RIGHT ON CRIME

EMERGING TECHNOLOGIES IN LAW ENFORCEMENT

WRITTEN BY
Christian Cochran
August 2025

TABLE OF CONTENTS

EMERGING TECHNOLOGIES IN LAW ENFORCEMENT

WRITTEN BY **Christian Cochran**

KEY POINTS

- **Emerging technology's** rapid proliferation in law enforcement comes with the promise of reducing crime through proactive measures and providing more efficient opportunities to solve crimes faster while reducing costs for agencies.
- **There are ethical, legal, and privacy** concerns with usage of AI in law enforcement which need to be explored through policymaking and oversight.
- **Case usage shows** positive and negative aspects for various applications of emerging technology for criminal justice.
- **The benefits of usage** seemingly outweigh the negatives. However, there remain areas where nationwide policy and regulatory changes can occur.
- **Emerging technology** brings forth optimism and hopes it will provide incredible benefits to law enforcement and communities. However, emerging technology must come with guardrails of transparency and oversight to ensure its implementation.

EXECUTIVE SUMMARY

Emerging technologies, especially artificial intelligence (AI), are rapidly transforming law enforcement operations. These advancements offer numerous benefits, such as enhanced efficiency, improved public safety, and cost-saving measures for agencies. AI technologies, like predictive policing and facial recognition, hold promises for reducing crime rates and improving investigative efficiency. Yet, significant ethical dilemmas and privacy issues arise from their use, in turn necessitating careful policymaking and oversight. Various case studies illustrate both positive and negative outcomes of AI applications in law enforcement, emphasizing the need for transparency and community involvement.

To manage the use of these emerging technologies effectively, state legislatures should explore policy changes and regulatory frameworks. Recommendations include promoting transparency, ensuring oversight, and establishing acceptable use standards. Involving community stakeholders in discussions about AI deployment is also advocated to build trust and accountability between law enforcement and the public. Challenges posed by AI technologies include balancing innovation with presumed privacy. Important United States Supreme Court cases shape the legal landscape regarding privacy expectations and technology use by law enforcement. Additionally, concerns about how the increasing volume of data collected by AI systems is used and protected lead to calls for stricter data privacy laws.

While AI offers significant opportunities for improving law enforcement practices, it is crucial to address the accompanying ethical, legal, and privacy challenges. A balanced approach that promotes innovation while safeguarding citizens' rights and fostering public trust in law enforcement practices is essential to ensuring the right-sized proper implementation of the technology.

KEY POINTS

1. AI in action: How AI technology, like machine learning and facial recognition, are being used by the police to do things like predict where crimes might happen.

2. Privacy and ethics: Highlights the prominent privacy and ethical concerns that come with using AI in law enforcement, thus stressing the need for transparency and getting the community involved to build trust.

3. Need for state-centric laws: New state laws are needed to ensure AI is used responsibly in law enforcement. These new laws should seek to protect people's rights while still allowing for technological advancements and usage for public safety.

INTRODUCTION

Over the last several years, communities have seen a rapid rise in technology usage by law enforcement. Artificial intelligence presents the next generation of advancement in law enforcement, with AI generated report writing, facial recognition technology, and public safety devices that protect schools through weapons detection and acoustic gunshot detection devices. The use of artificial intelligence and emerging technology in law enforcement offers a force multiplier to augment existing resources. As the nation moves forward, lawmakers and other stakeholders must consider ways in which technology can provide invaluable solutions while simultaneously balancing the concerns of ethical, legal, and societal impacts in the use of technology.

Artificial intelligence has seen rapid growth in commercial availability and public use, but misconceptions about its capabilities and how to define artificial intelligence persist.

> AI refers to technologies dating as far back as a 1952 "bot" that was programmed to play checkers, and as commonplace as the algorithmically curated content that one sees in a social media feed. Thus, we come to understand that the term "AI" does not necessarily describe particular applications or tools, but an entire field of advanced computational technology. (Whiting & Dunmoyer, 2024, p. 7)

The use of artificial intelligence in law enforcement carries the goals of increasing efficiency, positively impacting public safety, and providing cost-saving measures for the taxpayers. The incentives for law enforcement agencies' adoption of these technologies are well understood as the promise of technology brings forward offers incredible assistance, especially for resource limited agencies. However, certain questions must be asked:

1. What is the balance between privacy and public safety with emerging technologies?

2. How do we begin to regulate a fast-moving technology with almost limitless potential and right-size its role in the pursuit of justice?

