Congressional Research Service
Informing the legislative debate since 1914

Law Enforcement and Technology: Use of Automated License Plate Readers

August 19, 2024

Congressional Research Service
https://crsreports.congress.gov
R48160

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48160

August 19, 2024

Kristin Finklea
Specialist in Domestic Security

Law Enforcement and Technology: Use of Automated License Plate Readers

Over the past couple of decades, law enforcement use of automated license plate readers (ALPRs; also referred to as LPRs) has increased. These tools are now relatively commonplace in policing. According to the Bureau of Justice Statistics' 2020 Law Enforcement Management and Administrative Statistics Survey, larger law enforcement offices were more likely to use ALPR technology than smaller offices; nearly 90% of sheriffs' offices with 500 or more sworn deputies reported using the technology, and of police departments serving over 1 million residents, 100% used ALPRs.

ALPRs are camera systems that capture the license plate data of passing vehicles, along with related information. They are generally available in fixed and mobile formats. Fixed ALPR systems are mounted in specific locations, often using existing infrastructure such as light poles, traffic lights, buildings, or bridges. Mobile ALPR systems are frequently mounted on police vehicles or privately contracted vehicles. ALPRs automatically capture images or videos of passing vehicles. An algorithm then detects the license plates within the photo/video and reads the numbers. (ALPR technology can also detect additional, related information, including vehicle type and color, global positioning system [GPS] location data, and date and time.) After they capture and catalog license plate information, ALPR systems can compare these data against various databases, including what are known as *hot lists*, which contain license plates linked to vehicles of interest. If there is a match to a hot list license plate, the ALPR system can alert a police officer in real time.

Law enforcement agencies may use ALPRs for a variety of proactive and reactive policing purposes, including gathering intelligence and evidence, helping identify potential suspects, and facilitating crime scene analysis. There does not appear to be publicly available data on the frequency and extent to which ALPR technology is used for various purpose areas, and there are no data on its use at various phases of the criminal justice system—from generating investigative leads and helping establish probable cause for an arrest or indictment to serving as evidence in courtrooms.

Generally, federal law does not direct or prohibit specific tools and technologies—such as ALPRs—used by federal law enforcement agencies to aid investigations. However, there are policies that influence their use. For instance, the U.S. Department of Justice (DOJ) provides *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity*, which specifies what type of information may or may not be used in law enforcement and intelligence activities, even when law enforcement activities involve automated systems or artificial intelligence (AI). As such, while this DOJ guidance isn't specific to use of ALPRs, it broadly applies to law enforcement use of technologies such as ALPRs that may involve AI systems. In addition, the Federal Bureau of Investigation (FBI) maintains a *Criminal Justice Information Services (CJIS) Security Policy*, which provides guidance to all partners who may have access to CJIS information—including license plate data in CJIS.

No specific federal legislative framework exists that governs federal law enforcement use of ALPRs, though there are federal laws and policies broadly governing law enforcement investigations and intelligence gathering. Some observers argue that ALPR use can enhance law enforcement operations—including using them as tools to help locate missing persons or stolen vehicles. Others have raised concerns that law enforcement use of ALPRs could infringe upon individuals' privacy rights if law enforcement agencies' collection and retention of data on vehicle locations are used to track law abiding citizens. Policymakers may debate these tradeoffs as they conduct oversight and deliberate on legislation that may influence federal, state, local, and tribal law enforcement use of ALPR technology.

Contents

Contacts

Over the past couple of decades, law enforcement use of automated license plate readers (ALPRs; also referred to as LPRs) has increased.[1] These tools are now relatively commonplace in policing. According to the Bureau of Justice Statistics' (BJS') 2020 Law Enforcement Management and Administrative Statistics Survey, larger law enforcement offices were more likely to use ALPR technology than smaller offices; nearly 90% of sheriffs' offices with 500 or more sworn deputies reported using the technology, and of police departments serving over 1 million residents, 100% used ALPRs.[2] These readers are one of many tools law enforcement agencies have in their toolkits to help investigate crime. Initially, ALPRs were thought of as a tool to help combat automobile theft, but their use has expanded. Agencies use ALPRs for a variety of purposes, including gathering intelligence and evidence, helping identify or apprehend potential suspects in a range of criminal investigations, locating missing or kidnapped individuals, and facilitating crime scene analysis.[3]

