative rules could govern and regulate the use of geofence warrants, going above the constitutional floor or mandating protections in the absence of a precedential holding.<sup>320</sup> But Congress has displayed little inclination to act. Similarly, although a few promising signs have emerged in certain state legislatures, no bill that would curb geofence use by law enforcement has neared passage.

At the time of writing, Congress has not indicated a willingness to regulate law enforcement's access to geofence data. The only direct mention of geofence warrants in Congress came in a July 2020 appearance by the chief executive officers of Alphabet (Google's parent company), Amazon, Apple, and Facebook before the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law.<sup>321</sup> During that hearing, Representative Kelly Armstrong explained to Alphabet CEO Sundar Pichai that he believed geofence warrants were "the single most important issue" before the Subcommittee, because such warrants fall short of the Fourth Amendment's probable-cause and particularity requirements.<sup>322</sup> "People would be terrified to know,"

---

320. Cf. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) (explaining how the Stored Communications Act created a "set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information"); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 24-26 (2004) (detailing how the Wiretap Act set protections above the constitutional floor after the Supreme Court's decision in *Berger*).

321. See *User Clip: Google "Geofence" Warrants Questioned*, C-SPAN (July 29, 2020), <https://perma.cc/WR4C-66TC>. A 2019 letter to Google from the House Committee on Energy and Commerce also expressed concern about the SensorVault's storage of precise location data. Letter from U.S. House of Representatives Comm. on Energy & Com. Members to Sundar Pichai, Chief Exec. Officer, Google 1-3 (Apr. 23, 2019), <https://perma.cc/JSW7-W9AY>. No response from Google has been reported.

322. *User Clip: Google "Geofence" Warrants Questioned*, *supra* note 321, at 02:06-02:10.

Representative Armstrong emphasized, “that law enforcement can grab general warrants and get everybody’s information anywhere.”<sup>323</sup>

There has been slightly more movement at the state level. In April 2020, legislators in New York’s Assembly and Senate introduced legislation to ban law enforcement’s use of geofence searches.<sup>324</sup> New York’s proposed ban—the first such legislation nationally—would prohibit “the search, with or without a warrant, of geolocation data of a group of people who are under no individual suspicion of having committed a crime.”<sup>325</sup> As of this writing, however, neither bill has advanced out of committee.<sup>326</sup>

Some states have their own data privacy regimes that grant additional protections beyond federal requirements. For example, California’s Electronic Communications Privacy Act (CalECPA) generally requires a warrant to access “electronic device information” regardless of who possesses the data.<sup>327</sup> Other states, including Maine,<sup>328</sup> Massachusetts,<sup>329</sup> Minnesota,<sup>330</sup> Montana,<sup>331</sup> New Hampshire,<sup>332</sup> Rhode Island,<sup>333</sup> Utah,<sup>334</sup> and Vermont<sup>335</sup> have similar judicial or statutory requirements for a warrant to obtain digital location

---

323. *Id.* at 01:56-02:00.

324. Assemb. 10246-A, 243d Leg., Reg. Sess. (N.Y. 2020), <https://perma.cc/8BQJ-VF79>; S. 8183, 243d Leg., Reg. Sess. (N.Y. 2020), <https://perma.cc/M4Z7-L7QB>.

325. N.Y. Assemb. 10246-A; N.Y.S. 8183; Lapowsky, *supra* note 318; *see also* Uberti, *supra* note 30; Mike Maharrey, *New York Bill Would Ban Geolocation Tracking and Geofencing Warrants*, TENTH AMEND. CTR. (Apr. 15, 2020), <https://perma.cc/M2YD-J4F4>; Press Release, Surveillance Tech. Oversight Project, S.T.O.P. Welcomes Introduction of NY Geolocation Tracking Ban (Apr. 10, 2020), <https://perma.cc/4A7E-2FPY>.

326. *Assembly Bill A10246A*, N.Y. ST. SENATE, <https://perma.cc/6YSR-WXWN> (archived Oct. 23, 2021); *Senate Bill S8183*, N.Y. ST. SENATE, <https://perma.cc/DV9L-USFT> (archived Oct. 23, 2021). Another bill in Utah that would have placed some limits on the use of geofence warrants gained traction in 2021 but ultimately did not pass. H.R. 251, 64th Leg., 2021 Gen. Sess. (Utah 2021), <https://perma.cc/C63U-97KH>; *H.B. 251 Electronic Location Amendments*, UTAH ST. LEGISLATURE, <https://perma.cc/248V-5MGJ> (archived Jan. 29, 2022); Art Raymond, *Bill Targets How Police Use Info Showing Where You’ve Been and What Internet Searches You Make*, DESERET NEWS (Feb. 25, 2021, 9:52 PM MST), <https://perma.cc/4SYY-L96F>.

327. CAL. PENAL CODE §§ 1546(g), 1546.1(c) (West 2021).

328. ME. REV. STAT. ANN. tit. 16, § 648 (2021).

329. *Commonwealth v. Augustine*, 4 N.E.3d 846, 863-66 (Mass. 2014).

330. MINN. STAT. § 626A.42 subd. 2 (2021).

331. MONT. CODE ANN. § 46-5-110 (2021).

332. N.H. REV. STAT. ANN. § 644-A:2 (2021).

333. 12 R.I. GEN. LAWS § 12-32-2 (2021).

334. UTAH CODE ANN. § 77-23c-102 (West 2021).

335. VT. STAT. ANN. tit. 13, §§ 8101, 8102 (2021).

information.<sup>336</sup> Warrants governed by CalECPA must include the “time periods covered,” the “applications or services covered, and the types of information sought,” and they must “describe with particularity the information to be seized by specifying . . . the target individuals or accounts.”<sup>337</sup> CalECPA’s particularity requirement was briefed in *Dawes* as independent grounds to invalidate the warrant.<sup>338</sup> It is not yet clear, however, whether existing state privacy laws can address the concerns of geofence warrants. And many states lack data privacy regimes altogether.

## B. Corporate Constitutional Policy

Because of legislative inaction, private corporate policy has replaced democratic governance for geofence warrants. When judges consider geofence warrants, they should therefore note that what comes before them is not the product of democratically considered legislation, but rather the result of internal policy decisions by a single corporation, Google, with which law enforcement has complied.<sup>339</sup>

Early geofence warrants sought subscriber information and location history for all devices within the geofence—essentially an unrestrained,

---

336. See generally *State Location Privacy Policy*, ELEC. PRIV. INFO. CTR., <https://perma.cc/55CU-JSWK> (archived Oct. 23, 2021) (tracking pending and passed state legislation focused on location privacy); *Cell Phone Privacy*, ACLU, <https://perma.cc/2D6E-VE6Y> (archived Oct. 23, 2021) (highlighting the ACLU’s various efforts to increase cell phone users’ privacy rights). For those users willing to proactively limit what location (and other personal) data is held by mobile carriers and technology corporations, the California Consumer Privacy Act (CCPA) protects any personal information that “identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,” including geolocation data. CAL. CIV. CODE § 1798.140(o)(1) (West 2021). Under the CCPA, an individual can find out what types of personal data a business has collected and how such information is to be used. Individuals can also direct businesses to (1) delete their personal information if certain conditions are met; or (2) refrain from selling their data to third parties. *Id.* §§ 1798.100, .105, .110, .115, .120, .130, .135.

337. CAL. PENAL CODE § 1546.1(d)(1) (West 2021).

338. See *Dawes* Motion to Quash & Suppress, *supra* note 81, at 16–19. CalECPA, in contrast to similar federal laws, includes a statutory suppression remedy. Compare PENAL § 1546.4(a), with 18 U.S.C. §§ 2703, 2708.

339. This Subpart’s discussion builds on literature examining (1) how a lack of legislation can affect the exercise of constitutional rights; and (2) the role of corporations in this context. See generally Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 575–78, 653–54 (2018) (noting that law enforcement increasingly uses unregulated hacking technology to access encrypted computer systems); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1601–03 (2018) (exploring how private platforms’ policies increasingly control public debate, free speech, and democratic norms).

unmasked data dump.<sup>340</sup> In response to these broad requests, Google adopted an internal policy of objecting to any request that was not a probable-cause search warrant.<sup>341</sup> It also created the current three-step process in an effort to narrow the amount of identifying information produced.<sup>342</sup> Without judicial or legislative action, Google essentially imposed a warrant requirement and ex ante search protocols. The corporation even filed an amicus brief in *Chatrie* asserting that its own policy should be the constitutional minimum.<sup>343</sup>

And law enforcement has deferred to Google's policy. Consequently, most affidavits accompanying geofence warrants are boilerplate, sharing the same multistep form and general supporting statements.<sup>344</sup> Law enforcement has apparently decided that it is better to avoid litigation against well-resourced Google and not challenge its policy.

Google's power in the geofence-warrant process parallels the larger social and political power of technology companies. As Alan Rozenshtein writes, "[b]y entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of surveillance intermediaries: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance."<sup>345</sup> In recent years, these surveillance intermediaries have increasingly challenged subpoenas and search warrants; commentators have tied this change to consumer privacy concerns after Edward Snowden's 2013 surveillance disclosures.<sup>346</sup> In one notable instance, Microsoft invoked its duty to its customers when it sued the federal government over the routine inclusion of secrecy orders alongside search warrants.<sup>347</sup> The threat of Google litigating in

---

340. Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

341. See, e.g., Affidavit ¶ 1 n.1, *In re the Search of Info. Regarding Accts. Associated With Certain Location and Date Info.*, No. 18-mj-00169 (W.D. Tex. Jan. 10, 2019), ECF No. 9-1 ("Google has indicated that it believes a search warrant is required to obtain the location data sought in this application.").

342. See Declaration of Sarah Rodriguez, *supra* note 10, ¶ 5.

343. See *supra* notes 199-201 and accompanying text.

344. See, e.g., sources cited *supra* note 80.

345. Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 105 (2018) (emphasis omitted); see also Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) ("The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not.").

346. See *Developments in the Law—More Data, More Problems*, 131 HARV. L. REV. 1714, 1726-27 (2018) (discussing the rise in litigation "challenging the government over requests for information" since the Snowden revelations).

347. See Brad Smith, *Keeping Secrecy the Exception, Not the Rule: An Issue for Both Consumers and Businesses*, MICROSOFT: MICROSOFT ON THE ISSUES (Apr. 14, 2016), <https://perma.cc/5Z5G-TGF5>.

the geofence context fits into this broader trend.<sup>348</sup> But while Google may have post-Snowden economic incentives to consider privacy concerns, it remains a body with little direct accountability. Absent legislation, Google is beholden only to its shareholders and its corporate purpose.

Privacy “on the ground” thus remains the product of corporate norms and private review processes.<sup>349</sup> While the European Union has mandated a robust privacy regime under the General Data Protection Regulation (GDPR),<sup>350</sup> the United States remains a regulatory patchwork lacking meaningful, binding national privacy requirements.<sup>351</sup> Without clear standards from legislation, corporations fashion their own protocols and thresholds for responding to subpoenas, warrants, and other law-enforcement requests.<sup>352</sup> Democratic oversight is dangerously absent, a shortcoming that even some technology companies are eager to see remedied. As Apple CEO Tim Cook told the

---

348. See Brewster, *supra* note 67; Rozenshtein, *supra* note 345, at 109 (“Intermediaries couple a proceduralism that rejects voluntary cooperation with government requests to an aggressive litigiousness against government demands for data and restrictions on publicizing those requests.” (emphasis omitted)).

349. See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261-63 (2011) (describing the rise of corporate privacy audits, privacy certification programs, and chief privacy officers).

350. Council Regulation 2016/679, 2016 O.J. (L 119) 1; see *The EU General Data Protection Regulation: Questions and Answers*, HUM. RTS. WATCH (June 6, 2018, 5:00 AM EDT), <https://perma.cc/M6A3-RYHV> (surveying the GDPR’s various requirements, including consumer consent, special protections for sensitive information, disclosure, privacy by design, and the right to be forgotten).

351. See Michael Beckerman, Opinion, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), <https://perma.cc/RDA7-T8S9> (arguing that federal inaction on data privacy legislation has resulted in “inconsistent treatment of data depending on a variety of factors, including the residency of the consumer and the type of businesses with whom they interact”). The standards that do exist are long outdated, with Congress continually refusing to update the Electronic Communications Privacy Act of 1986 (ECPA), which rests on an understanding of technology that is now obsolete. See *ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1 (2013) (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary) (“The Electronic Communications Privacy Act of 1986 . . . is complicated, outdated, and largely unconstitutional.”); *id.* at 48 (statement of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.) (“The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2013, ECPA frustrates users’ reasonable expectations of privacy.”); see also Kerr, *supra* note 320, at 1208 (noting that the Stored Communications Act, which forms part of ECPA, “is a bit outdated and has several gaps in need of legislative attention”).

352. The absence of legislation also allows corporations to self-regulate in other realms traditionally protected by the Constitution, including speech. See Klonick, *supra* note 339, at 1615, 1666-69 (describing how moderation by private online platforms shapes U.S. speech norms).

European Parliament, “our own information . . . is being weaponized against us with military efficiency.”<sup>353</sup> “Scraps of data,” Cook noted, “each one harmless enough on its own, are carefully assembled, synthesized, traded, and sold.”<sup>354</sup> Accordingly, after he praised “the transformative work of the European institutions tasked with a successful implementation of the GDPR,” Cook voiced Apple’s “full support of a comprehensive federal privacy law in the United States.”<sup>355</sup>

As it currently stands, corporations are free to shift their privacy policies in response to global events, political currents, and economic incentives. When Apple announced that it planned to scan U.S. iPhones and their encrypted messages for images of child sexual abuse, for example, the Electronic Frontier Foundation decried the decision as “a shocking about-face for users who have relied on the company’s leadership in privacy and security.”<sup>356</sup> After this and other backlash, Apple reversed its decision.<sup>357</sup>

But not all shifts are protective, and some shifts are less protective than others. Although Google has announced the development of a “Privacy Dashboard” for future rollout to Android users,<sup>358</sup> this feature will offer fewer tracking protections and consent workflows than Apple’s current iPhone operating system.<sup>359</sup> And Android phones, relative to iPhones, are more likely to be owned by poorer consumers.<sup>360</sup> As a result, if geofence warrants remain pervasive, those caught up in data returns from Google (or possibly other corporations) will disproportionately be Android users, on the whole a less

---

353. Eur. Data Prot. Supervisor, *Keynote Address from Tim Cook, CEO, Apple Inc.*, YOUTUBE, at 05:41-05:50 (Oct. 24, 2018), <https://perma.cc/8SAB-ELYW>.

354. *Id.* at 06:15-06:25.

355. *Id.* at 08:11-08:20, 08:52-08:59.

356. India McKinney & Erica Portnoy, *Apple’s Plan to “Think Different” About Encryption Opens a Backdoor to Your Private Life*, ELEC. FRONTIER FOUND. (Aug. 5, 2021), <https://perma.cc/Y7Z4-2SRA>; see Frank Bajak & Barbara Ortutay, *Apple to Scan U.S. iPhones for Images of Child Sexual Abuse*, AP NEWS (Aug. 6, 2021), <https://perma.cc/2WAD-HSUV>.

357. See Carly Page, *Apple Quietly Pulls References to Its CSAM Detection Tech After Privacy Fears*, TECHCRUNCH (Dec. 15, 2021, 6:24 AM PST), <https://perma.cc/P5AC-MKH9>.

358. See Sarah N-Marandi, *What’s New in Android Privacy*, ANDROID DEVS. BLOG (May 18, 2021), <https://perma.cc/4CYN-E6E9>.

359. Gerrit De Vynck, *Google Announces New Privacy Features for Android Phones—but Stops Short of Limiting Ad Tracking*, WASH. POST (May 18, 2021, 8:53 PM EDT), <https://perma.cc/47XW-ZVJ8>.

360. See Press Release, Slickdeals, *iPhone Users Spend \$101 Every Month on Tech Purchases, Nearly Double of Android Users, According to a Survey Conducted by Slickdeals* (Oct. 30, 2018), <https://perma.cc/4JY7-Y9W2>; see also Jim Edwards, *Here’s Why Developers Keep Favoring Apple Over Android*, SLATE (Apr. 4, 2014, 1:23 PM), <https://perma.cc/M5QB-9GE8>.

wealthy group. Absent legislation or executive action, the only chance of addressing such inequities may be through corporate policy.

Given our current regulatory vacuum, the role of courts in assessing geofence warrants is paramount. When a court considers a geofence warrant, there is a danger that it will uncritically rely on whatever information the government presents. Indeed, some commentators have argued that federal magistrates are subject to Department of Justice capture.<sup>361</sup> If courts uncritically rely on government positions regarding geofence warrants, they are transitively subject to Google capture. Courts must remain vigilant in enforcing the underlying probable-cause and particularity requirements of geofence warrants, and they should not simply rubber-stamp Google's *ex ante* search protocols. While Google's procedures may narrow the scope of a geofence warrant, they do not automatically create a search that is acceptable under the Fourth Amendment. In particular, courts should be skeptical of discretionary selective expansion, where law enforcement returns to and negotiates with Google instead of a magistrate to seek an expanded search.<sup>362</sup> Courts cannot unilaterally stop consumer data from being used in a widespread surveillance regime. But they can prevent corporate technology giants from replacing the constitutionally mandated check of a neutral judiciary.

## Conclusion

Geofence warrants raise important Fourth Amendment questions. Courts have yet to engage deeply with issues of probable cause, particularity, and search expansion as they relate to geofences. And with corporate procedural demands shaping the legal terrain, law enforcement's tendency toward minimally specific warrants has faced little resistance. Without legislative action or increased judicial scrutiny of geofence warrants, undemocratic, discretionary corporate policy will continue to shape location-history protections.

