Artificial Intelligence and Law Enforcement: The Federal and State Landscape

By Nicole Ezeh, Amber Widgery and Chelsea Canada

INTRODUCTION

Technology and policing are closely intertwined; think speed detection radar technology and surveillance drones. Law enforcement officials use technology to better detect, investigate and solve crime. Simultaneously, concerns exist about efficacy and appropriate use. Artificial Intelligence is no exception.

Law enforcement agencies across the country are increasingly encountering and adopting technology equipped with AI. While officers investigate crimes that use AI, they also recognize that incorporating AI can increase efficiency and expand capabilities. AI governance is still in its infancy and law enforcement as well as state and federal policymakers are tasked with balancing the benefits of using AI with constitutional concerns.

As AI rapidly develops, policy aimed at promoting responsible use and education for law enforcement agencies will evolve. This issue brief provides examples of how federal, state and local law enforcement are incorporating AI into their work and reviews state and federal actions impacting the adoption.

AI USE BY LAW ENFORCEMENT

Law enforcement agencies use AI in three ways: to assist humans with tasks and increase capacity, expand human capabilities and, in some limited instances, replace humans entirely with fully automated processes.

While not a complete listing of technology or uses, the following exemplifies the myriad ways law enforcement and AI intersect.

MACHINE LEARNING

Machine learning trains algorithms to improve performance on tasks using data analysis. Law enforcement agencies generally possess a tremendous amount of data, such as information on arrests, location of crime, type of charges and clearance rates. Machine learning can be used to help predict where criminal activity is likely to happen and tailor decisions on staffing and type of response. This works by summarizing and communicating large data sets, enabling law enforcement agencies to make informed decisions on the use of limited resources and share trends with the community when appropriate.

COMPUTER VISION

Computer vision, a subset of machine learning, teaches computers to interpret and understand visual information from images or videos. Facial recognition is one of the most well-established uses, but it is also used for fingerprint matching, DNA analysis and ear biometrics.

Additionally, cameras enabled with computer vision can be used to look for specific objects and assist in enforcement of traffic laws. For example, security cameras can detect specific people, suspicious behavior and weapons. Traffic cameras can identify a stolen vehicle or enforce speed, red light and seat belt laws, acting as a force multiplier for law enforcement agencies.

Concerns with the use of this type of AI technology center around the issue of bias, such as difficulty detecting and distinguishing features of individuals with darker skin. There are AI redaction strategies that can reduce bias by removing characteristics of race and ethnic origin that may influence criminal charges.

NATURAL LANGUAGE PROCESSING

Natural language processing is another subset of machine learning that enables machines to understand, interpret and generate human language to, for example, enhance report writing. Reports need to be detailed and accurate, but they also take time. Some agencies have adopted technology that can write initial drafts of police reports based on body camera footage and real-time officer narration. Reports are then reviewed for accuracy and supplemented by officers.

Natural language processing is also used to review body camera footage to flag highly professional responses for purposes of recognition or identify problematic interactions for supervisor intervention.

AUTONOMOUS ROBOTICS

Autonomous robots are machines that can perform physical tasks in the real world. For example, drones are used for traffic collision reconstruction, arson investigations and investigations of other accidents such as train derailments and crane collapses. Some agencies are also experimenting with drones as a first response to calls for service, especially in situations where personnel safety would be at risk, such as armed suspects, car chases, hostage situations, bomb threats and missing persons searches on difficult terrain.

PROCESS AUTOMATION

Process automation is designed to assist with specific tasks and can be achieved using different types of AI. One of the ways this has been adopted is computer-aided dispatch which can help to triage calls and improve response times. Calls can also be analyzed in real time and can help with translation when callers speak other languages. Process automation uses machine learning algorithms by using neural networks and deep learning techniques to perform specific functions. It has also been used for court reminder systems that help to reduce failure to appear in court and subsequent warrants and arrests.

THE POLICY LANDSCAPE

Federal state and local governments can exercise oversight over policing, including adoption of AI technology. This is in addition to internal governance by law enforcement agencies themselves.

There are nearly 18,000 state and local law enforcement agencies across the country. The vast majority are categorized as local. Most police departments are led by a chief and report to a city mayor or a designated entity, like a police

commission. Sheriffs, conversely, are generally elected at the county level and are accountable to voters with some budgetary oversight by county officials.

A state-level police agency exists in every state ranging in size from North Dakota's 139 officers to California's 7,202 officers. Legislatures provide annual funding for state police agencies such as highway patrols and bureaus of investigation.

At the federal level, there are 90 agencies that employ 136,815 full-time officers. While federal agencies sometimes differ greatly in scope and function from state and local agencies, the primary function of more than two-thirds of federal officers is criminal investigation.

As law enforcement agencies move to adopt AI, lawmakers at all levels of government have considered policies that balance the benefits of AI in policing with potential risks. No state or locality has adopted a comprehensive set of laws governing law enforcement use of AI. In states that have legislated, the approach has been either to limit the adoption of AI or address how very specific applications of the technology can be used.