Law enforcement use of ALPRs raises a range of questions for policymakers and the public. For instance, some may examine what policies and procedures agencies have in place to govern ALPR use and how police and policymakers conduct oversight for this technology. Some may also question how ALPR use may simultaneously enhance law enforcement agencies' work and potentially infringe upon individuals' privacy and civil liberties. These considerations have reportedly led to some states passing laws governing the use of ALPRs and the retention of data collected by these tools.[4]

This report focuses on the use of ALPRs specifically for law enforcement purposes. It provides an overview of how they work and federal law enforcement agencies' use of them—with an emphasis on U.S. Department of Justice (DOJ) agencies. The report also presents considerations for policymakers debating whether or how to affect federal, state, local, and tribal law enforcement agencies' use of ALPRs.

ALPRs and How They Work

Automated license plate readers are camera systems that capture the license plate data of passing vehicles, along with related information. They are generally available in fixed and mobile formats. Fixed ALPR systems are mounted in a specific location, often using existing infrastructure such as light poles, traffic lights, buildings, or bridges. Mobile ALPR systems are frequently mounted on police vehicles or can be installed on private vehicles contracted by companies that may share ALPR data with law enforcement.

ALPR systems work by automatically capturing images or videos of passing vehicles. An algorithm then detects the license plates within the photo/video and reads their numbers. ALPR

[1] In the late 1990s, ALPRs were first used by the U.S. Border Patrol, and the technology started to be used more by police departments in the 2000s. See Tom Simonite, "AI License Plate Readers Are Cheaper—So Drive Carefully," *Wired*, January 27, 2020; Keith Gierlack, Shara Williams, and Tom LaTourrette et al., *License Plate Readers for Law Enforcement: Opportunities and Obstacles*, RAND Corporation, 2014; and Cynthia Lum, Christopher S. Koper, and James Willis et al., "The rapid diffusion of license plate readers in US law enforcement agencies," *Policing: An International Journal*, vol. 42, no. 3 (2019). This report uses the acronyms ALPR and LPR interchangeably.

[2] Connor Brooks, *Sheriffs' Offices, Procedures, Policies, and Technology, 2020 – Statistical Tables*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, NCJ307234, November 2023; and Sean E. Goodison, *Local Police Departments, Procedures, Policies, and Technology, 2020 – Statistical Tables*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, NCJ307405, November 2023.

[3] Assistant Police Chief Travis Martinez, *Innovative Uses of Automated License Plate Readers to Enhance Criminal Investigations*, National Police Foundation, National Resource and Technical Assistance Center for Improving Law Enforcement Investigations, June 2019.

[4] National Conference of State Legislatures, *Automated License Plate Readers: State Statutes*, February 3, 2022.

technology can also detect additional, related information, including vehicle type and color, global positioning system (GPS) location data, and date and time. These tools also have the potential to identify individuals in the photos/videos through the use of facial recognition technology (FRT).[5] ALPR systems catalogue and store information, particularly license plate number, GPS data, and date and time. This data retention can help law enforcement track where vehicles have been over time.

After they catalog the license plate information, ALPR systems can compare these data against various databases, including what are known as *hot lists*, which contain a list of license plates linked to vehicles of interest. If there is a match to a hot list license plate, the ALPR system can alert a law enforcement officer in real time.[6]

As law enforcement use of ALPRs has become more commonplace, some observers have noted that one factor contributing to this expansion is that the price to use this technology has dropped substantially. And, while acquiring a new ALPR camera system can be costly, evolving technology now allows ALPR software to be used on existing security camera systems—including police vehicle dashboard cameras—for a fraction of the price of acquiring a new ALPR camera system.[7] For example, some estimates put the cost of a new ALPR device at $15,000-$20,000, while software installed on existing cameras to read license plates can reportedly cost as little as $50 per camera.[8]