As a closing note: Many commentators have highlighted the utility of geofence warrants, explaining that they "greatly enhance[] investigations,"<sup>363</sup> "help authorities catch criminals,"<sup>364</sup> and so on. These comments may be true,

---

361. See Mayer, *supra* note 339, at 651 ("In the district courts in particular, federal prosecutors are consummate repeat players . . . . The result appears to be a (mild) form of regulatory capture, in which prosecutorial arguments receive unusual deference." (footnote omitted)).

362. See *supra* notes 196-97 and accompanying text.

363. Devon Alan Frankel, Digital Dragnet: Geofence Warrants and Their Constitutional Issues 1 (2020), <https://perma.cc/8Z32-HD3U>.

364. Wendy Davis, *Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, but Is It Unconstitutional?*, ABA J. (Dec. 1, 2020, 1:50 AM CST), <https://perma.cc/>  
*footnote continued on next page*

but they miss the point. Geofence warrants are indeed a powerful investigative tool. The same can be said for Carpenter’s cell-site location information,<sup>365</sup> the eavesdrop orders placed on Berger’s conversations,<sup>366</sup> and the door-to-door search used to find and arrest Wilkes.<sup>367</sup> Such is the burden of the Bill of Rights: “Privacy comes at a cost.”<sup>368</sup>

---

J2GK-S3JU. Sandra Doorley, president of the District Attorneys Association of the State of New York and a district attorney in Monroe County, noted that geofence warrants have “proven to be helpful in solving crimes such as pattern burglaries, arsons and sexual assaults.” *Id.* (quoting Doorley). As previously discussed, carefully crafted geofence-warrant applications for these pattern crimes could pass constitutional muster. *See supra* notes 284-85 and accompanying text.

365. *See* *Carpenter v. United States*, 138 S. Ct. 2206, 2220-21 (2018) (placing limits on the use of this information).

366. *See* *Berger v. New York*, 388 U.S. 41, 58-59 (1967) (placing limits on the use of this practice).

367. *See* *Wilkes v. Wood* (1763) 98 Eng. Rep. 489, 498-99; Lofft 1, 18-19 (placing limits on the use of this technique).

368. *Riley v. California*, 573 U.S. 373, 401 (2014).

UNITED STATES of America  
v.  
Okello T. CHATRIE, Defendant.

Criminal Case No. 3:19cr130  
United States District Court for the Eastern District of Virginia  
(Richmond Division)

Filed 03/03/2022  
(Version Presented Here Edited by Brett Diehl)

M. Hannah Lauck, United States District Judge

## **I. Introduction**

\*<sup>1</sup> Ratified in 1791, the Fourth Amendment to the United States Constitution guarantees to the people the right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based “upon probable cause” and unless it “particularly describ[ed] the place to be searched, and the persons or things to be seized.” *Id.* The Supreme Court of the United States has since applied the principles embodied in this language to constantly evolving technology—from recording devices in public telephone booths, *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); to thermal-imaging equipment, *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001); and, most recently, to cell-site location data, *Carpenter v. United States*, --- U.S. ----, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018).

This case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. In recent years, technology giant Google (and others) have begun collecting detailed swaths of location data from their users. Law enforcement has seized upon the opportunity presented by this informational stockpile, crafting “geofence” warrants that seek location data for every user within a particular area over a particular span of time. In the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment. In the instant case, although the Motion to Suppress must ultimately be denied, the Court concludes that this particular geofence warrant plainly violates the rights enshrined in that Amendment.

## **II. Findings of Fact and Procedural History**

### **A. Findings of Fact<sup>1</sup>**

...

### **3. Google's Collection and Production of Location Data**

#### **a. Google's Suite of Location Services**

Google collects detailed location data on “numerous tens of millions” of its users. (ECF No. 96-1, at ¶ 13; ECF No. 201, at 205.) It acquires and stores this data through one of at least three services: (1) Location

History, (2) Web and App Activity (“WAA”), and (3) Google Location Accuracy (“GLA”). Google only searches Location History when it receives a geofence warrant.

### **i. Location History**

Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data. Google developed Location History to allow users to view their Location History data through its “Timeline” feature, a depiction of a user’s collected Location History points over time. (ECF No. 96-1, at ¶ 5; see ECF No. 202, at 79.) According to Google, this permits Google account holders to “choose to keep track of locations they have visited while in possession” of their mobile device. (ECF No. 96-1, at ¶ 4.) Importantly, Location History also supports Google’s advertising revenue.<sup>9</sup> For instance, McGriff testified that Location History data serves Google’s advertising business by providing “store visit conversions” or “ads measurement” to businesses based on user location. (ECF 201, at 196–97.) Without identifying any individual user, this “store conversion” data can follow a particular ad campaign and identify “how many users who saw a particular ad campaign actually went to one of those stores.” (ECF No. 201, at 197.) Google’s “radius targeting” also allows—again without identifying any user—“a business to target ads to users that are within a certain distance of that business.” (ECF No. 201, at 198.)

Location History is powerful: it has the potential to draw from Global Positioning System (“GPS”) information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol (“IP”) address information, and the signal strength of nearby Wi-Fi networks. According to Agent D’Errico, Location History logs a device’s location, on average, every two minutes.<sup>10</sup> Indeed, Location History even allows Google to “estimat[e] ... where a device is in terms of elevation.” (ECF No. 202, at 95.) McGriff testified that this capability helps locate someone in an emergency, or try to “determine if you are on the second [or first] floor of the mall” if the Google Maps directory has launched to help a user navigate indoors. (ECF No. 202, at 95–96.)

\*4 Google stores this data in a repository known as the “Sensorvault” and associates each data point with a unique user account. (ECF No. 201, at 130.) The Sensorvault contains a substantial amount of information. McGriff testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and receives and stores *all* location history data in the Sensorvault to be used in ads marketing. Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data, and then uses the data to, for instance, assist decision-making in Google Maps. As another example, Google uses this data to depict whether certain locations are busy during particular hours. Both McGriff and Rodriguez declared that, to identify users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence. (ECF No. 96-1, at ¶ 23 (“Google must search across *all* [Location History] data,” and “run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant.”); ECF No. 96-2, at ¶ 7 (“Google must conduct the search across *all* [Location History] data.”).) Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.

Still, Location history is off by default. A user can initiate, or opt into, Location History either at the “Settings” Level, or when installing applications such as Google Assistant, Google Maps, or Google Photos. Although the specific software pathway each user sees at any given moment can differ based on numerous factors, McGriff acknowledged that it was “possible that a user would have seen the option” to opt into

Location History multiple times across multiple apps. (ECF No. 202, at 77–78.) For instance, Google may prompt the user to enable Location History first in Google Maps, then again when he or she opens Google Photos and Google Assistant for the first time.<sup>11</sup>

Once a user opts into Location History, Google is “always collecting” data and storing *all* of that data in its vast Sensorvault, even “if the person is not doing anything at all with [his or her] phone.” (ECF No. 201, at 114–15; *see* ECF No. 201, at 115 (“Once enabled, [Google is] now collecting [the user’s] location history all the time.”).) Even if a user enables Location History through an application and later deletes that app, Location History will “still collect[ ]” data on the user because Location History is tied to an individual’s Google *account*, not to a *specific app*. (ECF No. 201, at 123–24.) Thus, after a user opts into the service, Location History tracks a user’s location across every *app* and every *device* associated with the user’s account. Approximately one-third of all active Google users have Location History enabled on their accounts.

In certain circumstances, Google can estimate a device’s location down to three meters. Location History cannot, however, pinpoint an individual’s location with absolute precision. Instead, Google *estimates* a phone’s coordinates. When Google, through Location History, reports a device’s estimated location by placing a point on a map, it also depicts around that point a “confidence interval”—a circle of varying sizes—which indicates Google’s confidence in its estimation. (ECF No. 201, at 38, 212; ECF No. 202, at 253–54.) The smaller the circle around a phone’s estimated location, the more confident Google is in that phone’s exact location, and *vice versa*. In general, “Google aims to accurately capture roughly 68 percent of users” within its confidence intervals. (ECF No. 201, at 213.) “[I]n other words, there[ is] a 68 percent likelihood that a user is somewhere inside” the confidence interval. (ECF No. 201, at 213.)

## **ii. Web and App Activity**

Web and App Activity collects a wider variety of information than Location History. If a user opts into WAA and has authorized all other requisite device permissions, WAA collects certain data points when a user *affirmatively engages* in certain activities.<sup>12</sup> For example, when a user performs a Google search, Google may, through WAA, keep a record of that search so that it can “automatically suggest[ ]” that search to the user at a later time. (ECF No. 96-1, at ¶ 16.) Google maintains that WAA allows a user to “experience faster searches and more helpful app and content recommendations.” (ECF No. 96-1, at ¶ 16.) “Some of [the data obtained through WAA] can include location information, although the source of the location information will vary depending on the activity, the device, and the user’s other settings.” (ECF No. 96-1, at ¶ 16.) Location History “and WAA are separate services that store data in separate databases.” (ECF No. 96-1, at ¶ 16.) That is, “WAA data is not used to calculate the locations that are stored in [Location History], and completing a search across [Location History] data does not search or draw on WAA data in any way.” (ECF No. 96-1, at ¶ 16.)

## **iii. Google Location Accuracy**

\*5 Lastly, Google Location Accuracy—only available on Android devices<sup>13</sup>—allows a user’s phone to draw in location data from sources other than GPS information. “If a user has the GLA setting on, the Android[ device’s] location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors[ ] to estimate the device’s location.” (ECF No. 96-1, at ¶ 17.) Thus, “the device’s location information that is sent to and stored in [Location History] ... may be calculated using not only GPS-sourced data, but also [more detailed] WiFi-or cell-sourced data from the GLA database.” (ECF No. 96-1, at ¶ 17.) “In other

words, GLA data might be used by the device to calculate a [more precise] location data point that is then stored in [Location History].” (ECF No. 96-1, at ¶ 17.) Like WAA, Google generally stores GLA data separate from Location History information.

Again, as a general matter, Google appears to draw only from Location History to produce records for geofence requests, as WAA and GLA do not collect enough data points to pinpoint “devices within a certain period of time within a certain radius.” (ECF No. 202, at 138; *see* ECF No. 201, at 211; ECF No. 96-1, at ¶¶ 20–22.) In keeping with this principle, here, Google only produced to law enforcement information from its Location History database.

...

#### **d. Google's Process in Answering a Geofence Warrant**

Geofence warrants represent “a novel but rapidly growing [investigatory] technique.” (ECF No. 59-1, at 8.) When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the “geofence,” often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time. (*See* ECF No. 96-2, at ¶ 4.) The requested time windows for these warrants “might span a few minutes or a few hours.” (ECF No. 96-2, at ¶ 4.)

In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google “observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate ... increased over 500% from 2018 to 2019.” (ECF No. 59-1, at 8.) In 2019, Google received “around 9,000 total geofence requests.”<sup>18</sup> And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States. Google, *Supplemental Information on Geofence Warrants in the United States* (last visited Mar. 1, 2022), <https://bit.ly/3o7Znqc>.

\*<sup>9</sup> Google began to take issue with certain early geofence warrants because the requests were too broad. As related by Legal Investigations Specialist Rodriguez, the warrants “sought [Location History] data that would identify *all* Google users who were in a geographical area in a given time frame.” (ECF No. 96-2, at ¶ 5 (emphasis added).) Thus, in 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice (“CCIPS”), to develop internal procedures on how to respond to geofence warrants. “To ensure privacy protections for Google users, ... Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures.” (ECF No. 96-2, at ¶ 5.) Seemingly developed as a result of Google's collaboration with CCIPS, this de-identification and narrowing “protocol typically ... entails a three-step process.” (ECF No. 96-2, at ¶ 5; *see* ECF No. 202, at 553.) As noted earlier, the Court draws its understanding of this process from an amalgam of in-person testimony and a declaration submitted by current Google Tooling and Programs Lead and former Legal Specialist Sarah Rodriguez.

#### **i. Step 1**

*First*, at Step 1, law enforcement receives a warrant “compelling Google to disclose a *de-identified* list of all Google user[s]” whose Location History data indicates were within the geofence during a specified timeframe. (ECF No. 96-2, at ¶ 6 (emphasis added).) In response to the warrant, Google must “search ... *all*

[Location History] data to identify users” whose devices were present within the geofence during the defined timeframe. (ECF No. 96-2, at ¶ 7; ECF No. 96-1, at ¶ 23.) “Google does not know which users may have ... saved [Location History] data before conducting th[is] search.” (ECF No. 96-2, at ¶ 7.)

Rodriguez stated that, as part of this first step, Google provides the Government with responsive user records identified in the Sensorvault. Google deems a record “responsive” if a user's estimated location (*i.e.*, the stored coordinates of the phone in Location History) falls within the boundaries of the geofence. (ECF No. 96-1, at ¶ 25.) Rodriguez confirmed that, for every device whose “stored latitude/longitude coordinates fall within the radius described in the warrant,” Google turns over a “‘production version’ of the [users’] data.” (ECF No. 96-2, at ¶ 8.) This production version “includes a [de-identified] device number,<sup>19</sup> the latitude/longitude coordinates and timestamp of the stored [Location History] information, the map's [confidence interval], and the source of the stored [Location History],” (*i.e.*, “whether the location was generated via Wi-Fi, GPS, or a cell tower”). (ECF No. 96-2, at ¶ 8.)

According to Rodriguez, the sizes and timeframes of geofences “vary considerably from one request to another.” (ECF No. 96-2, at ¶ 8.) Because Google produces *all* location points captured within the geofence over the timeframe, “[t]he volume of data produced at [Step 1] depends on the size and nature of the geographic area and length of time covered by the geofence request.” (ECF No. 96-2, at ¶ 8.) Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data.

Indeed, Google places significant discretion on the LIS employee who initially reviews a particular geofence warrant. This “specialist” will first process and review the warrant. (ECF No. 202, at 178–79.) If the specialist believes the warrant “needs further review”—for example, if the geofence seems too large or the timeframe too long—he or she may first “engage with [the requesting] law enforcement officer to collect more information about the investigation.” (ECF No. 202, at 179, 182.) From there, the specialist will “consult with [Google's] legal counsel.” (ECF No. 202, at 179.) If Google's counsel objects to the warrant, Google may have a “conversation” with law enforcement to alleviate Google's concerns, or it may “require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue.” (ECF No. 202, at 187.) Assuming law enforcement eventually assuages Google's concerns with the warrant, Google then provides the Government with the de-identified geofence data.

## **ii. Step 2**

**\*10***Second*, according to Rodriguez, at Step 2, the Government “reviews the de[-]identified [data] to determine the [Sensorvault] device numbers of interest.” (ECF No. 96-1, at ¶ 10.) If law enforcement needs “additional de[-]identified location information for a [certain] device” to “determine whether that device is actually relevant to the investigation,” law enforcement, at this step, “can compel Google to provide additional ... location coordinates *beyond* the time and geographic scope of the original request.”<sup>20</sup> (ECF No. 96-2, at ¶ 10 (emphasis added).) These additional location points “can assist law enforcement in eliminating devices” from the investigation that were, for example, “not in the target location for enough time to be of interest, [or] were moving through the target location in a manner inconsistent with other evidence.”<sup>21</sup> (ECF No. 96-2, at ¶ 11.) Notably, Google imposes “no geographical limits” on this Step 2 data. (ECF No. 202, at 184.) Thus, if a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points for identified users over an expanded timeframe at Step 2. This means that, at Step 2, no geographic barrier confines the information searched.

Google does, however, typically require law enforcement to narrow the number of users for which it requests Step 2 data so that the Government cannot not simply seek geographically unrestricted data for *all* users within the geofence. Google has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow. But if law enforcement requests “a lower number of devices from St[ep] 1 to St[ep] 2,” this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks. (ECF No. 202, at 190.) Again, assuming Google has no further objections to law enforcement's Step 2 request, Google provides law enforcement with de-identified but geographically unrestricted data.

### **iii. Step 3**

*Finally*, at Step 3, drawing from the de-identified data Google has produced so far, “the [G]overnment can compel Google ... to provide *account-identifying information*” for the users “the [G]overnment determines are relevant to the investigation.” (ECF No. 96-2, at ¶ 12 (emphasis added).)<sup>22</sup> This “account-identifying information” includes the name and email address associated with the account. (ECF No. 96-2, at ¶ 12; ECF No. 202, at 192.) Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is “[p]ossibl[e]” that Google would approve a Step 3 request that is not narrowed after Step 2 at all. (ECF No. 202, at 194.)

...

### **III. Analysis**

\*17 Chatrle seeks to suppress evidence obtained from the June 14, 2019 Geofence Warrant that covered 70,686 square meters of land around the Bank, located in a busy part of the Richmond metro area. Despite the Court's concerns about the validity of this warrant and the adoption of unsupervised geofence warrants more broadly, the Court will deny Chatrle's Motion to Suppress because the officers sought the warrant in good faith.

#### **A. The Court Will Briefly Address Fourth Amendment Standing**

Because the Court will independently deny Chatrle's motion to suppress by considering the validity of the Geofence Warrant, the Court “need not wade into the murky waters of standing,” *i.e.*, whether Chatrle has a reasonable expectation of privacy in the data sought by the warrant. *United States v. James*, No. 18cr216, 2018 WL 6566000, at \*4 (D. Minn. Nov. 26, 2018); *see Byrd v. United States*, — U.S. —, 138 S. Ct. 1518, 1530, 200 L.Ed.2d 805 (2018) (Fourth Amendment standing “is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.”).

Nonetheless, the Court notes its deep concern (underlying both Fourth Amendment standing, and the third-party doctrine discussed below) that current Fourth Amendment doctrine may be materially lagging behind technological innovations. As Fourth Amendment law develops in a slow drip, “technology [continues to] enhance[ ] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes.” *Carpenter v. United States*, — U.S. —, 138 S. Ct. 2206, 2214, 201 L.Ed.2d 507 (2018). Relevant here, although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. *See* Part II.A.3.a, *supra*. The Government thus has an almost unlimited pool from which to seek location data, and “‘[w]hoever the suspect turns out to be,’ they have ‘effectively been tailed’ ” since they enabled Location History. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (quoting *Carpenter*, 138 S. Ct. at 2218).