STATE LEGISLATIVE ACTIONS

State legislators in at least 30 states considered over 150 bills relating to government use of AI in 2024. Legislation addressed inventories to track the use of AI across state government, impact assessments, creating AI use guidelines, procurement standards and government oversight bodies. Some of these bills apply to government agencies broadly and may impact technologies used by state and local law enforcement agencies. As state legislatures continue to focus on AI regulation, states are also introducing legislation regulating the specific use of technology by law enforcement that have AI capabilities.

FACIAL RECOGNITION TECHNOLOGY

Over the last five years, at least 18 states have considered legislation to regulate law enforcement's use of facial recognition technology. In 2020, Washington was one of the first states to enact more comprehensive legislation regulating how state agencies and law enforcement use AI.

Washington's 2020 S 6280 and Colorado's 2022 S 113 require an accountability report, data management, security protocols, training procedures and testing, for government entities to use facial recognition technology. Additionally, entities must obtain a warrant or court order to use the technology to conduct ongoing surveillance, real-time identification or tracking. Utah enacted a law that prohibits government entities from using facial recognition on an image database except for law enforcement agencies. Agencies must submit a request and adhere to notice, data protection and disclosure requirements.

Some states have opted to temporarily or otherwise limit law enforcement use of FRT. In 2019, California enacted a three-year moratorium on use of facial recognition in body cameras. Oregon prohibits the use of facial recognition software captured by body cameras worn by law enforcement and New Hampshire limits use without proper authorization. Illinois enacted a law that prohibits law enforcement from using drones equipped with facial recognition, while Vermont's 2021 legislation prohibits the use of facial recognition, except in cases involving sexual exploitation of children. Maine passed a law the same year prohibiting the search of "facial surveillance systems," with exceptions for serious crimes.

States have made clear that law enforcement cannot rely on facial recognition results as the single investigatory tool. Alabama now prohibits state and local agencies from using facial recognition as the sole basis for making an arrest or for establishing probable cause in a criminal investigation. Maryland authorized agencies to utilize facial recognition to

establish probable cause or positive identification of an individual only if the results are supported by additional, independently obtainable evidence.

Other states convened study groups to provide recommendations for the use of facial recognition. Kentucky's 2022 legislation tasked a working group with creating a model policy for use by law enforcement agencies. That same year, Colorado created the Facial Recognition Task Force to investigate its use by state and local government agencies.

DRONE TECHNOLOGY

Drone capabilities are advancing as AI is incorporated into the technology. At least 15 states have passed laws that require law enforcement to obtain warrants before using drones. State legislatures continue to focus on the use of drones by law enforcement, and drone laws have been enacted in recent years.

In 2021, Florida expanded the authorized purposes for law enforcement drone use to include collecting evidence at crime scenes, assessment of damage during an emergency and vegetation or wildlife management. That same year Tennessee passed a law allowing officers to use drones for evidence collection; it was made permanent in 2023.

Illinois recently expanded its drone law to allow use by law enforcement at special events, to locate victims in an emergency and to conduct infrastructure inspection when requested by a local government. Utah now allows law enforcement to use drones in places that are off limits to others, like above certain critical infrastructure facilities.

States are addressing the potential cybersecurity risks associated with drones used by law enforcement. Tennessee passed a law that prohibits state agencies from purchasing equipment that meets criteria for posing cybersecurity risks. In 2021, Florida passed a law that requires drones purchased by law enforcement to be from an approved manufacturers' list. Drones not from an approved manufacturer must be disconnected two years later. In 2024, Florida appropriated $25 million for drone replacement grants. Through this program, law enforcement agencies are required to provide the Florida Center for Cybersecurity within the University of South Florida the retired drones to analyze potential cybersecurity threats.

AUTOMATED LICENSE PLATE READERS

At least 18 states enacted laws addressing the use of automated license plate readers or the retention of data collected by the automated readers. The devices capture computer-readable images that allow law enforcement to compare plate numbers against plates of stolen cars or cars driven by individuals suspected of criminal activity. They are mounted on police cars, road signs and traffic lights and capture thousands of plate images.

Data collected from the devices can enhance law enforcement's ability to investigate and enforce the law but also raises concerns about inaccurate information placed into databases and shared without restrictions on use, retained longer than necessary and used or abused in ways that could infringe on individuals' privacy.

Under Kansas law, a public agency is not required to disclose records that contain captured license plate data or the location of a license plate reader. Georgia law limits use of them to law enforcement purposes and required data to be destroyed no later than 30 months after it was collected, with limited exceptions. The law also mandates each agency maintain current policies regulating the use and train officers on appropriate use of the technology.