How LPRs May Be Used by Law Enforcement Agencies

Law enforcement agencies—including federal law enforcement—may use LPRs for a variety of proactive and reactive policing purposes. The International Association of Chiefs of Police (IACP) has identified four broad categories of LPR uses.[9]

- **Community caretaking**. LPRs may help locate missing individuals, including those who may be kidnapped or otherwise endangered. They may also be used to provide additional context to suspicious or unexplained situations to help determine whether a crime has been committed.
- **Investigations**. In the course of investigations, LPRs can be used to collect evidence, including evidence that helps identify or apprehend suspects or locate and recover stolen vehicles. Police can also analyze stored LPR data to help identify patterns of suspicious or criminal activity.
- **Crime prevention**. While it may be difficult to measure when something doesn't happen (i.e., when a crime is prevented), some have noted that the presence of LPRs may deter individuals from engaging in unlawful activity. LPRs may also help provide investigative leads so police can intervene in suspicious situations before criminal or harmful activity occurs.

[5] For information on law enforcement use of facial recognition technology, see CRS Report R46586, *Federal Law Enforcement Use of Facial Recognition Technology*.

[6] Axon Enterprise, Inc., *Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers*, October 2019. There are both local and national hot lists. The national list is maintained by the Federal Bureau of Investigation and is discussed elsewhere in this report.

[7] Tom Simonite, "AI License Plate Readers Are Cheaper—So Drive Carefully," *Wired*, January 27, 2020.

[8] Ibid.

[9] International Association of Chiefs of Police, *License Plate Reader (LPR) Systems: Use Cases*, 2024.

- **Traffic compliance**. LPRs may be used in cities' traffic systems that automate toll payment as well as citations or fines for traffic violations and infractions. Some have suggested that the presence of LPRs may help deter certain risky driving behaviors like speeding or violating traffic signals.

U.S. Department of Justice Use of LPRs

LPRs are used by a range of federal law enforcement agencies and their partners. This section highlights law enforcement entities within DOJ that use LPR technology or data, including data collected by their partners. While some information is available on agencies' use of the technology, there do not appear to be publicly available agency documents with comprehensive details on its use. This is not a phenomenon unique to LPRs. Agencies do not necessarily provide public documentation detailing use data for each of the tools they may employ in investigations. This may help protect sensitive law enforcement information and case details. As illustrated in the examples below, while agencies may use LPR technology themselves, they may also rely on LPR data that were collected by other law enforcement and partner entities.

- Federal Bureau of Investigation (FBI). FBI press releases indicate that the bureau and its investigative partners have used LPR technology for purposes including to help identify potential suspects in criminal investigations.[10] The FBI also runs an LPR Program—detailed below—that shares LPR information with law enforcement partners.
- Drug Enforcement Administration (DEA). The DEA administers a National License Plate Reader Program, to facilitate investigations related to drug trafficking criminal networks. The DEA notes that this program involves a "network of LPR equipment owned by DEA, other federal agencies, and state, local, and tribal police departments. All law enforcement agencies involved have Memorandums of Understanding with DEA detailing the parameters for use and sharing of the LPR information."[11]
- Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). ATF press releases indicate that the ATF and its investigative partners have relied on LPR technology for facilitating investigations, including to gather information on the location of suspects' vehicles.[12]
- U.S. Marshals Service. The USMS has relied on partners' use of LPRs to help locate wanted persons.[13]

DOJ does not appear to publish publicly available data on the frequency and extent to which LPR technology is used for each of the purpose areas described above. Similarly, there are no data on its use at various phases of the criminal justice system—from generating investigative leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms.

[10] See, for instance, DOJ, "License Plate Reader Helped Identify Robbery Suspect," press release, October 17, 2018; and FBI, "Alleged Armed Robber of Three Manhattan Banks Arrested and Charged in Manhattan Federal Court," press release, July 14, 2015.