Indeed, the “ ‘retrospective quality of [geofence] data’ enables police to ‘retrace a person's whereabouts,’ ” and “[p]olice need not even know in advance whether they want to follow a particular individual, or when.” *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218). Until recently, the ease with which law enforcement might access such precise and essentially real-time location data was unimaginable. And it is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps causes such data to “cross[ ] the line from merely augmenting [law enforcement's investigative capabilities] to impermissibly enhancing” them. *Id.* at 341.

What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. See *United States v. Knotts*, 460 U.S. 276, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) (“A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”). He or she thus may not be able to establish Fourth Amendment standing to challenge a time-limited acquisition of his location data at the bank.

**\*18** But the individual in his or her residence likely *would* have a heightened expectation of privacy. *Silverman v. United States*, 365 U.S. 505, 511, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961) (“At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his [or her] own home and there be free from unreasonable government intrusion.”). Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could not assert that individual's privacy rights in his or her criminal case, *United States v. Rumley*, 588 F.3d 202, 206 n.2 (4th Cir. 2009), that innocent individual would seemingly have no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a “right without a remedy.” *Hawkins v. Barney's Lessee*, 30 U.S. 457, 463, 5 Pet. 457, 8 L.Ed. 190 (1831) (“There can be no right without a remedy to secure it.”).

As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing “reasonable expectation of privacy” doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (considering the validity of using thermal imaging on one's home); *United States v. Jones*, 565 U.S. 400, 402-03, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (construing “the attachment of a [GPS] tracking device to an individual's vehicle” for twenty-eight days); *Carpenter*, 138 S. Ct. at 2217 n.3 (considering whether “accessing seven days of [an individual's cell site location information] constitutes a Fourth Amendment search”).

At base, these matters are best left to legislatures. See Zach Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), <https://tcm.ch/35mLHkP> (discussing a recently introduced New York bill that would ban the use of geofence warrants statewide). This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data. And, as discussed below, despite its ongoing efforts to improve, Google appears to do so under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works, nor do they know Google is logging their location 240 times a day. It is not within this Court's purview to decide such issues, but it urges legislative action. Thoughtful legislation could not only protect

the privacy of citizens, but also could relieve companies of the burden to police law enforcement requests for the data they lawfully have.

**B. Because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence, the Warrant Violates the Fourth Amendment**

At base, this particular Geofence Warrant is invalid. The Fourth Circuit has clearly articulated that warrants, like this one, that authorize the search of every person within a particular area must establish probable cause to search every one of those persons. Here, however, the warrant lacked any semblance of such particularized probable cause to search each of its nineteen targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed. And to the extent the Government would argue that Steps 2 and 3 cure the warrant's defects as to probable cause, such an argument is unavailing here. The Government itself contends that law enforcement demonstrated probable cause to obtain *all* the data sought without any narrowing measures (*i.e.*, de-anonymized and geographically unlimited data from everyone within the geofence). In any event, Steps 2 and 3—undertaken with no judicial review whatsoever—improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions. These steps therefore cannot buttress the rest of the warrant, as they fail independently under the Fourth Amendment's particularity prong.

**1. Legal Standard: The Warrant Requirement**

\*<sup>19</sup>The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Stated another way, the Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate.<sup>31</sup> *Dalia v. United States*, 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979) (internal quotations and citations omitted). If a warrant is invalid, the proper remedy in a criminal action is “ordinarily” to suppress the evidence derived from it. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

**a. Probable Cause**

Whether probable cause for a search exists is a “practical, common-sense” question, asking whether “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). It requires only “the kind of fair probability on which reasonable and prudent people, not legal technicians,” would rely. *United States v. Jones*, 952 F.3d 153, 158 (4th Cir. 2020) (citing *Florida v. Harris*, 568 U.S. 237, 244, 133 S.Ct. 1050, 185 L.Ed.2d 61 (2013)). Officers must present sufficient information to the magistrate judge<sup>32</sup> to allow him or her to exercise independent judgment. *Gates*, 462 U.S. at 239, 103 S.Ct. 2317. The magistrate cannot simply ratify the bare conclusions of others. *Id.* “When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant.” *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citations omitted). “[T]he duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.” *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

More specifically, a warrant must be “no broader than the probable cause on which it is based.” *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Indeed, the United States Court of Appeals for the Fourth Circuit has established that

warrants that authorize the search of “all persons on [a] premise[s]” must show probable cause “to believe that *all* persons on the premises at the time of the search are involved in the criminal activity.” *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (emphasis added) (second alteration in original), *overturned on other grounds by Pearson v. Callahan*, 555 U.S. 223, 129 S. Ct. 808, 172 L.Ed.2d 565 (2009). In other words, these warrants must demonstrate “good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity.” *Owens*, 372 F.3d at 276 (internal quotation marks omitted).

At base, probable cause demands that law enforcement possess “a reasonable ground for belief of guilt ... *particularized* with respect to the person to be searched or seized.” *Maryland v. Pringle*, 540 U.S. 366, 124 S. Ct. 795, 800, 157 L.Ed.2d 769 (2003) (emphasis added); *see Ybarra v. Illinois*, 444 U.S. 85, 91, 100 S.Ct. 338, 62 L.Ed.2d 238 (1979) (“Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.”) A “person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.” *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

### **b. Particularity**

\*20A warrant must also be sufficiently “particular[ ].” *Hurwitz*, 459 F.3d at 470. Thus, a warrant must “confine the executing [officers’] discretion by allowing them to seize only evidence of a particular crime.” *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). The warrant must therefore “identif[y] the items to be seized by their relation to designated crimes,” and the “description of the items [must] leave[ ] nothing to the discretion of the officer executing the warrant.” *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). “So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not ... the particularity standard is met.” *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).<sup>33</sup>

## **2. The Geofence Warrant Fails to Establish Particularized Probable Cause to Search Every Google User Within the Geofence**

Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause.<sup>34</sup> The United States Supreme Court has explained that warrants must establish probable cause that is “particularized with respect to the person to be searched or seized.” *Pringle*, 124 S. Ct. at 800. This warrant did no such thing. It first sought location information for *all* Google account owners who entered the geofence over the span of an hour.<sup>35</sup> For those Google accounts, the warrant further sought “contextual data points with points of travel outside of the” Geofence for yet another hour—and those data points retained *no* geographical restriction. (ECF No. 54-1, at 4.) Astoundingly, the Government claims that law enforcement established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any narrowing measures.<sup>36</sup> Yet the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.

\*21 Law enforcement attempted to justify the warrant by claiming that such a sweeping search “may [have] tend[ed] to identify potential witnesses and/or suspects.” (ECF No. 54-1, at 7.) Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield *witnesses* (some of whom

had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. *Cf. Owens*, 372 F.3d at 276. To be sure, a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information.<sup>37</sup> However, the warrant, on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Indeed, it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing. Law enforcement knew only that the perpetrator “had a cell phone in his right hand and appeared to be speaking with someone on the device.” (ECF No. 54-1, at 6.) After the police failed to locate the suspect via reviewing camera footage, speaking with witnesses, and pursuing two leads, law enforcement simply drew a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot.<sup>38</sup> The Government then requested location information for *every device* within that area. *See Carpenter*, 138 S. Ct. 2206, 2216 (2018) (describing cell phone location information as “encyclopedic”).

What is more, in one instance, this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery. Because the radius of one of the users' confidence intervals stretched to around 387 meters, the Geofence Warrant might have reported that user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the Government obtained the person's location data just the same. The Government claims that footage depicting the perpetrator holding a phone to his ear—and nothing else—justified this sweeping warrant. That, however, is simply not “[ ]reasonable.” U.S. Const. amend. IV.

**\*22** To further underscore the breadth of this search, Chatrie's expert Spencer McInville pointed out a likely “false positive” from the warrant—“Mr. Blue.” McInville testified that this “false positive” individual may not have ever stepped within the geofence—he may have simply driven “outside of the original geofence” on a nearby road, but could have nonetheless appeared “as if [he] were inside the geofence.” (ECF No. 201, at 43–44, 65.) Because Google's location estimate for that person could have been “incorrect,” Google may have *thought* the person had stepped foot in the target area. (ECF No. 201, at 43–44.) The Government therefore obtained two hours of unrestricted location data for an individual who perhaps had only driven within the outer vicinity of the crime scene.<sup>39</sup>

This Geofence Warrant therefore suffers from the same probable cause defect as that at issue in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020). In that case, the Government sought “to erect three geofences.” *Id.* 732. Two encompassed the same location during different timeframes, and the other captured a second location. *Id.* Each geofence lasted for forty-five minutes. *Id.* The court remarked that “the proposed warrant would admittedly capture the device IDs ... for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime.” *Id.* at 752. There, just as here, the warrant provided the Government “unlimited discretion to obtain from Google the device IDs ... of anyone whose Google-connected devices traversed the

geofences (including their vaguely defined margins of error), based on nothing more than the ‘propinquity’ of these persons to the Unknown Subject at or near the time” of the criminal activity. *Id.* at 753. As that court (and the Supreme Court in *Ybarra*) recognized—and as this Court now concludes—the Fourth Amendment’s probable cause requirement demands more than “mere propinquity” to a crime. *Id.* at 752; *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

Despite the Government’s reliance on *United States v. McLamb*, that case is inapposite. There, the Fourth Circuit upheld a warrant that allowed law enforcement to obtain identifying information of “any user entering a username and password into” an internet-based dark website where users could download or upload child pornography. *United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018). But there, a user’s “mere propinquity” to the website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing child pornography. *Id.* Here, on the other hand, a Google user’s proximity to the bank robbery does not necessarily suggest that the user participated in the crime. *McLamb* therefore does not inform this case.<sup>40</sup>

**\*23** Nor does the Government’s reliance on *United States v. James* persuade. The *James* court considered a warrant to collect cell tower information (so-called “tower dumps”) to determine whether “a particular cellular phone number (ostensibly held by the robber) could be identified during the timeframes of each of the respective robberies.” 2018 WL 6566000, at \* 1. Law enforcement sought the cell tower data based on the notion that a cell phone number present at the location and time of all six robberies created sufficient probable cause that the number belonged to the robber. *Id.* Ultimately, the court concluded that “there was a fair probability that data from the cellular towers” would contain identifying information about the perpetrator and that therefore the warrants sufficed to allege probable cause. *Id.* at \*4. As another court has noted however, *James* did not account for whether probable cause existed to search through the *other* individuals’ location information. *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751; *see also id.* at 752 (distinguishing another tower dump decision from the geofence context because the court discussing the tower dump “stopped the analysis once the court found probable cause in the ‘nexus’ between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to obtain all of those records.” (quoting *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D. Tex. 2013)). *James* therefore stopped short of considering whether “particularized” probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant.<sup>41</sup>

The Court cautions that it declines to consider today whether a geofence warrant may *ever* satisfy the Fourth Amendment’s strictures. *See In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020) (“[I]t is nearly impossible to pinpoint a search where only the perpetrator’s privacy interests are implicated.”). Consider, for example, one of the few other federal court opinions to address a geofence warrant—*In re Search of Information That Is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021) [hereinafter “DDC Opinion”]. There, law enforcement devised a two-step process to narrow the list of individuals whose data they would obtain. *Id.* at \*5–6. At Step 1, Google would identify all accounts who entered the geofence within the relevant time periods. *Id.* For each of these accounts, Google would turn over only anonymized data. *Id.*

The Government would then review that data, identify likely suspects based on the “mov[ement]” of the users’ devices through the geofence, and, crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. *Id.* The *court* could then, at its discretion, order Google to disclose to

the Government personally identifying information for devices that belonged to likely suspects. *Id.* In essence, to obtain a warrant authorizing disclosure of de-anonymized data, the Government was required to demonstrate that location data for a *particular* user or set of users would provide evidence of the crime. And crucially, the warrant left ultimate discretion as to which users' information to disclose to the reviewing court, not to Google or law enforcement.

**\*24** In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly circumscribed geofence at Step 1. *See Hurwitz*, 459 F.3d at 473 (a warrant must be “no broader than the probable cause on which it is based”). From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information. Although the *instant* warrant is invalid, where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional.<sup>42</sup>

At bottom however, particularized probable cause “cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.” *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338. The Court finds unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same “mere propinquity to others” rationale the Supreme Court has already rejected as an appropriate basis for a warrant. *Id.* This warrant therefore cannot stand.

### **3. This Geofence Warrant's Three-Step Process Does Not Cure Its Defects**

To the extent the Government would attempt to argue in the alternative that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing.<sup>43</sup> Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. In other words, “[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize.” *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (citing *Stanford v. Texas*, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965)). But Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.

**\*25** This warrant, for instance, contains no language objectively identifying *which* accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the *number* of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

The facts here underscore the breadth of discretion law enforcement possessed under this warrant.<sup>44</sup> After receiving anonymized information on the nineteen targeted users at Step 1, Det. Hylton requested the

additional location information (Step 2) and subscriber information (Step 3) “for all 19 device numbers produced in [S]tep 1.” (ECF No. 96-2, at ¶ 15.) In response, a Google specialist “called Detective Hylton and explained the issues in the Detective’s email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant.”<sup>45</sup> (ECF No. 96-2, at ¶ 16.) During that call, “[t]he LIS specialist also explained the importance of [S]tep 2 in narrowing.” (ECF No. 96-2, at ¶ 16.) Det. Hylton eventually narrowed his requests. Yet he did not specify to Google why he was choosing these particular users.

Google’s insistence on narrowing the list does not render this warrant sufficiently particular. For one thing, this warrant’s clear text does not specifically allow Google to limit the group of accounts that would be subject to further scrutiny. (See ECF No. 54-1, at 4–5 (noting only that Google “shall produce” further information).) But even if it did, Fourth Amendment discretion must be confined to the signing magistrate, not the executing officers or a third party. *United States v. Chadwick*, 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977) (“The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate ....”), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991). Stated plainly, Steps 2 and 3 “put[ ] no limit on the [G]overnment’s discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences.” *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754. These Steps accordingly fail to provide the executing officer with clear standards from which he or she could “reasonably ... ascertain and identify ... the place to be searched [or] the items to be seized.” *Blakeney*, 949 F.3d at 861. The Government therefore cannot rely on Steps 2 and 3 to supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment’s particularity requirement.

#### **4. The Third-Party Doctrine**

\***26** Lastly, the Court simply cannot determine whether Chatrie “voluntarily” agreed to disclose his Location History data based on this murky, indeterminate record. But the Court expresses its skepticism about the application of the third-party doctrine to geofence technology. Under this doctrine, “a person [generally] has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). However, in *Carpenter v. United States*, the Supreme Court refined this principle and held that an individual *does* possess an expectation of privacy in seven days of cell-site location information collected by a wireless carrier. 138 S. Ct. at 2217 & n.3. Here, the Government argues that Chatrie cannot claim a reasonable expectation of privacy in his Location History data because (1) he “voluntarily disclosed” the information to Google; and, (2) the two hours of location data sought here do not implicate the same privacy concerns as the seven days obtained in *Carpenter*. (ECF No. 41, at 11; see ECF No. 41, at 9–13.)

The Court thinks otherwise. Common sense underscores Supreme Court Justice Sonia Sotomayor’s observation in *United States v. Jones* about “voluntary” collection of electronic information unbeknownst to the subject of the warrant. As to the third-party doctrine, Justice Sotomayor observed that:

it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age.... I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.

*Jones*, 565 U.S. at 417–18, 132 S.Ct. 945 (Sotomayor, J., concurring). At base, the topic is complex. And considering the messiness of the current record as to how and when Chatrie “gave consent,” the Court cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie’s expectation of privacy in his data, even for “just” two hours. Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is “detailed, encyclopedic, and effortlessly compiled.” *Carpenter*, 138 S. Ct. at 2216; *see id.* at 2219 (“There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.”). Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one’s whereabouts during almost every minute of every hour of every day.

This is especially so given the limited and partially hidden warnings provided by Google. In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that “[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences,” and that he “can see [his] data, delete it and change [his] settings at account.google.com.” (ECF No. 147, at ¶ 7; *see* ECF No. 96-1, at ¶ 7; ECF No. 201, at 102; ECF No. 202, at 21.) However, the consent flow did not detail, for example, how frequently Google would record Chatrie’s location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he “stopped” location tracking it was only “paused,” meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).<sup>46</sup> (ECF No. 201, at 122, 136; ECF No. 202, at 71.)

**\*27** While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting “YES, I’M IN” at midnight while setting up Google Assistant, even if some text offered warning along the way. The record here makes plain that these “descriptive texts” are less than pellucid. Although the Court cannot reach a final decision on the issue today based on the current record here, Chatrie likely could not have, in a “meaningful sense, ... voluntarily ‘assumed the risk’ of turning over a comprehensive dossier of his physical movements” to law enforcement. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577); *see id.* at 2217 (“A person does not surrender all Fourth Amendment protection by venturing into the public sphere.”).

...

# STATE OF NEW YORK

84--A

2021-2022 Regular Sessions

## IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. QUART, DE LA ROSA, L. ROSENTHAL, EPSTEIN, HYNDMAN, BARRON, ABINANTI, OTIS, GOTTFRIED, SIMON, JACKSON, SEAWRIGHT -- read once and referred to the Committee on Codes -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the criminal procedure law, in relation to prohibiting the search, with or without a warrant, of geolocation and keyword data of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time or searched particular words, phrases, character strings, or websites

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. Short title. This act shall be known and may be cited as  
2 the "reverse location and reverse keyword search prohibition act".

3 § 2. The criminal procedure law is amended by adding a new article 695  
4 to read as follows:

### ARTICLE 695

#### REVERSE LOCATION AND REVERSE KEYWORD SEARCHES

##### Section 695.00 Definitions.

6 695.10 Issuance of reverse location court orders and reverse  
7 keyword court orders.