3. What are the long-term societal impacts of using this technology in terms of seeking justice?

This paper explores the growing integration of AI and emerging technologies within law enforcement, along with the opportunities and challenges they present. Furthermore, this paper examines the current usage of AI in law enforcement and analyzes the ethical, legal, and societal implications of these technologies.

CONCERNS WITH IMPLEMENTATION

Balancing Innovation with Privacy

According to a Pew Research Report, 81% of Americans are concerned with how their data is collected and used by companies. Seventy-one percent are concerned about how their data is used by the government. Interestingly, the report also highlights that 67% of Americans have little understanding what companies do with the data collected, and 71% have little or no understanding of what government agencies do with the data collected at all (McClain et al., 2023).

The role of privacy in an ever-changing, technology-based world is an issue that governmental entities have attempted to tackle for decades. The United States Supreme Court addressed the concept of reasonable expectation of privacy in the public facing world with *Katz v. United States* (1967), emphasizing that the Fourth Amendment protects "people, not places." A two-pronged test, also known as the Katz Test, determines whether a citizen has a reasonable expectation of privacy if two criteria are met:

- The person has established an actual (subjective) expectation of privacy.

- The expectation is one that society is willing to recognize as reasonable. (1967)

When it comes to how we interact with the world, we often submit countless pieces of our personal data to third party entities. The Court provided more clarity in what constitutes a reasonable expectation of privacy when information is collected by third party entities with *Smith v. Maryland* (1979) and *United States v. Miller* (1976). In *Smith v. Maryland*, the Court found that phone numbers collected by a pen register would have been collected by the phone company as a part of its normal operation, and therefore, one does not have a reasonable expectation of privacy that that information would be private. In *United States v. Miller* (1976), the Court found that a customer does not have a reasonable expectation of privacy in bank records shared with law enforcement pursuant to a subpoena, as the bank records are the bank's business records, not considered individual's "private papers" under the Fourth Amendment. As more companies collect personal data today, these cases may not completely capture the amount and types of data and information in which we submit to the world. Further, once the information leaves a person, how that data can be used without a person's knowledge is becoming increasingly alarming absent regulations and oversight.

In another case, *United States v. Dionisio* (1973), Justice Stewart provided a somewhat prophetic opinion relevant to modern discussions:

> The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. 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 (1973).

In a 21st century application, the Supreme Court addressed the issue of emerging technology usage by law enforcement in *Kyllo v. United States* (2001). The Court ruled that using a device not commonly available to the public to uncover details inside a home—which would otherwise remain unknown without physical intrusion—constitutes a search and is unreasonable without a warrant (2001).

The reasonable expectation of privacy threshold is much lower when it comes to vehicles, as shown in *United States v. Knotts* (1982). *Knotts* provides the application of technology which is used to augment the senses of an officer, determining it is not constituted as a search if it could be accomplished through unaided visual observation (1982). However, in *United States v. Jones* (2012), the Court ruled that the warrantless placing of a GPS device on a suspect's vehicle constitutes a search. Several justices raised concerns about the length of application (28 days) of the device, as the device had the potential to collect information beyond the crime being investigated. This issue of time is further contemplated by the Court in *Carpenter v. United States* (2018). The Court ruled that the warrantless acquisition of cell site location information (CSLI) violates the Fourth Amendment. The Court stated that while an individual does provide their information voluntarily to third parties, the user may not fully understand the level of information that they provide at the cell site. In the opinion of the Court, Chief Justice Robert holds:

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years. (2018, p. 13)

When it comes to the concerns regarding personal data and privacy, case law does not appear to completely capture the concerns brought forth from the use of emerging technology. Absent action by Congress, state legislatures have been at the forefront of addressing the rapid expansion emerging technology, data privacy, and addressing the potential ramifications that impact Americans . According to the National Conference of State Legislatures (NCSL), in 2024, at least 40 states introduced bills related to AI (NCSL, 2024).

Data Collection and Aggregation

States are moving to fill gaps in data privacy laws to protect consumers from the unknown sale of their data. For companies, the legislative landscape can be difficult to navigate as this has created a complicated patchwork of laws. Some state laws have disclosure requirements, retention policies for the length of time the data can be kept, and limitations on how companies can use the data. Currently, only Texas, Washington, and Illinois have laws that address how biometric identifiers can be used (Kobylka, 2024). Nevertheless, concerns remain about just how much data continues to be collected and what the usage of this data means for the public. Data is the new gold, and data brokers control the industry by collecting, aggregating, and buying and selling information to various entities.