[11] DEA, *Privacy Impact Assessment for the National License Plate Reader Program (NLPRP)*, April 19, 2019, p. 2.

[12] See, for instance, DOJ, "Pittsburgh Felon Charged with Possession of a Destructive Device after Throwing a Homemade Explosive from a Moving Vehicle in Pittsburgh's Lawrenceville Neighborhood," press release, January 6, 2021.

[13] Mt. Juliet Police Department, "An Escapee, Wanted by the U.S. Marshals, was Apprehended After Attempted Traffic Stop, License Plate Reader Alerts, and K9 Track," press release, December 20, 2023.

FBI's LPR Program

The FBI runs a License Plate Reader program to facilitate LPR information sharing with and between its law enforcement partners.[14] Specifically, through the National Crime Information Center (NCIC), the FBI maintains a hot list of vehicle data against which law enforcement agencies can compare their LPR data. The NCIC is operated by the FBI's Criminal Justice Information Services Division (CJIS) and serves as a clearinghouse of "records contributed by and accessible to criminal justice agencies nationwide. Its purpose is to enhance officer and public safety, and it has been called the lifeline of law enforcement."[15] The NCIC has 22 broad files, collectively containing over 18 million records. There are 15 persons files and 7 property files. The FBI notes that persons files generally may contain a range of information about individuals, including their associated license plate numbers.[16] Similarly, property files generally may contain a range of information about property, including vehicles and associated license plate numbers.

One of the property files in NCIC is the License Plate File. The FBI notes that:

> The License Plate File contains records of stolen license plates. Information in the License Plate File includes the license plate number, the state in which the license plate was issued, the year the license plate was issued, and the type of license plate (e.g., passenger automobile, motorcycle, trailer, truck, aircraft, antique automobile, bus, commercial vehicle, dune buggy, farm vehicle). Only law enforcement/criminal justice agencies can enter records into the License Plate File.[17]

Similarly, another relevant property file in NCIC is the Vehicle File. The FBI notes that:

> The Vehicle File contains records of stolen vehicles, vehicles used in the commission of a felony, or vehicles that a law enforcement agency seizes based upon a federally issued court order. Information in the Vehicle File includes the vehicle identification number, vehicle make, vehicle model, vehicle style, vehicle color, vehicle year, owner applied number (if applicable), and license plate number. Only law enforcement/criminal justice agencies can enter records into the Vehicle File.

Authorized criminal justice users may query NCIC with LPR data for authorized purposes, which range from solving crimes, apprehending fugitives, and combating terrorism to locating missing persons and stolen property and enhancing law enforcement officer safety. The NCIC supplies license plate data to authorized criminal justice users for use with LPRs. It extracts these data from various persons and property files; these data are refreshed twice daily and pushed out to authorized law enforcement agencies.[18] LPR systems allow law enforcement users to import data directly from NCIC to establish a hot list.[19] If officers query NCIC data with a license plate

[14] This program was approved by the FBI's Criminal Justice Information Services Advisory Policy Board in 2004. FBI, *License Plate Reader Technology Enhances the Identification, Recovery of Stolen Vehicles*, November 1, 2011.

[15] For more information, see FBI, *National Crime Information Center (NCIC)*, https://le.fbi.gov/informational-tools/ncic. The FBI notes that authorized users may only access data in NCIC for specified purposes, which are "apprehending fugitives, solving crimes, combating acts of terrorism, locating missing persons, locating and returning stolen property, protecting individuals during declared emergency situations, protecting victims of domestic violence, monitoring registered sex offenders, performing background checks for firearms, explosives, and weapon-related permits, and enhancing the safety of law enforcement officers"; FBI, *Privacy Impact Assessment for the National Crime Information Center*, November 7, 2022, p. 17.

[16] FBI, *Privacy Impact Assessment for the National Crime Information Center*, November 7, 2022.

[17] Ibid., p. 7.

[18] FBI, *License Plate Reader Technology Enhances the Identification, Recovery of Stolen Vehicles*, November 1, 2011.