8 695.20 Execution of reverse location and reverse keyword search-  
9 es.

10 695.30 Reverse location and reverse keyword searches;  
11 suppression of evidence.

12 695.40 Reverse location and reverse keyword searches; private  
13 right of action.

14 695.50 Physical searches excluded.

15 § 695.00 Definitions.  
16  
17

EXPLANATION--Matter in italics (underscored) is new; matter in brackets  
[-] is old law to be omitted.

LBD01721-05-1

1 As used in this article, the following terms shall have the following  
2 meanings:

3 1. "Government entity" shall mean any department or agency of the  
4 state or any political subdivision thereof, or any individual acting for  
5 or on behalf of the state or a political subdivision thereof.

6 2. "Reverse keyword court order" means any court order, including a  
7 search warrant, compelling the disclosure of records or information  
8 identifying any unnamed persons, by name or other unique identifier, who  
9 electronically searched for particular words, phrases, character  
10 strings, or websites, or who visited a particular website through a link  
11 generated by such a search, regardless of whether or not the order is  
12 limited to a specific geographic area or time frame.

13 3. "Reverse location court order" means any court order, including a  
14 search warrant, compelling the disclosure of records or information  
15 pertaining to electronic devices or their users or owners, whose scope  
16 extends to an unknown number of electronic devices present in a given  
17 geographic area at a given time as measured via global positioning  
18 system coordinates, cell tower connectivity, Wi-Fi data and/or any other  
19 form of location detection.

20 4. "Voluntary reverse keyword request" means any request in the  
21 absence of a court order, by any government entity for the provision of  
22 records or information identifying any unnamed persons, by name or other  
23 unique identifier, who electronically searched for particular words,  
24 phrases, character strings, or websites, or who visited a particular  
25 website through a link generated by such a search, regardless of whether  
26 or not the order is limited to a specific geographic area or time frame.

27 5. "Voluntary reverse location request" means any request in the  
28 absence of a court order by any government entity for records or infor-  
29 mation pertaining to electronic devices or their users or owners, whose  
30 scope extends to an unknown number of electronic devices present in a  
31 given geographic area at a given time, whether such device location is  
32 measured via global positioning system coordinates, cell tower connec-  
33 tivity, Wi-Fi data and/or any other form of location detection.

34 6. "Law enforcement officer" means any police officer, peace officer,  
35 or prosecutor.

36 § 695.10 Issuance of reverse location court orders and reverse keyword  
37 court orders.

38 No court shall issue a reverse location court order or a reverse  
39 keyword court order.

40 § 695.20 Execution of reverse location and reverse keyword searches.

41 1. No government entity shall seek, from any court, a reverse location  
42 court order or a reverse keyword court order.

43 2. No government entity shall make a voluntary reverse location  
44 request or a voluntary and reverse keyword request.

45 3. No government entity shall seek, secure, obtain, borrow, purchase,  
46 use, or review any information or data obtained through a reverse  
47 location request or a reverse keyword request.

48 4. No government entity shall seek the assistance of any non-govern-  
49 mental entity, any agency of the federal government, or any agency of  
50 the government of another state or subdivision thereof in obtaining  
51 information or data from a reverse location court order, reverse keyword  
52 court order, reverse location request, or reverse keyword request if the  
53 government entity would be barred from directly seeking such information  
54 under this article.

55 § 695.30 Reverse location and reverse keyword searches; suppression of  
56 evidence.

1 1. Upon motion from a defendant, a court shall order that evidence be  
2 suppressed or excluded if the court finds that such evidence:

3 (a) consists of a record acquired via a reverse location court order,  
4 reverse keyword court order, voluntary reverse location request, or  
5 voluntary reverse keyword request; or

6 (b) was obtained as a result of other evidence obtained under a  
7 reverse location court order, reverse keyword court order, voluntary  
8 reverse location request, or voluntary reverse keyword request.

9 2. This section shall apply regardless of the court which issued the  
10 order and regardless of whether the issuance of the order was permissi-  
11 ble under the procedures of that court.

12 3. This section shall apply regardless of any claim that the informa-  
13 tion or evidence is attenuated from an unlawful order or request, would  
14 inevitably have been discovered, or was simultaneously or subsequently  
15 obtained or reobtained through other means.

16 § 695.40 Reverse location and reverse keyword searches; private right of  
17 action.

18 1. Any individual whose records were obtained by any government entity  
19 in violation of section 695.20 of this article may institute a civil  
20 action against such government entity for any or all of the following:

21 (a) One thousand dollars per violation or actual damages, whichever is  
22 greater.

23 (b) Punitive damages.

24 (c) Injunctive or declaratory relief.

25 (d) Any other relief the court deems proper.

26 2. In assessing the amount of punitive damages, the court shall  
27 consider:

28 (a) The number of people whose information was disclosed.

29 (b) The proximity of the search to locations with heightened privacy  
30 concerns, including, but not limited to, houses of worship, political  
31 protests, and medical facilities.

32 (c) The persistence of violations by the particular government entity.

33 3. In any action brought under this section, the court shall award  
34 reasonable attorneys' fees, expenses and costs to a prevailing plain-  
35 tiff.

36 § 695.50 Physical searches excluded.

37 The foregoing limitations shall not apply to the search of any elec-  
38 tronic device lawfully seized and/or searched pursuant to a search  
39 warrant issued under article six hundred ninety of this title.

40 § 3. This act shall take effect immediately.



## Federal Court in Virginia Holds Geofence Warrant Violates Constitution

In the first order of its kind, a federal district court has [held](#) that a warrant used to identify all devices in the area of a bank robbery, including the defendant's, "plainly violates the rights enshrined in [the Fourth] Amendment." The court questioned whether similar warrants could ever be constitutional.

The case is [United States v. Chatrie](#), and addresses a controversial tool called a [geofence warrant](#). The police issued the warrant to Google seeking information on every device within the area of the robbery during a one-hour period. The geographic area was about 17.5 acres (about 3 and a half times the footprint of a New York city block) and included a church, a chain restaurant, a hotel, several apartments and residences, a senior living facility, a self-storage business, and two busy streets.

Google's initial search identified 19 devices, with a total of 210 individual location points. Google assigned anonymizing identifiers to each device and provided their locations to the police. Following a three-step process designed by Google, the police expanded the time period to two hours to get additional location information for 9 of the devices. Ultimately, police obtained detailed, identifying subscriber information for three devices. One of those belonged to the defendant.

Mr. Chatrie filed a motion to suppress the geofence evidence, and, after several hearings and extensive expert testimony, the court issued a thorough, 63-page order holding the warrant was unconstitutional. The court held that it's not enough for the police to allege that a crime was committed and the perpetrator used a cellphone. If the police want to get information on every device in the area,

they must also establish probable cause to search every person in the area, something that's likely impossible in a busy area like this one.

The court further held that Google's three-step process did not cure the warrant's defects. The initial anonymization of the data didn't help because, as the court recognized, "[e]ven 'anonymized' location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one- or two-hour period."

The second and third steps of the process, taken ostensibly to narrow the number of devices disclosed to police, couldn't buttress the search either. They were "undertaken with no judicial review whatsoever" and "provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval." There were no objective guardrails in the warrant or "any semblance of objective criteria to guide how officers would narrow the lists of users." And even though Google (rather than the police) insisted on narrowing at the second step, the court held "Fourth Amendment protections should not be left in the hands of a private actor."

*Chatrie* follows [several other courts](#) that have also held geofence warrants to be unconstitutional, but in each of those cases, the judges were reviewing the warrant before a defendant had ever been charged. The *Chatrie* case is different because the warrant was approved by a magistrate, and the investigation ultimately resulted in the case brought against Mr. Chatric. With the help of [experienced defense attorneys](#) and extensive testimony from Google and expert witnesses for both the defense and prosecution, the parties were able to create a robust factual record, which the court detailed in its [order](#). This should prove extremely helpful for other defendants challenging similar geofence warrants in the future.

The facts established in the case confirmed much of what we already suspected—that Google has a voluminous, detailed, and searchable database of location information, which it collects from "numerous tens of millions" of its users. The data comes from a database Google calls "Sensorvault," where it stores location data for one of its services called "Location History." Google collects Location History data from different sources, including wifi connections, GPS and Bluetooth signals, and cellular networks. And it logs a device's location, on average, every two minutes. This makes it much more precise than cell site location information and allows Google to estimate a device's (and by extension, the device owner's) location to within 20 meters or less.

This precision also allows Google to infer where a user has been, what they were doing at the time, and the path they took to get there. Google can even determine a user's elevation and establish what floor of a building that user may have been on. As the court noted, "Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data."

However, the fact witnesses also showed that, despite this claimed precision, the data may not be all that accurate. It may place a device inside the geofenced area that was, in fact hundreds of feet away and vice versa. This creates the possibility of both false positives and false negatives—people could be implicated for the robbery when they were nowhere near the bank, or the actual perpetrator might not show up at all in the data Google provides to police.

Unfortunately for Mr. Chatrue, despite the court's determination that the warrant was plainly unconstitutional, the court nevertheless refused to suppress the evidence. The court held that the officer acted in good faith on what he thought was a valid warrant. This is a frustrating outcome that lets the police off the hook in this case. However, the court's order makes clear that this can't happen again in the future. The police are now on notice that geofence warrants are, by default, unconstitutional, and there are very few—if any—scenarios in which they could satisfy the Fourth Amendment.

## RELATED CASES:

[CARPENTER V. UNITED STATES](#)

---

# JOIN EFF LISTS

## Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)



## EFF Files Amicus Brief Arguing Geofence Warrants Violate the Fourth Amendment

Should the police be able to force Google to turn over identifying information on every phone within a certain geographic area—potentially hundreds or thousands of devices—just because a crime occurred there? We don't think so. As we argued in an [amicus brief](#) filed recently in *People v. Dawes*, a case in San Francisco Superior Court, this is a general search and violates the Fourth Amendment.

The [court](#) is scheduled to hear the defendant's motion to quash and suppress evidence on August 25, 2020.

In 2018, police in San Francisco were trying to figure out who robbed a house in a residential neighborhood. They didn't have a suspect. Instead of using traditional investigative techniques to find the culprit, they turned to a new surveillance tool that's been gaining interest from police across the country—a “geofence warrant.”

Unlike traditional warrants for electronic records, a geofence warrant doesn't start with a suspect or even an account; instead it directs Google to search a vast database of location history information to identify every device (for which Google has data) that happened to be in the area around the time of the crime, regardless of whether the device owner has any link at all to the crime under investigation. Because these investigations start with a location before they have a suspect, they are also frequently called “reverse location” searches.

Google has a particularly robust, detailed, and searchable collection of location data, and, to our knowledge, it is the only company that complies with these warrants. Much of what we know about the data Google provides to police and how it provides that data comes from a [declaration](#) and an [amicus brief](#) it filed in a Virginia case called [United States v. Chatrue](#). According to Google, the data it provides to police comes from its database called “[Sensorvault](#),” where it stores location data for one of its services called “Location History.” Google collects Location History data from different sources, including wifi connections, GPS and Bluetooth signals, and cellular networks. This makes it much more precise than cell site location information and allows Google to estimate a device’s location to within 20 meters or less. This precision also allows Google to [infer](#) where a user has been (such as to a ski resort), what they were doing at the time (such as driving), and the path they took to get there.

Location History is offered to users on both Android and IOS devices, but users must opt in to data collection. Google [states](#) that only about one-third of its users have opted in to Location History, but this represents “numerous tens of millions of Google users.”

Police have been [increasingly seeking access](#) to this treasure trove of data over the last few years via geofence warrants. These warrants reportedly date to 2016, but Google [states](#) that it received 1500% more geofence warrants in 2018 than 2017 and 500% more in 2019 than in 2018. According to the New York Times, the company received as many as [180 requests in a single week](#) in 2019.

Geofence warrants typically follow a similar multi-stage process, which appears to have been [created by Google](#). For the first stage, law enforcement identifies one or more geographic areas and time periods relevant to the crime. The warrant then requires Google to provide information about any devices, identified by a numerical identifier, that happened to be in the area within the given time period. Google says that, to comply with this first stage, it must search through its *entire store* of Location History data to identify responsive data—data on tens of millions of users, nearly all of whom are located well outside the geographic scope of the warrant. Google has also [said](#) that the volume of data it produces at this stage depends on the size and nature of the geographic area and length of time covered by the warrant, which vary considerably from one request to another, but the company once provided the government with identifying information for nearly [1,500 devices](#).

After Google releases the initial de-identified pool of responsive data, police then, in the second stage, demand Google provide additional location history outside of

the initially defined geographic area and time frame for a subset of users that the officers, at their own discretion, determine are “relevant” to their investigation. Finally, in the third stage, officers demand that Google provide identifying information for a smaller subset of devices, including the user’s name, email address, device identifier, phone number and other account information. Again, officers rely solely on their own discretion to determine this second subset and which devices to target for further investigation.

There are many problems with this kind of a search. First, most of the information provided to law enforcement in response to a geofence warrant does not pertain to individuals suspected of the crime. Second, as not all device owners have opted in to Location History, search results are both over and under inclusive. Finally, Google has said there is only an estimated 68% chance that the user is actually where Google thinks they are, so the users Google identifies in response to a geofence warrant may not even be within the geographic area defined by the warrant (and therefore are outside the scope of the warrant).

Unsurprisingly, these problems have led to investigations that ensnare innocent individuals. In one case, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence warrant. However, the man’s travel history was part of an exercise tracking app he used to log months of bike rides—rides that happened to take him past the site of the burglary. Investigators eventually acknowledged he should not have been a suspect, but not until after the man hired an attorney and after his life was upended for a time.

This example shows why geofence warrants are so pernicious and why they violate the Fourth Amendment. They lack particularity because they don’t properly and specifically describe an account or a person’s data to be seized, and they result in overbroad searches that can ensnare countless people with no connection to the crime. These warrants leave it up to the officers to decide for themselves, based on no concrete standards, who is a suspect and who isn’t.

The Fourth Amendment was written specifically to prevent these kinds of broad searches.

As we argued in *Dawes*, a geofence warrant is a digital analog to the “general warrants” issued in England and Colonial America that authorized officers to search anywhere they liked, including people or homes — simply on the chance that they might find someone or something connected with the crime under investigation. The chief problem with searches like this is that they leave too

much of the search to the discretion of the officer and can too easily result in general exploratory searches that unreasonably interfere with a person's right to privacy. The Fourth Amendment's particularity and probable cause requirements as well as the requirement of judicial oversight were designed to prevent this.

Reverse location searches are the antithesis of how our criminal justice system is supposed to work. As with other technologies that purport to pull a suspect out of thin air—like [face recognition](#), [predictive policing](#), and [genetic genealogy](#) searches—there's just too high a risk they will implicate an innocent person, shifting the burden of proving guilt from the government to the individual, who now has to prove their innocence. We think these searches are unconstitutional, even with a warrant.

The defendant's [motion to quash](#) the geofence warrant and motion to suppress the evidence will be heard in [San Francisco Superior Court](#) on August 25, 2020.

[Our Amicus Brief](#)

[Defendant's Motion to Quash / Motion to Suppress](#)

## RELATED CASES:

[CARPENTER V. UNITED STATES](#)

---

# JOIN EFF LISTS

## Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:



# Geofence Warrants and Reverse Keyword Warrants are So Invasive, Even Big Tech Wants to Ban Them

ESPAÑOL

Geofence and reverse keyword warrants are some of the most dangerous, civil-liberties-infringing and reviled tools in law enforcement agencies' digital toolbox. It turns out that these warrants are so invasive of user privacy that big tech companies like Google, Microsoft, and Yahoo are willing to support banning them. The three tech giants have issued a public statement through a trade organization, "Reform Government Surveillance," that they will support a bill before the New York State legislature. The Reverse Location Search Prohibition Act, A. 84/ S. 296, would prohibit government use of geofence warrants and reverse warrants, a bill that EFF also supports. Their support is welcome, especially since we've been calling on companies like Google, which have a lot of resources and a lot of lawyers, to do more to resist these kinds of government requests.

Under the Fourth Amendment, if police can demonstrate probable cause that searching a particular person or place will reveal evidence of a crime, they can obtain a warrant from a court authorizing a limited search for this evidence. In cases involving digital evidence stored with a tech company, this typically involves sending the warrant to the company and demanding they turn over the suspect's digital data.

**Geofence and reverse keyword warrants completely circumvent the limits set by the Fourth Amendment.** If police are investigating a crime—anything from vandalism to arson—they instead submit requests that do not identify a single suspect or particular user account. Instead, with geofence warrants, they draw a

box on a map, and compel the company to identify every digital device within that drawn boundary during a given time period. Similarly, with a [“keyword” warrant](#), police compel the company to hand over the identities of anyone who may have searched for a specific term, such as a victim’s name or a particular address where a crime has occurred.

These reverse warrants have serious implications for civil liberties. Their increasingly common use means that anyone whose commute takes them goes by the scene of a crime might suddenly become vulnerable to suspicion, surveillance, and harassment by police. It means that an idle Google search for an address that corresponds to the scene of a robbery could make you a suspect. It also means that with one document, companies would be compelled to turn over identifying information on every phone that appeared in the vicinity of a protest, [as happened in Kenosha, Wisconsin during a protest against police violence](#). And, as EFF has argued in amicus briefs, it violates the Fourth Amendment because it results in an overbroad fishing-expedition against unspecified targets, the majority of whom have no connection to any crime.

In the statement released by the companies, they write that, “This bill, if passed into law, would be the first of its kind to address the increasing use of law enforcement requests that, instead of relying on individual suspicion, request data pertaining to individuals who may have been in a specific vicinity or used a certain search term.” This is an undoubtedly positive step for companies that have a checkered history of being [cavalier with users’ data](#) and enabling [large-scale government surveillance](#). But they can do even more than support legislation in one state. Companies can still resist complying with geofence warrants across the country, be much more transparent about the geofence warrants it receives, provide all affected users with notice, and give users meaningful choice and control over their private data.