The Florida Legislature addressed the concern of personal data collection through Senate Bill 262 (2023), which fully went into effect on July 1, 2024. This legislation provided Floridians a mechanism to have a better control their personal data regarding how it is collected, processed, and used (SB 262, 2023). Fines for companies not in compliance can be up to $50,000 per violation, and are triple the amount for violations involving a child (2023). Further, the law allows consumers to confirm and access their personal data, and can delete, correct, or obtain a copy of that personal data. Additionally, consumers can opt out of the processing of personal data such as sensitive data (including precise geolocation data), and can opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature (2023).

Senate Bill 262 applies to a select group of companies that collect and process consumer data. The law has several requirements, such as the company must generate $1 billion in annual revenue and 50% global gross revenue must come from selling online ads, including providing targeted advertising (2023). Furthermore, in order for the law to be applicable, the company must operate smart speakers, virtual assistants, or the company must operate an app store offering 250,000 different software applications for consumers to download and install (2023). Overall, this law is aimed at controlling how large technological companies oversee consumer data for the sake of the user's data privacy.

Law enforcement and intelligence agencies have found a huge benefit in the collection of this data and through data brokers have been able to purchase commercially available data. Critics point out the concern that the ability for law enforcement to bypass a warrant requirement (Warren, 2023). In 2024, the Fourth Amendment is Not For Sale Act (H.R. 4639, 2024) passed the House in Congress. However, the bill was not taken up by the Senate. The bill would have prohibited the ability for law enforcement to purchase consumer data commercially through data brokers and require law enforcement to obtain a court order. However, law enforcement groups were strongly opposed to the bill citing the bill would create an inability to conduct investigations, gather information commercially available to the public, and cite concerns for national security (NDAA, 2024).

On the state level, Montana addressed law enforcement access to consumer data through Senate Bill 282 (2025). The legislation prevented law enforcement from purchasing "sensitive data" which is defined in Section 30-14-2802 (24) (a-d), Montana Code, which includes "precise geolocation data," "the processing of genetic or biometric data for the purpose of uniquely identifying an individual," and "data collected from a child, and racial or ethnic information, religion, or citizenship status." However, Senate Bill 282 does provide for exceptions which include a warrant, consent of the individual to access their device, or investigative subpoena.

Florida Governor Ron DeSantis signed a bill creating the Government Technology Modernization Council, which is an advisory council within Florida's Department of Management Services designed to advise the state legislature on emerging technologies, including artificial intelligence (SB 1680, 2024).

In Texas, House Bill 2060 (2023) passed in the 88th Legislative Session and created an advisory council to study the impacts of artificial intelligence and its usage by governmental actors in Texas. The bill required state agencies to produce an inventory detailing how each artificial intelligence product was used by each agency, along with a code of ethics to guide further government adoption of this technology. Ultimately, the findings from this council triggered Senate Bill 1964 (2025), Texas' comprehensive public sector artificial intelligence law, which was signed into law in June 2025 and will take effect on September 1, 2025.

Artificial intelligence will continue to improve as the vectors for data collection increase. However, there remains a need to establish a regulatory framework for government use that strikes a balance between protecting Americans and their data and allowing innovation to blossom. Unfortunately, while it is promising to see the government taking the initiative by establishing advisory committees and managing the boon of emerging technology, the government will, by its nature, remain reactive. The swiftness of technological improvements is only matched by the deployment and usage of its products, creating a cat and mouse game of trying to keep up.

EMERGING TECHNOLOGY IN PRACTICE: CASE STUDIES

Emerging technology is poised to be a force multiplier by assisting in solving cases and the outright prevention of crimes. However, it is certainly not faults as this paper will explore. Concerns in its implementation such transparency not only in usage, but a Blackbox on how the technology works or the error rate of the product provide a large concern as much of this technology is already being actively used in investigations (Vickers, 2024). To combat these issues, guardrails should be explored. For example, there is much needed transparency from law enforcement in how these products work and how they will be implemented in a community. One sheriff in Florida has taken a proactive approach by partnering with a Florida Polytechnical University by reviewing artificial intelligence technology for use in law enforcement, create best practices and policies, training and assistance in artificial intelligence investigations and identify new artificial intelligence products to use or combat against when used by criminals (Fox 13 News Staff, 2024).