[19] According to the Major Cities Chiefs Association, this is the most common method of creating hot lists. Major Cities (continued...)

number and receive a positive match to their hot list or a record in the system, this match alone is not sufficient for an officer to establish probable cause and make an arrest; they must first confirm the information is accurate and up to date.[20]

ALPR Law and Policy Guidance for Law Enforcement

Generally, federal law does not direct or prohibit specific tools and technologies—such as ALPRs—used by law enforcement agencies to aid investigations. However, there are policies that influence their use.

While DOJ does not appear to have a publicly available policy specifically guiding federal law enforcement use of ALPRs,[21] other DOJ policies affect its use by federal law enforcement agencies. For instance, DOJ's *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* specifies that "federal law enforcement personnel may not consider race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or disability in law enforcement or intelligence activities" with the exception of instances where specific details provide assurance that the information is reliable and linked to a specific "criminal incident, scheme, or organization; a threat to national or homeland security; a violation of Federal immigration or customs law; or an authorized intelligence activity" and that the law enforcement activity is merited given the totality of circumstances.[22] These standards apply even when law enforcement activities involve automated systems or artificial intelligence (AI). These automated systems can capture images of individuals—images that may contain information on an individual's race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or disability. As such, while this DOJ guidance isn't specific to law enforcement use of ALPRs, it broadly applies to law enforcement use of technologies such as ALPRs that may involve AI systems, as ALPRs collect photos that may include, among other things, images of individuals in vehicles. For instance, law enforcement may not use photos captured by an ALPR and decide to take action against an individual based on the race of the driver, unless a situation meets the specified exceptions.

There is also federal guidance that applies broadly to the security of criminal justice information (CJI), including license plate data. For instance, the FBI maintains a *Criminal Justice Information Services (CJIS) Security Policy*, which provides guidance to all partners who may have access to CJIS information, including license plate data in CJIS. While this does not direct policies about the operations of partners' LPR programs, it guides "the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI" held in CJIS, which would include LPR data.[23]

Chiefs Association, *Automated License Plate Reader Technology in Law Enforcement: Recommendations and Considerations*, 2023, https://majorcitieschiefs.com/wp-content/uploads/2023/02/MCCA-Automated-License-Plate-Reader-Technology-in-Law-Enforcement.pdf.

[20] FBI, *Privacy Impact Assessment for the National Crime Information Center*, November 7, 2022.

[21] The American Civil Liberties Union (ACLU) obtained documents indicating DOJ may have an LPR policy, but if one has been developed, CRS has not been able to obtain a copy. See Bennett Stein, ACLU, *Internal Documents Show FBI Was 'Wrestling' With License Plate Scanner Privacy Issues*, May 15, 2015.

[22] DOJ, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity*, May 2023.

[23] FBI, *Criminal Justice Information Services (CJIS) Security Policy: Version 5.9.4*, December 20, 2023, p. i.

Additionally, there has been LPR-related research and guidance from DOJ agencies directed toward law enforcement at various levels of the criminal justice system. For example, DOJ's Bureau of Justice Assistance (BJA), in collaboration with the U.S. Department of Homeland Security (DHS), supported the development of a *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*. This guidance notes that while law enforcement and related justice entities are increasingly using LPR technology, "individual privacy, civil rights, and civil liberties must also be vigorously protected."[24] It suggests that developing an LPR policy should be one of many steps taken in establishing an LPR program, and notes that the program should include the following:

- educating and raising awareness on the importance of privacy, civil rights, and civil liberties protections;
- assessing agency privacy, civil rights, and civil liberties risks by evaluating the process of collecting, receiving, accessing, using, disseminating, retaining, and purging LPR information;
- developing an LPR policy on how the agency handles LPR information;
- evaluating whether the LPR policy will address current law, standards, and privacy protection recommendations;
- implementing the LPR policy and training LPR users on the rules and procedures;
- reviewing and updating the LPR policy in response to factors including experience, oversight, law, technology, and public expectations; and
- auditing the processes outlined in the LPR policy.[25]