## JOIN EFF LISTS

### Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address





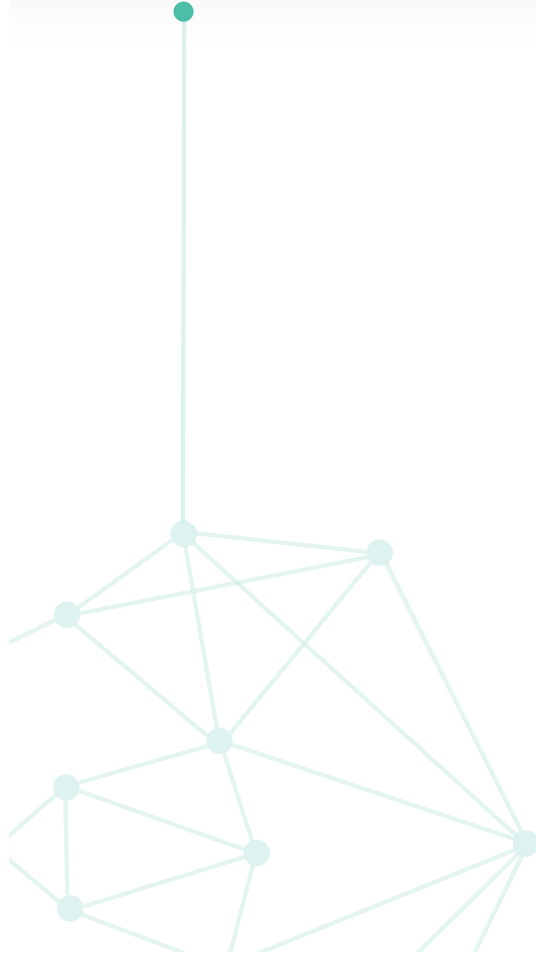




CENTER FOR CITY SOLUTIONS

# FACIAL RECOGNITION

## REPORT



### About the National League of Cities

The National League of Cities (NLC) is the voice of America's cities, towns and villages, representing more than 200 million people. NLC works to strengthen local leadership, influence federal policy and drive innovative solutions.

NLC's Center for City Solutions provides research and analysis on key topics and trends important to cities, creative solutions to improve the quality of life in communities, inspiration and ideas for local officials to use in tackling tough issues, and opportunities for city leaders to connect with peers, share experiences and learn about innovative approaches in cities.

### Authors

**Lena Geraghty**, Program Director of Urban Innovation, Center for City Solutions

### Acknowledgements

The authors would like to acknowledge:

**William Ossoff** and **William Wright**, Harvard Law School Cyberlaw Clinic Students, and Professor **Susan Crawford** for their research and contributions to this report.

**Angelina Panettieri**, Legislative Director of Information Technology and Communications, for her research and policy guidance.

**Cooper Martin**, Director of Sustainability & City Solutions, Center for City Solutions, for his guidance and review of the report.

**Erin Peterson**, Program Specialist for NLC-RISC, for reviewing the report.

**Ashleigh Imus** for copyediting.

# Table of Contents

<b>Facial recognition guide for cities</b>	<b>5</b>
<b>What is facial recognition? How does it work?</b>	<b>6</b>
Source of video or photographs	
Software for algorithmic analysis	
Comparison data sets	
<b>How do cities, towns and villages use facial recognition?</b>	<b>10</b>
Private vs. public use	
Identification vs. surveillance	
Driver's license photos vs. mug shots	
Evidentiary requirements	
Input requirements	
Type of crime	
<b>What are the benefits and risks for local governments' use of facial recognition?</b>	<b>12</b>
Benefit: Investigative efficiencies	
Risk: Bias in facial recognition technology	
Risk: Constitutional concerns: First and Fourth Amendments	
Risk: City liability	
<b>How are cities regulating facial recognition?</b>	<b>24</b>
City of Seattle, Washington	
City of Detroit, Michigan	
San Francisco Bay Area, California	
<b>How can cities better approach the topic of facial recognition publicly?</b>	<b>32</b>
1. Engage with residents to develop policies, and be transparent about facial recognition use.	
2. Establish a training program for law enforcement and other users of a facial recognition system.	
3. Limit the scope of facial recognition use to reduce the risk of misidentifications and privacy violations.	
4. Institute rigorous standards for data storage and cybersecurity to ensure protection of citizens' biometric data.	
5. Follow best practices for drafting contracts to ensure accuracy and reduce legal risk.	



## Facial recognition guide for cities

As cities, towns and villages embrace emerging technologies and determine their use in local government operations, elected officials will have to navigate difficult conversations and decisions, balancing privacy and transparency with efficiency. Facial recognition, the process by which peoples' faces captured in video footage or photographs are compared to a database of known individuals to find a likely match and identify an unknown person, is an emerging technology that warrants careful consideration.

Facial recognition technology is becoming more common in both the private and public sectors in the U.S. Grocery stores use it to track customers' shopping habits. Many people use it to unlock their cellphones. Police departments use it to determine the identity of suspects from video camera footage. Like many other emerging technologies, facial recognition technology has become widespread before public policy discussions have occurred in communities across the country.

Cities are at various stages of regulating use of facial recognition, wrestling with challenging conversations about both government and private-sector use of this technology. This report details what facial recognition is, how cities are using it, how cities are regulating it and how city officials can best approach public conversations about facial recognition use in their communities.



# What is facial recognition? How does it work?

**F**acial recognition technology works by comparing images of an unknown person's face with a database of known individuals' faces in order to find a match and identify an unknown person. Facial recognition systems generally require three elements:

- ◆ A source of video footage or photographs to be analyzed,
- ◆ Software to process captured images for comparison using algorithmic analysis and
- ◆ Databases against which those images can be compared.

## Source of video or photographs

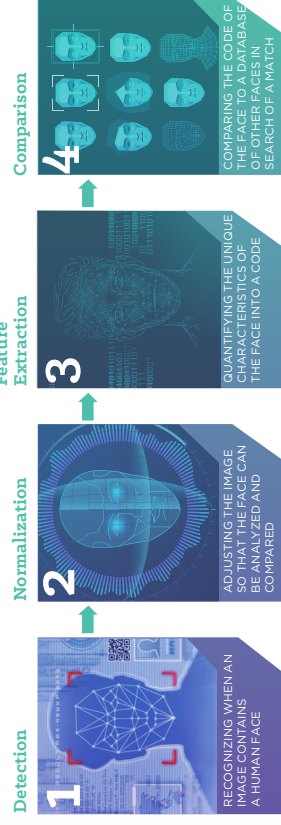
Facial recognition technology identifies unknown people from video footage or photographs. Video surveillance is a frequent source of this imagery. Although widespread video surveillance in cities is not new, it continues to increase. Building-mounted cameras and traffic cameras are common throughout most American cities, operated by both public and private entities. Many police forces use body cameras and vehicle cameras. Law enforcement also routinely deploys surveillance cameras to scan crowds and ensure security during high-profile events. Drone-mounted cameras -- already used by some cities -- provide another source of imagery. Additionally, most personal cellular devices have cameras, allowing the public to record images and video.

## Software for algorithmic analysis

A facial recognition system's central component is a set of algorithms that identifies faces within video or photographic images, extracts characteristics unique to those faces and matches these characteristics to known faces in a pre-existing database. Modern algorithms can accomplish this with a high degree of reliability. A 2014 study showed that facial recognition algorithms recognized faces more accurately than humans did within a given data set, distinguishing faces with 98.5% accuracy compared to 97.5% accuracy for the study's human participants.<sup>1</sup> The algorithms have grown steadily more reliable since then, reportedly achieving greater than 99% accuracy in some cases.<sup>2</sup> Although there are many different algorithms and ways to apply them, the process of facial recognition generally comprises the following steps, each of which entails the application of a distinct algorithm:

## Comparison data sets

The comparison phase described above relies on data sets of images of known people against which a captured image of a face can be compared. Many municipalities have access to various such data sets. Police forces generally maintain mug shot databases, and at least 26 states allow law enforcement to run searches against state databases of driver's licenses and ID photos.<sup>3</sup> In general, the better populated the comparison data set is, the greater likelihood of a match. Even if facial recognition technology worked perfectly, the only way to find a match for every captured face would be to have a comparison data set encompassing the entire world's population.



# How do cities, towns and villages use facial recognition?

## Private vs. public use

Both the public and private sectors in cities across the country use facial recognition. Some apartment buildings have begun to use facial recognition for security purposes.<sup>4</sup> Some airlines use facial recognition for check-in.<sup>5</sup> Sports arenas and concert venues use facial recognition to monitor crowds.<sup>6</sup> Public and private schools around the country, including public schools in Texas City, Texas,<sup>7</sup> and private schools in Seattle, Washington,<sup>8</sup> use facial recognition both for security purposes and to ensure that suspended students do not try to sneak into school events. Boise, Idaho, has plans to use facial recognition to keep banned people out of city hall.<sup>9</sup> Many companies also now offer facial recognition as a central part of their consumer products. The

latest version of the iPhone allows users to unlock their phones using facial recognition. Facebook also has used facial recognition for many years to suggest whom to tag in a photo. Google's Nest home security cameras now include facial recognition capabilities.<sup>10</sup> Amazon has also explored the possibility of installing facial recognition into its Ring home security cameras.<sup>11</sup> This could have implications for law enforcement; more than 400 law enforcement agencies have partnerships with Ring in which they can access the video footage captured by Ring cameras installed in private homes.<sup>12</sup>

Facial recognition is commonly used in public safety settings in cities, towns and villages. Many law enforcement agencies at the local, state and federal levels have deployed facial recognition to aid their investigations and more easily identify people. However, there are significant differences in how these facial recognition systems are used across cities and across law enforcement agencies:

## Identification vs. surveillance

Some cities limit the use of facial recognition to identification purposes. These municipalities use facial recognition searches of a photo database to identify a suspect whose photo they already have. Some cities use facial recognition to identify a person who has already been arrested or detained in connection with a crime but refuses to identify him or herself.

Other cities conduct real-time facial recognition surveillance, in which cameras can recognize and rapidly compare faces to a database, often in search of a "hot list" of suspects. Los Angeles, California, reportedly has this real-time facial recognition capability.<sup>13</sup>

## Driver's license photos vs. mug shots

Cities are also divided regarding the databases they use to conduct facial recognition searches. Cities such as New York City, New York and Detroit, Michigan, only use databases of mug shots, which limits the scope of searches to people previously processed by the criminal justice system. Other cities, including Lincoln, Nebraska, also search driver's license photos from state department of motor vehicle databases.<sup>14</sup>

## Evidentiary requirements

Some cities set an evidentiary requirement for police before they can run a facial recognition search. For example, Albuquerque, New Mexico, requires police to demonstrate probable cause before they run a search on a suspect. San Diego, California, police are required to have reasonable suspicion before they run a facial recognition search. By contrast, Lincoln, Nebraska, does not require either of these standards before authorities conduct a search.<sup>15</sup>

## Input requirements

The images for use in a facial recognition search range in quality and type. When police fail to obtain a clear photo of a suspect, some departments, including Washington County, Oregon, use sketches or artist renderings as a substitute for the photo.<sup>16</sup> Other departments, including in New York City, have used celebrity doppelgangers as substitutes for suspect photos.<sup>17</sup> Other cities, including Seattle, Washington, have used only actual photos of suspects as inputs.

## Type of crime

Some cities have also chosen to limit their use of facial recognition to certain types of criminal investigations. Detroit, Michigan, whose city council approved a new policy in September 2019, now requires that the department use facial recognition only to investigate violent crimes and home invasions.<sup>18</sup>



# What are the benefits and risks for local governments' use of facial recognition?



There are benefits and risks for government entities' use of facial recognition. Facial recognition can bring efficiencies into the investigative process.

However, facial recognition systems also reflect racial, gender and age bias in the data sets on which they are trained. Misidentifying people from information generated by a facial recognition system can have real-life negative effects. As with any emerging technology, the lack of legal guidance can make it difficult for cities to ensure that organizations use facial recognition technology in the best way and do not risk legal action or liability.

**Facial recognition can bring efficiencies into the investigative process. However, facial recognition systems also reflect racial, gender and age bias in the data sets on which they are trained.**

## BENEFIT Investigative efficiencies

Public safety officials state that facial recognition systems create efficiencies and provide investigative leads that would not exist otherwise. With the proper guardrails in place and sufficient checks and balances guiding the confirmation process, facial recognition technology can identify suspects with fewer policing resources. This could be particularly helpful when local governments face reduced revenues, funding and resources due to COVID-19.

## RISK Bias in facial recognition technology

Facial recognition technology has made great strides in recent years, but the technology in use today tends to make more errors in identifying dark-skinned people and women than light-skinned people and men. A 2018 American Civil Liberties Union (ACLU) study used Amazon's Rekognition, one of the leading facial recognition programs at that time, to search for matches between members of Congress and a database of mug shots.<sup>19</sup> This search produced false positive matches, or incorrectly reported that an unknown picture matched a known picture in a database, for 28 members of Congress, 40% of whom were people of color, even though only roughly 20% of Congressional members are

people of color. A 2018 MIT study showed that IBM and Microsoft systems designed to identify a face's gender worked nearly perfectly on White men but had a 20% failure rate on women of color.<sup>20</sup>

The National Institute of Standards and Technology (NIST) is considered the foremost authority on evaluating facial recognition algorithms.<sup>21</sup> Their 2019 test of facial recognition technology vendors assessed how well 189 facial recognition algorithms, submitted by 99 developers around the world, identified people of different demographics. The study found a wide range in accuracy across developers, with many algorithms 10 to 100 times more likely to inaccurately identify people.

When looking at U.S. law enforcement images, the algorithms identified American Indian, Black and Asian American people as false positive identifications more frequently compared to White people. NIST also found that false positives were more likely with women, the elderly and children, compared to men and middle-aged adults, although the effects of these false positives were smaller than the issues with identification based on race.<sup>22</sup>

Why does the technology continue to misidentify people of color and women? The authors of a 2012 Institute of Electrical and Electronics Engineers (IEEE) study state that part of the misidentification problem with women may occur because they tend to wear more cosmetics than men do, decreasing the consistency of images of their face from one capture to the next.<sup>23</sup> Several technologists attributed higher error rates for people of color because there is less contrast in the imagery than for White individuals, making the mapping of facial features inherently less precise.<sup>24</sup> However, the most compelling explanation of these error rates is that facial recognition algorithms reflect the fact that there is a disproportionately higher number of White images in the training image data set. The algorithms optimize

their performance on the sets of sample faces used to train them. Training sets tend to overrepresent White men, therefore the algorithms become highly proficient at identifying the faces of White men, to the detriment of people of color. In 2011, researchers evaluated a set of algorithms' accuracy and found that, "the East Asian fusion algorithm is more accurate at recognizing the East Asian faces and the Western fusion algorithm is more accurate on the Caucasian faces."<sup>25</sup>

Ambivalence among facial recognition technology companies perpetuates the problem. Not all facial recognition companies test their algorithms for racial bias.<sup>26</sup> NIST began regularly testing for performance by race only in 2017.<sup>27</sup> There has been some progress in this realm; for example, in January 2019, IBM released a data set of 1 million faces, claiming it better represents the human population than do other less current data sets.<sup>28</sup>

However, cities can still hold facial recognition technology vendors accountable. Many cities seeking vendors for facial recognition technology have minimum thresholds for accuracy overall; they should also have accuracy thresholds with respect to demographic groups.<sup>29</sup> The technology's strong performance regarding White males has masked its shortcomings concerning other groups, especially people of color, giving cities a false impression of reliability.

**The first known misidentification and wrongful arrest because of a false positive facial recognition match in the U.S. occurred in Detroit, Michigan. Robert Julian-Borchak Williams, a Black man, was accused and arrested by two Detroit Police Department officers in January 2020 on shoplifting charges, based on store video footage of an October 2018 incident. A review of the investigative process revealed a lack of controls in the process and loose standards for identification. The city has since updated its facial recognition policy.**

Hill, K. (2020, June 24). Wrongfully Accused by an Algorithm. New York Times. <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>



It is critical that facial recognition technology companies do all they can to avoid false matches. A false match can lead law enforcement to investigate or arrest an innocent person. Although misidentifications do not always lead to wrongful convictions, a search or arrest itself can be humiliating or trigger trauma, and both entail an increased risk of confrontation or violent escalation. Blacks have a disproportionate number of encounters with police, so they will likely be queried more often in facial recognition searches.<sup>30</sup>

They are also arrested at a higher rate than other groups — in some states, five times as often.<sup>31</sup> They are overrepresented in mug shot databases, meaning that facial recognition technology is more likely to identify a person as a suspect in the U.S. if the person is Black. Because the data sets used for training facial recognition algorithms are distinct from the comparison data sets that these algorithms use in practice, the underrepresentation of Blacks in training data sets and their overrepresentation in mug shot databases make the population for which the technology works least accurately the group most vulnerable to misidentification.

American law enforcement's widespread use of facial recognition technology could negatively and disproportionately affect Black communities. Until commercial companies make training data sets more representative, and cities and the public have processes for holding companies accountable for racial disparities in their algorithms' performance, the use of facial recognition technology will continue to raise significant concerns of racial equity.

The technology's strong performance regarding white males has masked its shortcomings concerning other groups, giving cities a false impression of reliability.

## RISK

### Constitutional concerns: First and Fourth Amendments

Law enforcement's use of facial recognition technology raises several constitutional issues. The Constitution does not state whether the police can use something like facial recognition technology, and courts have yet to fully deal with this issue. However, the primary concerns are

- ◆ whether identifying someone through facial recognition constitutes an unlawful search under the Fourth Amendment and
  - ◆ whether this could infringe upon First Amendment rights of assembly and free speech.
- Ultimately, although government use of facial recognition technology would not per se infringe upon First and Fourth Amendment rights, sufficiently widespread and pervasive deployment of the technology could be interpreted to do so.