Predictive Policing

Law enforcement agency heads have limited resources and must know how, when, and where to implement them, as it is critical to public safety success. Law enforcement is often reactive, but there is a need to focus on more proactive solutions to prevent crime and protect the public.

In the 1990s, New York Police Commissioner Bill Bratton introduced COMPSTAT (Compare Stats), a groundbreaking approach in law enforcement. The program consisted of four key elements: accurate intelligence, rapid deployment of resources, effective tactics, and relentless follow-up (Benbouzid, 2019). As technology advanced in the early 2000s, predictive policing emerged, integrating COMPSTAT's management style with crime data and Geographic Information Systems (GIS) technology (2019). What once took a small team of under-resourced analysts

days to complete was transformed by machine learning algorithms, which made the process faster, more cost-efficient, and capable of forecasting (Mugari & Obioha, 2021).

Predictive policing cannot tell the future, but it serves as a valuable tool for law enforcement agencies to track crime in their communities and to efficiently use scarce resources on a macro-level. However, it has faced its share of controversy. The primary input for these algorithms is historical crime data and crime locations, meaning that the output is limited by the quality of the data that is input (Hunter et al., 2022, pp. 752-753). Additionally, concerns have been raised about the lack of transparency in such algorithms, which can hinder accountability. This opacity and the potential for over-policing data can skew results, resulting in heavier policing in communities can strain relationships (Hunter et al., 2022, p. 753).

Body Cameras Leveraging Artificial Intelligence

Law enforcement agencies nationwide have rapidly increased the use of body-worn cameras in the last decade for the perceived benefits of increased transparency, evidence documentation, tracking officer behavior, reducing complaints, and reviewing officer-involved incidents (Miller et al., 2014). However, some shortcomings of the body-worn cameras were discovered during their early implementation, such as the officer's ability to turn off the cameras, internal and external concerns with privacy, and the problem of filtering through a large amount of data collected. Law enforcement agencies, as a result, have instituted policies requiring the body-worn cameras run nonstop throughout an officer's shift (Sessions, 2024). Additionally, certain agencies have allowed supervisors to access their officers' cameras remotely (Phillips, 2023). While footage of the body-worn cameras can promote transparency and increase the public's trust in law enforcement, critics of the cameras take issue with the lack of privacy and selective transparency by law enforcement to release the footage (Farooq, 2023).

While body-worn cameras provide an opportunity for increased transparency, having a large amount of data to be reviewed by supervisors is extremely difficult, as there is so much footage collected. As a result, unless there is an arrest, officer behavioral issue, or a citizen complaint, the footage may go unseen otherwise. Accordingly, many agencies are turning to artificial intelligence. Several software options are available with price depending on the size of the department (Serrie & Daigle, 2023). Several companies have software that analyzes body-worn camera footage and alerts supervisors by flagging certain behaviors of officers during their interactions with the public. The supervisors can set the standards for conduct, like prohibition of profanity directed at the public, de-escalation and escalation, and politeness (Paul, 2023). TrustStat is software that uses training originally studied at Defense Advanced Research Projects Agency (DARPA), which was developed for the United States Army to examine the relationship between soldiers and locals in Afghanistan and Iraq where encounters would go poorly and, ultimately, violent (NBC News, 2014). From this initial research, the company was created to focus technology on police encounters in the community (Farooq, 2024).

Several agencies who were early adopters of this kind of technology, including those in Seattle, WA, and Aurora, CO, are now removing them from service (Santos, 2023; Bradbury, 2024). Law enforcement in both cities were users of Truleo software and have decided not to renew their contracts . The technology has received considerable pushbacks from law enforcement as they feel as though they are being spied on (Carter, 2023). Research has shown that officer perception of fairness is lowered when automatic activation of their body-worn camera occurs and this drops even lower when used in conjunction with artificial intelligence reviews (Adams, 2025). However, when the footage is reviewed by a human, officers find this slightly fairer even if the review of the footage is conducted at random (2025). Using artificial intelligence in conjunction with body-worn cameras does show the potential to create an atmosphere of transparency while assisting supervisors

and agencies in working through massive amounts of data, and to allow agencies to be proactive rather than reactive when dealing with officer behavior and professionalism. However, having a human involvement can mitigate concerns for officers and the public alike.