Policy Considerations Concerning Law Enforcement Use of ALPRs

No specific federal legislative framework exists that governs federal law enforcement use of ALPRs; rather, there are federal laws and policies broadly governing law enforcement investigations and intelligence gathering. Some states have ALPR-specific laws, contributing to a patchwork of laws and polices across the country.[26] Some observers argue that ALPR use can enhance law enforcement operations—including using them as tools to help locate missing persons or stolen vehicles. Others have raised concerns that law enforcement use of ALPRs could infringe upon individuals' privacy rights if, for example, law enforcement agencies' collection and retention of data on vehicle locations are used to track law abiding citizens. Policymakers may debate these tradeoffs as they conduct oversight and deliberate on legislation that may influence federal, state, local, and tribal law enforcement use of ALPR technology.

Oversight of LPR Use

If Congress debates law enforcement use of specific technologies such as LPRs, it may consider how any boundaries might apply. For example, while many tools and technologies used by law

[24] DOJ/BJA and DHS, *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*, February 2017.

[25] Ibid.

[26] National Conference of State Legislatures, *Automated License Plate Readers: State Statutes*, February 3, 2022, https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes.

enforcement agencies to aid investigations have not been specifically permitted or prohibited by law, Congress has legislated on and conducted oversight of certain technologies that could affect individual privacy. With electronic surveillance, for instance, investigators must generally obtain a warrant to conduct wiretaps;[27] however, exceptions exist for emergency situations that may involve death or serious injury, threaten national security, or involve conspiracies of organized crime.[28]

Policymakers may also examine whether federal law enforcement agencies have developed and maintained an LPR program—including an LPR policy—as recommended in the joint DOJ/DHS *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities.* Congress may consider these issues as they conduct oversight of federal law enforcement use of LPRs. They may do this through a variety of mechanisms, including hearings and directives to oversight entities such as the Government Accountability Office (GAO) or various department Inspectors General.

Influencing Law Enforcement use of LPRs

Policymakers can legislate directly on federal law enforcement agencies' ability to utilize certain technologies such as LPRs, as well as specify under which circumstances federal law enforcement may use these tools. They can also direct federal departments and agencies to develop or rely on established guidelines surrounding the technologies, require them to use technology that meets specified standards, and conduct broad oversight of federal law enforcement agencies' use of technology such as LPRs.

Congress can also influence state, local, and tribal law enforcement agencies' use of LPRs through the provision or withholding of grant funding. Programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program[29] and the Community Oriented Policing Services (COPS) program[30] are regularly used to incentivize certain activities by state and local law enforcement and could similarly be leveraged to support or restrict agencies' use of LPRs. Indeed, both JAG and COPS funds have been used to support law enforcement agencies' LPR programs around the country.[31] If policymakers wanted to provide additional guidance on the use of grant funds, Congress could further specify when, and under what circumstances, grant programs may be used to support law enforcement use of LPRs. And, federal grant administering agencies can require that grantees adhere to certain requirements with respect to LPR use. For instance, DHS requires all fusion centers that are supported under the Homeland Security Grant Program and use LPR data or tools for investigative, analytic, or intelligence purposes to "maintain an approved LPR policy" that adheres to the joint DOJ/DHS *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*.[32] Policymakers

[27] 18 U.S.C. §§2510, et seq. See also DOJ, Justice Manual, Title 9, 9.7000: Electronic Surveillance.

[28] 18 U.S.C. §2518.

[29] For more information, see CRS In Focus IF10691, *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program*.

[30] For more information, see CRS In Focus IF10922, *Community Oriented Policing Services (COPS) Program*.

[31] DOJ, BJA, *Expansion of Flock Automated License Plate Reader (ALPR) Safety Camera Program*, https://bja.ojp.gov/funding/awards/15pbja-23-gg-03112-jagx; DOJ, Office of Community Oriented Policing Services, *FY24 COPS Technology and Equipment Program Invitational Solicitation*, https://cops.usdoj.gov/pdf/2024ProgramDocs/tep/solicitation.pdf.