FEDERAL ACTIONS

CONGRESSIONAL ACTION

Congress and the Biden administration both contemplated the role of artificial intelligence technology in federal law enforcement crime response and investigation. Though the 118th Congress did not consider many bills on AI and policing, the Biden administration put out several policies and reports, including an executive order from the president. It remains to be seen whether the Trump administration will continue the efforts of the previous administration or pursue new approaches to artificial intelligence and law enforcement.

LEGISLATION INTRODUCED IN THE 118TH CONGRESS

HR 8005: Child Exploitation and Artificial Intelligence Expert Commission Act of 2024. This bill establishes the Commission of Experts on Child Exploitation and AI to investigate and make recommendations to improve law enforcement's ability to detect, prevent, and prosecute AI-enabled child exploitation crimes. This was a bipartisan effort, with 15 Democrats and nine Republicans cosponsoring the bill.

HR 6143: American Security Drone Act of 2023. This bill was passed through the National Defense Authorization Act for Fiscal Year 2024. It prohibits federal agencies from using drones manufactured in certain foreign countries to protect national security interests and foster U.S. manufacturing of drone technology.

OTHER CONGRESSIONAL ACTIONS AND REPORTS

The Government Accountability Office testified before Congress and released a report on federal law enforcement use of facial recognition technology. According to the report, seven federal agencies use the technology, including the Customs and Border Protection, Federal Bureau of Investigation, Secret Service, Bureau of Alcohol, Tobacco, Firearms, and Explosives, Drug Enforcement Agency, Homeland Security Investigations, and the U.S. Marshalls Service.

BIDEN ADMINISTRATIVE ACTIONS

The Biden administration released a plethora of agency reports beginning with President Joe Biden's Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence in October 2023. The executive order directed federal agencies to produce reports and analyses on the use of AI by the federal government. In the law enforcement field, the order directed the Departments of Justice and Homeland Security to report the use of AI in the criminal justice system, consider how they can use their authorities to prevent algorithmic- and AI-related discrimination, and develop AI use recommendations for state and local law enforcement agencies.

The administration released several other reports and recommendations on law enforcement's use of artificial intelligence. In October 2024, the White House released a fact sheet outlining AI use restrictions and risk management practices in law enforcement necessary to safeguard national security. It also released a memorandum supporting the use of AI in a manner that fosters safety, security, and trustworthiness. Both documents emphasized the importance of protecting the constitutional rights of the public as well as those suspected of criminal activity. The memorandum highlighted the importance of not introducing biases based on protected characteristics and actions, such as race, ethnicity or participation in political speech.

AGENCY REPORTS AND GUIDELINES

In December 2024, the Department of Justice released its final report in response to Executive Order 14110. The report discusses AI use in cases such as identification and surveillance, forensic analysis, predictive policing and risk assessment. The report includes best practices and measures to be taken before and after deploying AI technology. The report

recommends that any criminal justice agency interested in using AI and creating an AI governance program should first identify the problem they wish to address and the reasons why the use of AI is preferable to non-AI alternatives. It highlights the importance of clear organizational structures for oversight, training and retaining a workforce with adequate resources to enact and enforce policies, and mitigating risks, among other recommendations.

In March 2024, the Department of Homeland Security released its Artificial Intelligence Roadmap, which outlines the agency's AI initiatives and the potential these initiatives have on homeland security as an enterprise. The document details the agency's approaches to AI use, such as ensuring all AI use cases meet due process requirements for legal proceedings, using AI to advance equity instead of amplifying existing societal inequities and taking a whole-of-government, collaborative approach with responsible use as a guiding light. The report identifies opportunities for collaboration with and engagement from the private sector. The DHS maintains an AI use case library on its website.

TRUMP ADMINISTRATIVE ACTIONS

President Donald Trump issued many executive orders in the first week of his presidency. As of the publishing of this brief, two of these orders were related to artificial intelligence.

The first, EO 14148: Initial Rescissions of Harmful Executive Orders and Actions, rescinds Biden's EO 14110, which ordered the creation of the agencies reports outlined above. The second, Removing Barriers to American Leadership in Artificial Intelligence sets the Trump administration's AI policy moving forward. The order states "It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." It also directs agency heads to review the reports, policies, and actions created pursuant to the revoked EO 14110 to make sure they are in line with the Trump administration's new policy. This leaves room for at least some of the work done under the Biden executive order to stay in place.

CONCLUSION

As AI technology continues to advance, government policies at all levels will likely evolve. Ongoing research into the effectiveness of AI applications in policing may have a part in shaping these policies. Research can also help develop better training programs to maximize the benefits of AI in law enforcement while minimizing the risks of misuse, bias and inaccuracies. Discussions about privacy, transparency and legal implications will likely remain central to an evolving landscape. Coordinated efforts across all levels of government may aid in the integration of AI-enabled technology in law enforcement that ensures responsible and effective use.

Nicole Ezeh is an associate legislative director in NCSL's State-Federal Relations Division

Amber Widgery is a program principal for the Civil and Criminal Justice Program

Chelsea Canada is a program principal in NCSL's Financial Services, Technology and Communications Program