### Fourth Amendment issues

The Fourth Amendment protects people from unlawful police searches where they have a reasonable expectation of privacy. In *Katz v. United States*, the Supreme Court held that a reasonable expectation of privacy depends on

- ◆ whether the person subjectively expected privacy in that circumstance and
  - ◆ whether society recognizes that expectation of privacy as reasonable.<sup>32</sup>
- In theory, the use of facial recognition technology in a public safety context — surveilling public spaces and capturing the image of someone's face — seems to uphold the Fourth Amendment guidelines. Entering a public space generally removes a reasonable expectation of privacy; in *Katz* the Court stated, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."<sup>33</sup> Special cases, such as the act of entering the phone booth at issue in *Katz*, have been treated as exceptions in which it is reasonable for a person to expect some measure of privacy despite being in public.<sup>34</sup> However, the surveillance video that most municipalities use for facial recognition applications is captured in public spaces that would not include any such exception.

The Supreme Court has deemed a person's face to be beyond Fourth Amendment protection. In *United States v. Dionisio*, the Supreme Court refused to recognize an expectation of privacy over certain personal attributes, stating, "Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."<sup>35</sup>

However, the Court has started to expand the expectation of privacy it considers reasonable in cases in which modern technology drastically enhances law enforcement's capabilities. The Court is increasingly willing to find violations of Fourth Amendment rights when new technologies allow the government to track people far more persistently than was previously possible. In *Jones v. United States*, the Court held that a GPS tracker attached to a person's car for several weeks constituted a Fourth Amendment violation.<sup>36</sup>

The Court held that although a driver could not reasonably expect their location at any one instant to be private while they traveled in public, they did have a reasonable expectation that no one would know every location they visited.<sup>37</sup> In *Carpenter v. United States*, the Supreme Court held that warrantless acquisition of data listing the cell towers that a person's phone pinged for 127 days, which gave investigators a map of his movements, constituted

a violation of his Fourth Amendment rights, as the knowledge of all of his movements over this period gave the government an excessively intimate and invasive window into his life.<sup>38</sup>

In both cases, although knowledge of the person's location at one instant was not particularly invasive, knowledge of their location at every instant across many days did cross that line. If police use facial recognition technology to track people's whereabouts for an extended period, this could be deemed a violation of Fourth Amendment rights. However, if the police use it in limited fashion to confirm or deny a person's presence at any one time and place, this would likely not be deemed a violation of Fourth Amendment rights, as long as that location is a public place that does not create a reasonable expectation of privacy.

The Court has also held that use of non-publicly available technology to conduct otherwise impossible searches violates Fourth Amendment rights. In *Kyllo v. United States*, the Supreme Court held that police use of a thermal imaging device to determine whether a man was growing marijuana in his apartment was an unlawful search.<sup>39</sup> The police did not physically enter the suspect's home; nonetheless, the lack of widespread public use or knowledge of devices that could remotely penetrate the home in that manner created a reasonable expectation of privacy that the Court was willing to recognize.

However, the thermal scanner was not widely available, and the way the police used it — scanning the exterior wall of a person's home to provide information about what was occurring inside — was not something the public generally knew was possible. Facial recognition technology is available in enough applications that the public cannot be said to be unaware of it. A 2019 Pew Research Center survey found that most American have heard of facial recognition technology (86%), with 25% having heard a lot about it.<sup>40</sup> In the vein of new technology enabling violations of privacy, *California v. Ciraolo* is more relevant to facial recognition technology than is *Kyllo*.<sup>41</sup> In *Ciraolo*, the Supreme Court held that police use of a plane to conduct aerial surveillance on a suspected marijuana grower's property was not unlawful, as the

routine practice of commercial flight in public airways at that point in history made any expectation of privacy unreasonable regarding objects plainly visible from the sky.<sup>42</sup> These cases both turn on whether law enforcement uses the technology to gain information about people in a way that the public could reasonably expect. As public video surveillance is not a new concept and facial recognition technology is also now widespread, the latter's use to identify individuals in public would likely not raise the same Fourth Amendment concerns as did *Kyllo*.

#### First Amendment issues

Law enforcement's use of facial recognition technology can potentially infringe on First Amendment rights of free speech and assembly. Some argue that facial recognition technology can do this by depriving people of their ability to speak and gather anonymously, because the knowledge that they are being tracked could deter people from engaging in speech or assembly in which they otherwise would engage.<sup>43</sup>

The Supreme Court has held that the First Amendment right of free speech includes the right to speak anonymously.<sup>44</sup> In *NAACP v. Alabama*, the Court held that the NAACP could not be compelled to disclose its members' identities, as doing so would hinder their ability to express their ideas.<sup>45</sup> In *Talley v. Alabama*, the Court held that the First Amendment protected

the right to distribute pamphlets anonymously, stating, "[t]here can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."<sup>46</sup> The Supreme Court's recognition that a degree of anonymity is necessary for free expression runs contrary to facial recognition technology's capacity to essentially end anonymity in public spaces.

Judicial treatment of police surveillance of public gatherings is mixed. In *Laird v. Tatum*, the Supreme Court held that the military's surveillance of a public gathering did not inhibit the group's ability to express their views, absent any danger of a direct injury stemming from the surveillance.<sup>47</sup> However, at some point, surveillance can cross the line. In 2015, the Third Circuit ruled in *Hassan v. City of New York* that extensive police surveillance of Muslim Americans following the September 11 attacks did harm a group that was singled out for its religious affiliations, and was thus constitutionally impermissible.<sup>48</sup>

Facial recognition technology may entail more passive surveillance than in *Hassan*. However, the technology also goes far beyond simply photographing a gathering as in *Laird*, when it means not only photographing but also immediately identifying people. In 2016 the police used facial recognition technology on pictures in social media posts to identify and arrest protestors in Baltimore after

Freddie Gray's death.<sup>49</sup> The ACLU stated that this raised significant First Amendment concerns.<sup>50</sup> Police use of facial recognition technology as another investigative tool is unlikely to be held categorically impermissible under the First Amendment. However, certain uses, such as using the technology to monitor specific gatherings or to track specific groups over extended time periods, could inhibit free expression and assembly rights and be held to violate the First Amendment. Although continued improvements to facial recognition technology could remedy many of the other problems stemming from it, the threat that facial recognition technology poses to constitutionally protected rights will only increase as the technology grows more accurate.

## RISK

### City liability

The doctrine of sovereign immunity traditionally protects governments and government officials from lawsuits. However, both states and the federal government have carved out exceptions allowing government officials to be held liable in certain situations.

#### Liability for violations of constitutional rights

In a 2017 report, the Bureau of Justice Assistance in the U.S. Department of Justice warned that “misuse of face recognition information may expose agencies participating in such systems to civil liability.”<sup>53</sup> One of these sources of liability stems from 42 U.S.C. § 1983, a statute giving people the right to sue a “person” acting under government authority who deprives them of their constitutional rights, such as those discussed above under the First and Fourth Amendments. People can directly sue individual government officials in their personal capacities. However, given that governments can pay more money in damages or in a settlement than individuals can, plaintiffs will often try to sue the government.

In the 1978 case *Monell v.*

*Department of Social Services*, the Supreme Court held that a city is a “person” for the purposes of § 1983 liability, opening cities to liability for constitutional violations. Cities can either be sued directly, or they can be held liable for their

employees’ actions.<sup>52</sup> Cities can only be held liable for their employees’ actions if the employees act under the color of authority and the violation resulted from an official policy that is the “moving force” of the constitutional violation. Courts have determined several specific categories of city actions that can result in a violation under § 1983:

- ◆ **A formal policy established by the city or an informal policy or custom that is so pervasive as to constitute a de facto policy of the city.** For example, a police department policy of using deadly force absent probable cause of an imminent threat of harm would amount to a violation of citizens’ Fourth Amendment rights.<sup>53</sup> In the context of facial recognition, if courts were to determine that facial recognition surveillance in public areas violates the Fourth Amendment, a city that officially deploys this surveillance would be at risk of liability under § 1983.
- ◆ **A failure to train or supervise employees to such an extent as to demonstrate “deliberate indifference” toward constitutional rights.**<sup>54</sup> For example, if cities deploy facial recognition technology without training officers in how to use it and these officers subsequently falsely arrest numerous people, the cities could be held liable for Fourth Amendment violations. The doctrine of “qualified immunity” may protect officers from liability under § 1983 when they are sued as individuals. Officers are liable

for violations of constitutional rights only if a “reasonable officer” would know that his or her conduct was unlawful in the situation in question.<sup>55</sup>

#### ◆ A single decision by a “final policymaker” for the government.

This “final policymaker” would be an official with authority to decide on a policy for a given subject matter. This could be a mayor or an official delegated to make decisions in a certain area. State courts have different approaches to determining who constitutes a “final policymaker” for the purposes of this rule.<sup>56</sup> In the facial recognition context, if there is no public discussion about the use of facial recognition during official duty but a chief executive approves it unilaterally, cities could be held liable for unintended or improper consequences.

#### ◆ A higher-ranking official knows and approves of a subordinate’s decision that violates a citizen’s constitutional rights.

A mere failure to overrule a subordinate does not amount to an affirmative endorsement.<sup>57</sup> However, without a policy that provides proper checks and balances for the use of facial recognition technology, city officials could be liable for improper actions of its public safety department.

#### Municipal tort liability

Apart from considering federal § 1983 constitutional claims, cities could also face municipal liability for torts such as negligence or battery. Most states have passed tort claims laws, which allow people to sue state and local officials for certain torts. These laws are often modeled on the Federal Tort Claims Act (FTCA) of 1946, which enables people to sue the federal government for similar violations. Under the FTCA and most state tort claims acts, governments are liable for tort violations committed by their employees only if those officials acted within the scope of their employment.

However, the types of claims for which cities are liable vary widely depending on the state. Some states waive immunity only for certain types of claims. No claims have yet been brought against a government under tort law for the misuse of facial recognition. However, a pending

claim against Apple in a federal court in New York could indicate how courts will handle this issue. Apple accused Ousmane Bah of stealing from one of its stores after the company's facial recognition algorithm misidentified him as the perpetrator.<sup>58</sup> Bah claims that the actual perpetrator presented as identification Bah's learner's permit, which does not include a photo and which Bah lost on the street in the months prior. As a result, Apple's facial recognition software linked the perpetrator's face, captured on surveillance footage, with Bah's name and address. Bah is now suing Apple for negligence, claiming that it carelessly used its facial recognition software to wrongfully identify him, seeking \$1 billion in damages.<sup>59</sup> The litigation is ongoing. The outcome of this lawsuit will indicate how courts may treat similar claims against cities or companies for the negligent use of facial recognition technology resulting in misidentifications.

### State biometric privacy laws

A few states (e.g., Oregon, California, Illinois, Texas and Washington) have passed biometric privacy laws that hold private companies liable for privacy violations resulting from the collection of biometric data. These laws regulate companies' retention and protection of biometric data, and they require individual consent for collection of biometric data.<sup>60</sup> None of these laws hold governments directly liable, but the laws could have implications for cities seeking to acquire facial recognition technology. Vendors may be more reluctant to operate in states that have strict biometric privacy laws, as they may face greater liability. Alternatively, to mitigate this liability risk, vendors may seek to shift liability to cities. If cities agree to indemnify facial recognition vendors in their contracts with these vendors, they could face greater legal and monetary risk.

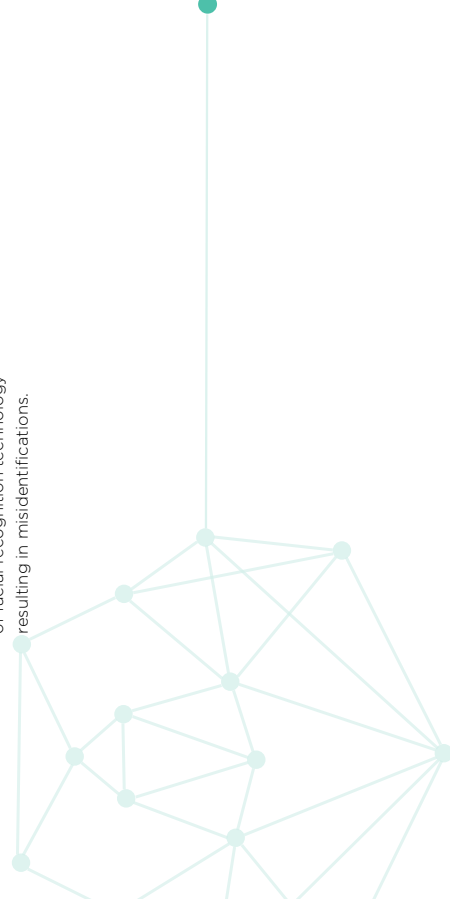
### Shifting of liability in contracts

Contracts between cities and vendors demonstrate various approaches to liability. In some contracts, cities have agreed to assume much of the liability for claims resulting from the misuse of facial recognition technology, agreeing to indemnify the vendor and pay for damages that may result from lawsuits. Article XI of the San Diego Association of Government (SANDAG) contract with FaceFirst states, "FaceFirst shall not be responsible, and shall have no liability to Customer or any third parties allegedly aggrieved in connection with the use of the product by Customer." Under Article XII of the contract, SANDAG agrees to "defend at its expense any legal proceeding brought by a third party...against FaceFirst," provided that the claim against FaceFirst is connected with SANDAG's failure to comply with "any applicable law."<sup>61</sup> Under this contract, if SANDAG collects data in a way that violates a state data privacy law, it could be liable to pay for damages assessed against FaceFirst.

A Detroit, Michigan, contract with DataWorks Plus reflects an alternative approach, under which the vendor assumes much of the liability risk. Under Article 2.04 of that contract, DataWorks Plus agrees to "remain liable in accordance with applicable law for all damages to the City caused by the Contractor's negligent performance or nonperformance of any of the Services furnished under this Contract." DataWorks Plus also agrees to fully indemnify Detroit for

any claims asserted against the city that arise from DataWorks Plus's own negligence.<sup>62</sup> By contrast, FaceFirst agrees to fully indemnify SANDAG only for intellectual property claims, that is, claims that FaceFirst's technology violated another company's patents or copyrights.<sup>63</sup>

Before the City and County of San Francisco, California, banned facial recognition, its contract with Cogent struck a middle ground between these two cases. As in the Detroit contract with DataWorks Plus, Cogent agreed to indemnify the city and its employees from claims "arising directly or indirectly from Contractor's performance of this Agreement." However, unlike the DataWorks Plus contract, Cogent included a limitation in this indemnification clause: it disclaimed all responsibility in cases resulting from the "active negligence or willful misconduct" of San Francisco.<sup>64</sup> As these cases illustrate, minor changes in the language of a city's contract with a facial recognition vendor can have substantial implications for the city's risk of liability.



# How are cities regulating facial recognition?

A few states have passed legislation limiting the scope of facial recognition usage, including three states that have banned law enforcement from using facial recognition on body cameras (California, New Hampshire and Oregon). In its 2019–2020 session, the U.S. Congress held hearings and proposed bills related to facial recognition, but none of these proposed laws would directly impact local law enforcement. Federal or state legislation may eventually preempt or nullify local legislation. However, cities are taking the lead in shaping facial recognition policy. Not every city that now uses facial recognition has voted on a policy to govern its use. Some cities have developed policies that limit the scope of law



## How Some Cities Regulate Facial Recognition for Government Use



### LIMITED SCOPE OF USE

New York, New York  
Detroit, Michigan  
Seattle, Washington  
Lawrence, Massachusetts  
Davis and Palo Alto, California  
Nashville, Tennessee  
Pittsburgh, Pennsylvania



### BAN

San Francisco, Oakland and Berkeley, California  
Boston, Brookline, Cambridge, Northampton, Easthampton and Somerville, Massachusetts  
Portland, Oregon  
Portland, Maine  
Jackson, Mississippi  
New Orleans, Louisiana  
Madison, Wisconsin  
Minneapolis, Minnesota

\*Only includes examples with publicly available policies

enforcement's permitted uses. Several cities have banned the technology entirely. Most cities regulating facial recognition focus solely on governmental use. To date, only the City of Portland, Oregon, has restricted private use of facial recognition. This section highlights a few cities and their experiences with facial recognition technology.