[32] For more information, see DHS, *Homeland Security Grant Program*, https://www.dhs.gov/homeland-security-grant-program-hsgp; see also DOJ/BJA and DHS, *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*, February 2017.

may examine whether a similar requirement regarding LPR policies may be appropriate for other federal grantees.

LPR Technology and Police-Community Relations

In the current discourse about police-community relations,[33] there have been questions about whether law enforcement use of LPRs could contribute to tensions between the police and the communities they serve. The joint DOJ/DHS *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities* notes that "a comprehensive LPR policy that is developed in a transparent manner and properly enforced fosters trust—not only within and between justice partners but also by the public, whose LPR information may be collected and utilized."[34] Some local police complaint review boards have also recommended enhanced transparency of information on law enforcement use of LPRs. For instance, in Washington, DC, the Police Complaints Board released a report on LPRs recommending, among other things, that the Metropolitan Police Department be transparent with the public about data collected with LPRs to help improve community relations and enhance public trust.[35] Policymakers could opt to examine not only the availability and transparency of federal law enforcement LPR policies but also those of state, local, and tribal law enforcement who may be recipients of federal grant funding.

LPR Accuracy and Data Security

The accuracy of LPR technology has come under scrutiny, particularly instances wherein individuals have claimed that LPRs—particularly the algorithms that detect license plates within the photo/video and read the numbers from the license plates—have made errors resulting in the wrong vehicle/individual coming under scrutiny of law enforcement. Some observers have noted that while the accuracy of LPR technology has been improving, as of 2019 at least one estimate had put the accuracy of LPRs at around 90%.[36] And, this less than perfect accuracy has led some to question possible implications of law enforcement taking actions based on imperfect technology. For instance, there is a concern that innocent individuals may become, even temporarily, the subject of law enforcement attention or investigation if their license plate matches what is an incorrect or incomplete read by an LPR system.

The security of data collected and held by federal agencies and their contractors—through a variety of technologies, including LPRs—is of ongoing interest to Congress. For instance, in June 2019 U.S. Customs and Border Protection (CBP) revealed that images of faces and license plates were compromised in a cyberattack on one of its subcontractors that provides LPR technology to the agency.[37] This breach reportedly exposed confidential agreements, hardware schematics, and other records related to border security.[38] Breaches like this highlight the vulnerability of data,

[33] For more information, see CRS Report R43904, *Public Trust and Law Enforcement—A Discussion for Policymakers*.

[34] DOJ/BJA and DHS, *License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*, February 2017, p. 2.

[35] District of Columbia, Office of Police Complaints, *Police Complaints Board Releases Report on Automated License Plate Readers*, September 25, 2020.

[36] Justin Klawans, "The pros and cons of license-plate reader technology," *The Week*, December 17, 2023. This estimate is just that: an estimate provided by an observer, rather than the result of a formal scientific study.

[37] For more information, see CRS Insight IN11143, *Exposed Data Highlights Law Enforcement Use of Selected Technologies*.

[38] Drew Harwell, "Surveillance Contractor That Violated Rules by Copying Traveler Images, License Plates Can Continue to Work with CBP," *Washington Post*, October 10, 2019.

including LPR data captured and held by governmental agencies. In evaluating the security of federal law enforcement data systems, policymakers may pay particular attention to the security of LPR data and other criminal justice information.

Federal law enforcement agencies are required to provide information to the public on their data collection systems through Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).[39] Policymakers could question whether these are sufficient measures to notify the public about federal law enforcement agencies use of LPRs to search against databases in which individuals' personal data are held. In addition, they could opt to conduct oversight over the timeliness with which federal law enforcement agencies publish and update relevant PIAs and SORNs.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer

[39] This requirement is not specific to federal law enforcement. Federal agencies are subject to requirements under Section 208 of the E-Government Act of 2002 (P.L. 107-347) regarding the protection of personal information collected, maintained, or disseminated using information technology. For more information, see Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22, September 26, 2003. In this guidance, a *PIA* is defined as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." In addition, SORNs are required to be published for any newly created or revised system of records.