### Regulating surveillance technology

Guided by the ACLU's Community Control Over Police Surveillance framework, at least 15 cities across the country have passed surveillance technology ordinances. Most of these ordinances indirectly govern

the use of facial recognition and require community oversight over any use of surveillance technology.<sup>65</sup> For example, Oakland's surveillance ordinance, considered one of the strictest in the country, requires law enforcement to create a "technology impact report" on new surveillance technologies that covers issues such as data storage and civil liberties.<sup>66</sup>



SEATTLE, WASHINGTON



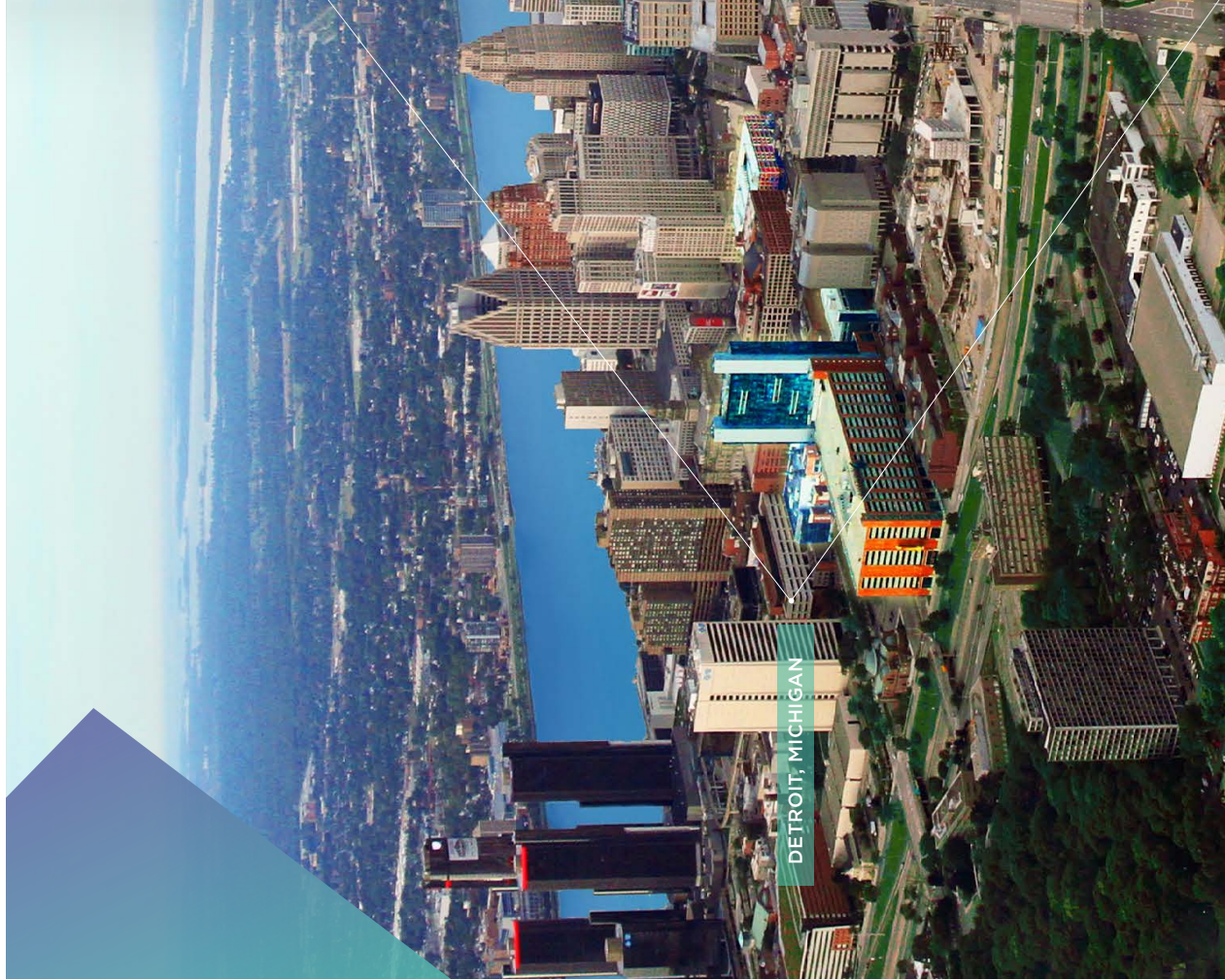
## CITY OF SEATTLE, WASHINGTON

### Policy limiting use of facial recognition, but technology no longer used

The City of Seattle, Washington, began using facial recognition technology in 2014. With the help of a \$1.5 million grant from the Department of Homeland Security, Seattle, Washington, purchased a facial recognition system from NEC. The Seattle City Council voted on a facial recognition use policy that allowed law enforcement to use the technology in limited circumstances. Specifically, Seattle permitted the use of facial recognition to identify people taken into custody when they could not be identified by other means. The Seattle City Council approved funding for the system under a policy created in consultation with the ACLU of Washington. Seattle Sound 911, a public safety agency covering three counties in the Seattle region, operated the system.<sup>67</sup>

Seattle required that the vendor achieve a 96% identification accuracy rate.<sup>68</sup> Police used the system in a limited capacity to identify people who had been taken into custody but could not be identified. According to city officials, police conducted fewer than 50 searches in four years. Recognizing the system's limited utility, Seattle Police stopped using the technology in 2018. Also motivating this decision was the difficulty of receiving approval for the system's use through the city's new surveillance oversight ordinance, passed in 2017, because of the overly bureaucratic process for approved use and public calls to ban the use of facial recognition.





## CITY OF DETROIT, MICHIGAN

### Policy limiting use of facial recognition

Initiating a three-year contract with the facial recognition vendor DataWorks Plus, Detroit, Michigan, purchased a facial recognition system in July 2017 for \$1 million. Under Detroit's public-private partnership Project Green Light, businesses and organizations could purchase and install facial recognition cameras that feed captured images to the police.

These images could then be compared to a database of mug shot photos maintained by Detroit police.<sup>69</sup> After a series of public debates, the Detroit Board of Police Commissioners, a civilian oversight body composed of officials either elected or appointed by the mayor, adopted a new policy in September 2019.

This policy prohibits the use of real-time surveillance and allows the use of facial recognition only during investigations of violent crimes and home invasions.

The policy also requires that at least two officers verify matches produced by the facial recognition system. It imposes harsh penalties for officers who abuse the technology, including termination of employment.<sup>70</sup>





## SAN FRANCISCO BAY AREA, CALIFORNIA



### SAN FRANCISCO BAY AREA, CALIFORNIA Policies banning facial recognition

Many cities in the San Francisco Bay Area have banned city officials' use of facial recognition. The San Francisco Police Department used facial recognition for nine years prior to the Board of Supervisors' decision to ban the technology in May 2019. San Francisco purchased a system from 3M Cogent and, like Seattle, required the vendor to regularly test the accuracy of its algorithm. San Francisco Police could search between half a million and one million mug shots. San Francisco's use policy was not publicly available before the Board of Supervisors voted to ban use of the technology.<sup>71</sup> San Francisco Supervisor Aaron Peskin, who introduced the bill, argued that a ban was necessary because the technology is "so fundamentally invasive" that it should not be used at all.<sup>72</sup>

The City of Oakland followed suit in banning facial recognition in July 2019. City Council President Rebecca Kaplan explained her rationale for introducing her bill banning the technology: "I welcome emerging technologies that improve our lives and facilitate city governance, but when multiple studies show a technology is flawed, biased, and is having unprecedented, chilling effects to our freedom of speech and religion, we have to take a stand."<sup>73</sup>

After discussing facial recognition in 2018 and much of 2019 at city council meetings and the council's Public Safety Committee, the City of Berkeley Council became the fourth U.S. city to ban facial recognition, in October 2019, citing concerns about both privacy and racial bias.<sup>74</sup>



# How can cities better approach the topic of facial recognition publicly?

Cities have a responsibility to their communities to thoughtfully explore emerging technologies that can aid the greater good. The conversation concerning facial recognition is particularly sensitive given the technology's imperfections and how it is frequently implemented and used behind closed doors. By following these recommendations, cities can better facilitate public discussions about facial recognition technology in their communities.



## 1 Engage with residents to develop policies, and be transparent about facial recognition use.

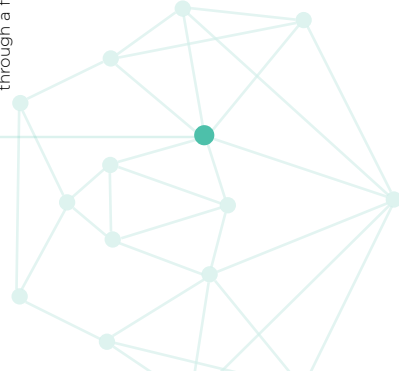
- ◆ Require elected officials to vote on any decision to use facial recognition technology before law enforcement can implement it.
- ◆ Insist on community input in a public forum (e.g., by hosting town hall meetings) before voting on a decision to use facial recognition.
- ◆ Collaborate with a diverse group of non-governmental organizations and stakeholders when designing a policy, in order to achieve broader community buy-in.
- ◆ Consider establishing a citizen oversight board, with real authority and budget, that regularly reports on the state of biometric surveillance in the city.
- ◆ Make any facial recognition use policies publicly available online.
- ◆ After a facial recognition policy has been adopted, establish a public awareness campaign in order to educate citizens on the scope of the technology and the city's use policy.
- ◆ Ensure that the public can submit complaints about any issues they encounter related to the government's use of facial recognition.
- ◆ Disclose to the public the locations of cameras deployed in public areas if those cameras provide imagery to be used in facial recognition.
- ◆ Require regular internal auditing by independent ombudsmen to ensure that the system is working as intended and not discriminating against certain groups.
- ◆ Consider requiring recurring votes to reauthorize a facial recognition use policy annually or biannually.
- ◆ Conduct an annual or biannual review of the facial recognition system's effectiveness, and ensure elected officials' access to the review (e.g., how often it is used and assists investigations).

## 2 Establish a training program for law enforcement and other users of a facial recognition system.

- ◆ Require that all officers who are cleared to use the technology be extensively trained on how to use it. Make sure that officers are aware of the probabilistic nature of the technology.
- ◆ Establish a high probability threshold for matches before the technology can be used in an investigation.
- ◆ Require double-blind confirmation before a match is determined. Two different officers must independently review and confirm the match. Retain thorough records of use of the system and approvals.
- ◆ Prohibit officers from making an arrest based solely on a facial recognition match.
- ◆ Set a high standard for the quality of photos that officers can run through a facial recognition search.
- ◆ Forbid officers from using police sketches or celebrity doppelganger photos in lieu of real photos of suspects.
- ◆ Require implicit bias training to ensure that bias does not influence the ways in which officers use the technology.
- ◆ Educate officers on the legal consequences of misusing the technology, including violations of constitutional rights and, depending on the state, tort violations.
- ◆ Require that officers who deliberately misuse the technology be swiftly held accountable by the department or city, including through suspensions or firings, regardless of outside lawsuits.

## 3 Limit the scope of facial recognition use to reduce the risk of misidentifications and privacy violations.

- ◆ Require that officers have at least individualized, reasonable suspicion of a crime before running a suspect's photos through a facial recognition database for identification purposes.
- ◆ Limit the use of facial recognition to investigations of violent offenses.<sup>76</sup>
- ◆ Limit the use of real-time public surveillance to a narrow set of situations involving life-threatening emergencies or major violent crimes such as terrorism, and ensure that law enforcement obtains a warrant based on probable cause before conducting such surveillance.
- ◆ If feasible, consider installing a system that alerts law enforcement only when surveillance cameras capture a suspect's face, which will reduce privacy violations of innocent people.
- ◆ Consider the pros and cons of using either mug shot photos or driver's license photos as the source of a facial recognition database.
- ◆ A database of driver's license photos includes more people and, thus, may be more likely to include a suspect. Furthermore, it is not skewed toward subsections of the population, particularly people of color, that are overrepresented in mug shot databases.<sup>76</sup> However, every driver in a state will be vulnerable to a false identification. If a city wants to use driver's licenses as the source of a photo database, consider waiting for state legislature approval so that citizens are aware that their photos are used in this way.
- ◆ Mug shot databases are smaller and may be less likely to include a suspect. Certain population groups, particularly people of color, are overrepresented in these databases. However, if properly updated to remove people found to be innocent, these databases include only people convicted of a crime and who have, thus, already lost some liberties. If a city wants to use mug shots as the source of a photo database, ensure that the database includes only people convicted of a crime and not those who were exonerated or never charged.



## 4 Institute rigorous standards for data storage and cybersecurity to ensure protection of citizens' biometric data.

- ◆ Delete any photo or video footage that has been analyzed with facial recognition technology and is not pertinent to an ongoing investigation.
- ◆ Regularly scrub databases of mug shot photos to exclude people found innocent or against whom charges were dropped.
- ◆ Restrict the length of time that data is stored to reduce the risk of a data breach<sup>77</sup>
- ◆ Restrict storage of biometric data to a single database to minimize the number of entry points potentially vulnerable to hackers.
- ◆ Require all employees who access the system to follow basic cybersecurity hygiene practices, including, at a minimum, establishing two-factor authentication on their accounts. Restrict permitted access both in written policies and as a technical matter.
- ◆ Ensure state-of-the-art forensic tracking of any use of a facial recognition system before it is deployed.
- ◆ Create policies and systems governing and constraining sharing of facial recognition results within city hall or police departments, to limit opportunities for non-approved uses of the technology.



## 5 Follow best practices for drafting contracts to ensure accuracy and reduce legal risk.

- ◆ Contracts with facial recognition vendors should require the vendors to regularly test their algorithms for both accuracy and racial bias.
- ◆ Require vendors to certify that their technology's algorithms use a demographically representative training set. These certifications should be updated regularly.
- ◆ Organizations using cameras provided by contractors should require the cameras to meet high photo-quality standards.
- ◆ Remove contract language in which a vendor disclaims responsibility for the facial recognition algorithm's accuracy.
- ◆ Pay close attention to the wording of indemnification clauses, to ensure that the city does not adopt too much liability for the vendor and that the vendor is held accountable for its errors. This is particularly important in states that have biometric privacy laws under which private companies can be held liable.
- ◆ Before signing a long-term contract with a vendor for a full facial recognition program, consider signing a short-term contract for a pilot program to determine whether facial recognition is useful and worthwhile.

# Endnotes

- <sup>1</sup> Whitehead, N. (2014, April 23). *Face Recognition Algorithm Finally Beats Humans*. Science. Retrieved from [https://www.sciencemag.org/news/2014/04/face-recognition-algorithm-finally-beats-humans?z3f\\_98](https://www.sciencemag.org/news/2014/04/face-recognition-algorithm-finally-beats-humans?z3f_98).
- <sup>2</sup> Brownlee, J. (2019, May 31). *A Gentle Introduction to Deep Learning for Face Recognition*. Machine Learning Mastery. Retrieved from <https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/>.
- <sup>3</sup> Garvie, C. et al. (2016, October 18). *The Perpetual Line-up*. Georgetown Center on Privacy and Technology. Retrieved from <https://www.perpetualineup.org/>.
- <sup>4</sup> King, K. (2019, October 7). *New York City Lawmakers Look To Regulate Facial Recognition Tools*. Wall Street Journal. Retrieved from <https://www.wsj.com/articles/new-york-city-lawmakers-look-to-regulate-facial-recognition-tools-11570485799>.
- <sup>5</sup> Steele, K. (2018, November 29). *Delta Unveils First Biometric Terminal in U.S. in Atlanta*. Next Stop: Detroit. Delta Press Release. Retrieved from <https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit>.
- <sup>6</sup> Draper, K. (2018, March 13). *Madison Square Garden Has Used Face-Scanning Technology on Customers*. New York Times. Retrieved from <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>.
- <sup>7</sup> Simonte, T. & Barber, G. (2019, October 17). *The Delicate Ethics of Using Facial Recognition in Schools*. WIRED. Retrieved from <https://www.wired.com/story/delicate-ethics-facial-recognition-schools/>.
- <sup>8</sup> Mikkelsen, D. (2018, October 31). *Two Seattle Schools Among First To Use Facial Recognition Software in U.S.* King5 News. Retrieved from <https://www.king5.com/article/news/education/two-seattle-schools-among-first-to-use-facial-recognition-software-in-us/281-609937626>.
- <sup>9</sup> Harding, H. (2019, July 9). *Boise Will Spend \$52,000 on Facial Recognition To Keep "Banned" People Out of City Hall*. Idaho Statesman. Retrieved from <https://www.idahostatesman.com/news/local/community/boise/article32411592.html>.
- <sup>10</sup> Crist, R. (2019, September 9). *Google's Got a New Face-Tracking Camera for Your Home. We've Got Questions*. Cnet. Retrieved from <https://www.cnet.com/news/google-nest-hub-max-a-new-face-tracking-camera-for-your-home-weve-got-questions/>.
- <sup>11</sup> Nguyen, N. & Mac, R. (2019, August 30). *Ring Says It Doesn't Use Facial Recognition, But It Has "A Head Of Face Recognition Research"*. Buzzfeed. Retrieved from <https://www.buzzfeednews.com/article/nicolinguyen/amazon-ring-facial-recognition-ukraine>.
- <sup>12</sup> Siminoff, J. (2019, August 28). *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*. Ring Blog. Retrieved from <https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/>.
- <sup>13</sup> Garvie, C. & Frankle, J. (2016, April 7). *Facial-Recognition Software Might Have a Racial Bias Problem*. The Atlantic. Retrieved from <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/47699/>.
- <sup>14</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>15</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>16</sup> Garvie, C. (2019, May 16). *Garbage In, Garbage Out*. Georgetown Center on Privacy and Technology. Retrieved from <https://www.flawedfacedata.com/>.
- <sup>17</sup> Garvie, *Garbage In, Garbage Out*.

- <sup>18</sup> Cwiek, S. (2019, September 19). *Detroit Police Commissioners Approve Facial Recognition Policy*. Michigan Radio. Retrieved from <https://www.michiganradio.org/post/detroit-police-commissioners-approve-facial-recognition-policy>.
- <sup>19</sup> Snow, J. (2018, July 26). *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. American Civil Liberties Union. Retrieved from <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.
- <sup>20</sup> Buolamwini, J. et al. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of Machine Learning Research, 81, 1-15. Retrieved from <https://proceedings.mlr.press/v81/buolamwini18.html>.
- <sup>21</sup> Simonte, T. (2019, July 22). *The Best Algorithms Struggle to Recognize Black Faces Equally*. WIRED. Retrieved from <https://www.wired.com/story/best-algorithms-struggle-to-recognize-black-faces-equally/>.
- <sup>22</sup> National Institute of Standards and Technology. (2019, December). *National Institute of Standards and Technology Interagency or Internal Report 828*. Retrieved from <https://doi.org/10.6028/NIST.IR.8280>.
- <sup>23</sup> Klare, B. et al. (2012). *Face Recognition Performance: Role of Demographic Information*. IEEE Transactions on Information Forensics and Security, 7, 1789-1802. Retrieved from <http://openbmtrics.org/publications/klare2012demographics.pdf>.
- <sup>24</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>25</sup> Phillips, P.J. et al. (2011). *An Other-Race Effect for Face Recognition Algorithms*. ACM Transactions on Applied Perception, 8(2), 1-11.
- <sup>26</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>27</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>28</sup> Smith, J. (2019, January 29). *IBM Research Releases 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition Systems*. IBM Research Blog. Retrieved from <https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/>.
- <sup>29</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>30</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>31</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>32</sup> Katz v. United States, 389 U.S. 347 (1967).
- <sup>33</sup> Katz v. United States, 389 U.S. 351 (1967).
- <sup>34</sup> Katz v. United States, 389 U.S. 348 (1967).
- <sup>35</sup> US v. Dionisio, 410 U.S. 1 (1973).
- <sup>36</sup> United States v. Jones, 565 U.S. 400 (2012).
- <sup>37</sup> United States v. Jones, 565 U.S. 404 (2012).
- <sup>38</sup> Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
- <sup>39</sup> Kyllo v. United States, 533 U.S. 27, 29-30 (2001).
- <sup>40</sup> Smith, A. (2019, September 5). *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*. Pew Research Center. Retrieved from [https://www.pewresearch.org/internet/wp-content/uploads/sites/9/09/05.19/facial\\_recognition\\_FULLREPORT\\_update.pdf](https://www.pewresearch.org/internet/wp-content/uploads/sites/9/09/05.19/facial_recognition_FULLREPORT_update.pdf).
- <sup>41</sup> California v. Cirado, 476 U.S. 207, 213 (1986).

- <sup>42</sup> California v. Ciraolo, 476 U.S. 207, 215 (1986).
- <sup>43</sup> Hamann, H. et al. (2019, Spring). *Facial Recognition Technology: Where Will It Take Us? The American Bar Association Criminal Justice Magazine*. Retrieved from [https://www.americanbar.org/groups/criminal\\_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/](https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/).
- <sup>44</sup> Nat'l Ass'n for Advancement of Colored People v. State of Ala. Ex rel. Patterson, 357 U.S. 449 (1958).
- <sup>45</sup> Nat'l Ass'n for Advancement of Colored People v. State of Ala. Ex rel. Patterson, 357 U.S. 449 (1958).
- <sup>46</sup> Talley v. California, 362 U.S. 60, 63 (1960).
- <sup>47</sup> Laird v. Tatum, 408 U.S. 1 (1972).
- <sup>48</sup> Hassan v. City of New York, 804 F.3d 277, 292 (3d Cir. 2015).
- <sup>49</sup> Brandom, R. (2016, October 11). *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*. The Verge. Retrieved from <https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geo-fied-a-api>.
- <sup>50</sup> American Civil Liberties Union. (2016, October 18). *Letter to Principal Deputy Assistant Attorney General Vanita Gupta*. Retrieved from [https://www.aclu.org/sites/default/files/field\\_document/coalition\\_letter\\_to\\_doj\\_crt\\_re\\_face\\_recognition\\_10-18-2016\\_1.pdf](https://www.aclu.org/sites/default/files/field_document/coalition_letter_to_doj_crt_re_face_recognition_10-18-2016_1.pdf).
- <sup>51</sup> U.S. Department of Justice. (2017, December). *Face Recognition Policy Development Template*. Bureau of Justice Assistance, U.S. Department of Justice. Retrieved from <https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf>.
- <sup>52</sup> Monell v. Dep't of Soc. Servs., 436 U.S. 658 (1978).
- <sup>53</sup> Tennessee v. Garner, 471 U.S. 1 (1985).
- <sup>54</sup> City of Canton v. Harris, 489 U.S. 378 (1986).
- <sup>55</sup> Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). The Supreme Court has further clarified that officers are to receive broad deference when the law is unsettled, and that only those officers who are "plainly incompetent" or "knowingly violate the law" will not be covered by qualified immunity. See *Kisela v. Hughes*, 138 S. Ct. 1148, 1152 (2018).
- <sup>56</sup> City of St. Louis v. Praprotnik, 485 U.S. 112 (1988).
- <sup>57</sup> Lytle v. Carl, 382 F.3d 978, 987 (9th Cir. 2004).
- <sup>58</sup> Shaban, H. & Flynn, M. (2019, April 23). *Teen Sues Apple for \$1 Billion, Blames Facial Recognition at Stores for His Arrest*. *Washington Post*. Retrieved from <https://www.washingtonpost.com/technology/2019/04/23/teen-sues-apple-billion-blames-facial-recognition-stores-his-arrest/>.
- <sup>59</sup> Bah v. Apple, Inc., 19-cv-03539, Complaint (S.D.N.Y., Apr. 22, 2019). Retrieved from <https://www.scribd.com/document/407291893/Bah-v-Apple-Inc-19-cv-03539-U-S-District-Court-Southern-District-of-New-York>.
- <sup>60</sup> Seyfarth Shaw LLP. (2020, June 9). *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*. JDSupra. Retrieved from <https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/>.
- <sup>61</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>62</sup> Lipton, B. (2019, August 27). *Rep. Rashida Tlaib and Detroit Police Spar Over City's Milon-Dollar Facial Recognition Contract. Here It Is*. Muckrock. Retrieved from <https://www.muckrock.com/news/archives/2019/aug/27/rep-rashida-tlaib-detroit-facial-recognition/>.
- <sup>63</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>64</sup> Garvie et al., *The Perpetual Line-up*.

- <sup>65</sup> American Civil Liberties Union. *Community Control Over Police Surveillance*. Retrieved from <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance>.
- <sup>66</sup> Tadayon, A. (2018, May 2). *Oakland To Require Public Approval of Surveillance Tech*. *East Bay Times*. Retrieved from <https://www.eastbaytimes.com/2018/05/02/oakland-to-require-public-approval-of-surveillance-tech/>.
- <sup>67</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>68</sup> Mileitch, S. (2016, October 18). *Seattle Police Win Praise for Safeguards With Facial-Recognition Software*. *Seattle Times*. Retrieved from <https://www.seattletimes.com/seattle-news/crime/seattle-police-wins-praise-for-safeguards-with-facial-recognition-software/>.
- <sup>69</sup> Garvie, C. & Moy, L. (2019, May 16). *America Under Watch*. *Georgetown Center on Privacy and Technology*. Retrieved from <https://www.americaunderwatch.com/>.
- <sup>70</sup> Cwiek. *Detroit Police Commissioners Approve Facial Recognition Policy*.
- <sup>71</sup> Garvie et al., *The Perpetual Line-up*.
- <sup>72</sup> Metz, R. (2019, May 14). *San Francisco Just Banned Facial-Recognition Technology*. CNN. Retrieved from <https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html>.
- <sup>73</sup> Ravani, S. (2019, July 17). *Oakland Bans Use of Facial Recognition Technology*. Citing Bias Concerns. *San Francisco Chronicle*. Retrieved from <https://www.sfnchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php>.
- <sup>74</sup> McKay, T. (2019, October 16). *Berkeley Becomes Fourth U.S. City To Ban Face Recognition in Unanimous Vote*. *Gizmodo*. Retrieved from <https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recognti-1839087651>.
- <sup>75</sup> Cwiek. *Detroit Police Commissioners Approve Facial Recognition Policy*.
- <sup>76</sup> Friedman, B. & Ferguson, A. (2019, October 31). *Here's a Way Forward on Facial Recognition*. *New York Times*. Retrieved from <https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html>.
- <sup>77</sup> Bala, N. & Watney, C. (2019, June 20). *What Are the Proper Limits on Police Use of Facial Recognition?* Brookings. Retrieved from <https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/>.



**NLC** NATIONAL  
LEAGUE  
OF CITIES

---

CITIES STRONG TOGETHER



# New Polls Show Facial Recognition Supported By Majority of Americans, Raising More Doubts About the Merits of Bans

By [Ashley Johnson](#)

November 30, 2021

Opponents of facial recognition technologies frequently try to pit the debate as one between the government and ordinary Americans. Anti-technology advocates frame the technology this way because they know that if they can scare Americans into believing that this is a dystopian technology, perhaps Americans will support bans. But most Americans have too much common sense to fall for their spin.

This framing might have convinced a few cities to fall in line, but most Americans see through it. Recent polling from Zogby Analytics builds on previous findings that show a large majority of Americans support beneficial uses of facial recognition technology, including law enforcement use.

Zogby's polling found that three-in-four residents in Massachusetts and Virginia see law enforcement use of facial recognition as appropriate and beneficial. A large majority of residents of both states supported its use for finding missing children, prosecuting sex offenders and traffickers, finding endangered adults, investigating criminal activity, apprehending and prosecuting violent offenders and drug traffickers, and identifying individuals on a terrorist watchlist at public events.

These results line up with a 2019 study by the Center for Data Innovation, which found that only 26 percent of Americans believe the United States government should strictly limit the use of facial recognition technology, and only 18 percent believe the government should strictly



limit its use if it comes at the expense of public safety. A 2020 study by NetChoice similarly found that 83 percent of Americans want state and local governments to improve law enforcement use of facial recognition rather than banning it. A majority of individuals polled supported the technology's use for lead generation, keeping child predators off school grounds, finding missing senior citizens, and locating terrorists during an active terrorist attack.

These and other beneficial uses of facial recognition technology would enable law enforcement to save time and money investigating crimes while obtaining more accurate results than doing the same work through a slow, expensive, inaccurate manual process. Opponents of facial recognition would ban its use completely and cut off police departments and the citizens they protect from these benefits, citing concerns of mass surveillance and widespread bias. But again and again, studies show that most Americans do not want the technology banned.

Rather than support bans on law enforcement use of facial recognition technology, Americans are more likely to support reasonable precautions against inappropriate use of the technology, such as performance standards that would address concerns about inaccuracy and bias and clarification on how Americans' existing constitutional rights and freedoms will continue to protect them regardless of the tools and technologies law enforcement uses.

Framing facial recognition as government versus citizens, rather than acknowledging the significant overlap between these two groups' shared interests in public safety and security and how facial recognition can protect citizens rather than surveil them, will continue to lead to overly restrictive bans like those cities across America have already enacted. These cities have cut themselves off from the many benefits of facial recognition technology, putting their citizens in danger. Rather than follow their lead, other cities, states, and the federal government should listen to what the majority of Americans want and opt for balanced rules and regulation over blanket bans.

## Related ITIF Content

---

November 16, 2021

Should Law Enforcement Use Facial Recognition to Identify Capitol Insurrectionists? Not According to EFF

May 22, 2019

Facial Recognition Bans Handcuff Law Enforcement



July 12, 2021

## Podcast: A Doorman for the Masses—Debunking Attacks on Facial Recognition, With Daniel Castro



### Information Technology & Innovation Foundation

700 K Street NW, Suite 600  
Washington, DC 20001  
mail@itif.org | (202) 449-1351

[Map & Directions](#)

### Other Projects and Affiliates

Global Trade and  
Innovation Policy Alliance

@Work Series: Employment in the Innovation Economy

Innovate4Health

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#)

Structured content powered by [Sanity.io](#)

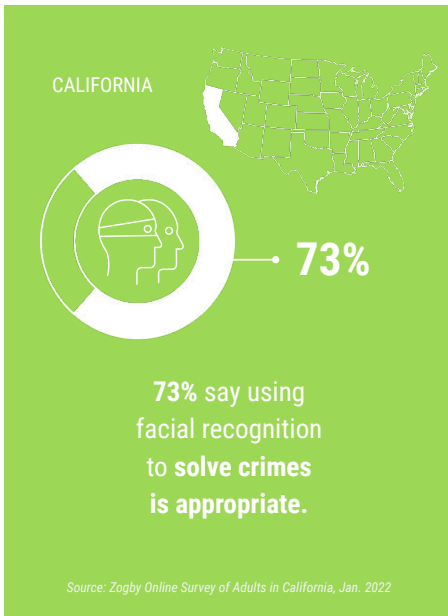
[Copyright Notice](#) | [Privacy Policy](#)

[Sitemap](#)



# CALIFORNIA POLLING

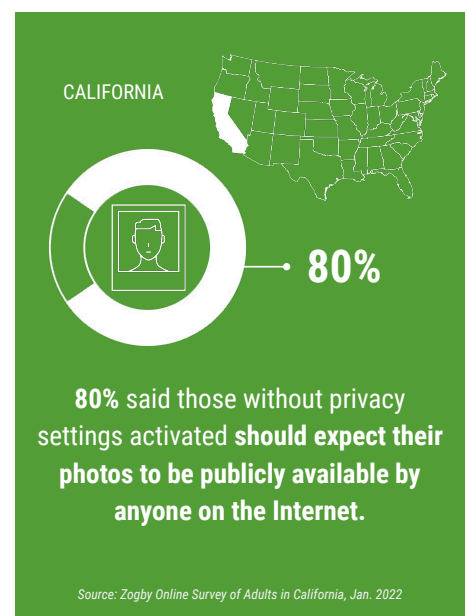
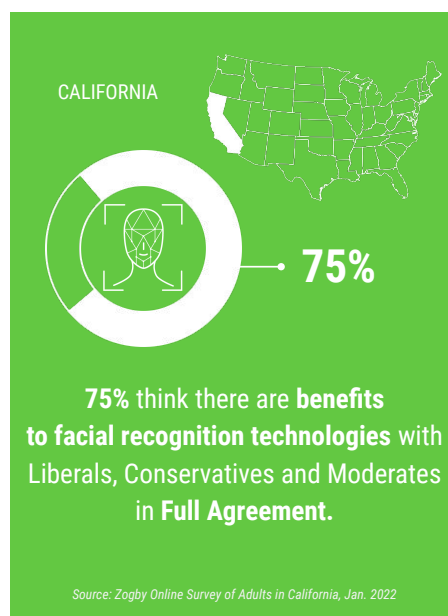
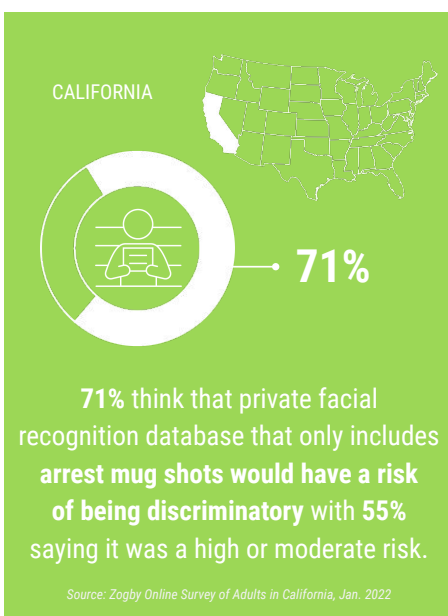
Zogby Analytics Online Survey of Adults in California, Jan. 2022



16

# CALIFORNIA POLLING

Zogby Analytics Online Survey of Adults in California, Jan. 2022



17

# Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots

**For Immediate Release:** AUG 13, 2019



**Media Contact:** [press@aclunc.org](mailto:press@aclunc.org), (415) 621-2493

**Media Contacts:** Daisy Vieyra/ACLU of CA 916-824-3266

Nannette Miranda/Ting 916-319-2019

**SACRAMENTO** — After putting facial recognition technology to the test using photos of all 120 members of the State Legislature, the American Civil Liberties Union of California [released results](#) that further support the need for [AB 1215](#) by Assemblymember Phil Ting (D-San Francisco), which bans facial recognition in police body cameras. The analysis shows that facial recognition software marketed to law enforcement agencies mistakenly matched the faces of one out of five lawmakers, 26 lawmakers total, with images in an arrest photo database, including Ting's. More than half of those falsely identified are lawmakers of color, illustrating the risks associated with the technology's dangerous inaccuracies and the certain erosion of civil liberties should California police departments add the technology to officer body cameras.

"This experiment reinforces the fact that facial recognition software is not ready for prime time - let alone for use in body cameras worn by law enforcement," said Ting. "I could see innocent Californians subjected to perpetual police line ups because of false matches. We must not allow this to happen."

The software falsely identified several Northern California lawmakers, including Assembly members Adam Gray, David Chiu, Frank Bigelow, Jim Cooper, and Mark Stone, and Senators Brian Dahle, Cathleen Galgiani, Jerry Hill, Jim Beall, Scott Wiener, and Steve Glazer. In the real world, such mistakes could have falsely implicated those legislators in a number of alleged crimes. Modeling the test after law enforcement's current known uses of facial recognition technology, the ACLU compared every California state legislator with 25,000 public arrest photos. An independent expert from UC Berkeley verified the results.

"Facial recognition-enabled police body cameras would be a disaster for communities and their civil rights, regardless of the technology's accuracy," said Matt Cagle, Technology and Civil Liberties Attorney, ACLU of Northern California. "Even if this technology was accurate, which it is not, face recognition-enabled body cameras would facilitate massive violations of Californians civil rights."

A [similar test conducted last year](#) by the ACLU misidentified 28 sitting members of Congress. Multiple studies of facial recognition technology have found systems to be inaccurate when used against women and people of color. Axon, a prominent body camera manufacturer, announced in June that it would not add facial recognition to its body camera systems, after its ethics board declared that it could not "ethically justify its use on body-worn cameras." Microsoft also recently refused to allow a California law enforcement agency to use its facial recognition software with officer body cameras due to ethics concerns.

The California State Senate is expected to vote on AB 1215, also known as The Body Camera Accountability Act, in the coming weeks. The Legislature must pass all bills by September 13. The list of falsely identified California lawmakers is available [here](#).

*The Body Camera Accountability Act (AB 1215) is supported by a wide coalition of organizations that safeguard the rights, safety, and freedom of all Californians in all our diversity: ACLU of California, API Chaya, Anti Police-Terror Coalition, Asian Law Alliance, Citizens Rise!, Center for Media Justice, Color of Change, Council on American-Islamic Relations – California, CRASH Space, Data for Black*

*Lives, Electronic Frontier Foundation, Fight for the Future, Indivisible CA, Justice Teams Network, Media Alliance, National Association of Criminal Defense Lawyers, Oakland Privacy, RAICES, README at UCLA, Root Access, San Jose/Silicon Valley NAACP, Secure Justice, Library Freedom Project, Tor Project, and X-Lab.*

###

File Under: **Technology & Civil Liberties**

## BECOME A MEMBER

Real change starts with you – and every one of us can help make a difference.

**JOIN US**

## STAY INFORMED

Sign up for ACLU updates

Your Email

Postal Code

**SIGN UP**