Axon US is a leading supplier of body-worn cameras and less lethal weapons for law enforcement agencies and has developed software that can perform case record management and evidence processing. In concert with body-worn camera technology, Axon US has a feature called "Redaction Assistant" that scans videos to locate faces, audio, and any content that can be redacted by the users (Axon, n.d.). Axon US has released a product called "Draft One" which utilizes body-worn cameras to create police reports. The program allows the officer to edit the report through placeholders where the officers must interact with the report at certain points in the draft, and the officer must sign off approval on the reports (Police1 Staff, 2024).

However, one concern raised with the use of artificial intelligence in report writing by law enforcement is the ability for the technology to "hallucinate," or the action of creating items or making observations that do not exist, which impacts programs that use large language model (LLM) or computer vision (IBM, n.d.). While examples of this issue have not been noted as of the writing of this paper, there has been no shortage of hallucinations by artificial intelligence in the courtroom. Nationwide, there have been examples of attorneys submitting legal briefs where the technology simply makes up citations (Merken, 2025). If this were to happen in a police report, there are reasonable concerns that this error could lead to false information could be written, overlooked, and submitted into the report by artificial intelligence, potentially upending someone's life (Ferguson, 2024). Conversely, the error could destroy the credibility of the report, and cause charges in a case to be dropped.

One possible preventative solution is having officers notate the use of such products with a sentence at the end of their report. For example, the officer would write, "This report is based on information obtained by Officer John Doe's body camera and is written using generative artificial intelligence (Draft One), with input by Officer Doe." Currently, the Palm Beach County Sheriff's Office (FL) provides a paragraph at the bottom of their reports indicating the report was created wholly or partially through the use of the technology (Mass & Lipton, 2025). In Utah, preemptive legislation targeted the accuracy of police reports generated by artificial intelligence in the 2025 legislative session. The legislation "[r]equires a police report or other law enforcement record to include a disclaimer if the report or record was created wholly or partially by using generative artificial intelligence," and further requires the "author of a police report or other law enforcement record that was created wholly or partially by using generative artificial intelligence to certify that the author has read and reviewed the report or record for accuracy" (SB 180, 2025). While this statement can help to provide transparency, the oversight and responsibility of what is written in the report should still remain with the officer.

In Florida's 2025 Legislative Session, Senate Bill 1444 (2025), and its related House companion, Committee Substitute for House Bill 1371 (2025), had sections regulating the usage of artificial intelligence through the use of body cameras. In the Senate version, the legislation proposed regulating any data that was collected and processed using artificial intelligence in concert with a body-worn camera, stating that such data "must be subject to human oversight and may not be the sole basis for an arrest" (SB 1444 C1, 2025). The House bill's artificial intelligence section on pages 6-7 prohibited a law enforcement agency from reviewing or monitoring "audio or video data recorded by a body camera for purposes of initiating an investigation into a law enforcement officer's conduct or taking any disciplinary action against a law enforcement officer" (HB 1371, 2025). Ultimately, the artificial intelligence language was amended out of the bills.

Emerging Technology Firearms Detection Devices

Automatic gunshot detectors are often acoustic listening devices which capture the soundwaves from a sonic boom or muzzle blast when a weapon is fired (Mares, 2022). Multiple devices are set up and then triangulate the noise based on the time it takes to reach the device to establish a location of the gunshot (Mares, 2022). Companies like Soundthinking (formerly known as ShotSpotter) have been deployed in nearly 150 communities across the United States uses acoustic listening devices to notify law enforcement of gunshots that would otherwise go undetected and unreported in the community. The Jacksonville Sheriff's Office in Florida has reported that since the implementation of these devices, they have seen a reduction of 25% alerts from the technology from the previous year (Stofan, 2024). Moreover, the agency reported 74 shootings in 2024 down from 81 in 2023 (2024).

However, not all communities share the same result. Chicago and Houston are dropping their contracts with Soundthinking (Ebrahimji, 2024). In Houston, the mayor cited a limited return on investment with the product, and commented that while there have been a few high-profile arrests, the overall investment has not yielded the intended results (Groogan, 2024). Further, one member of the city council commented that the money would be spent better employing more officers (Groogan, 2024). As a result, Houston will allow for the $3.5 million, five-year contract is set to expire in 2027 (Fox-Sowell, 2024).

In Chicago, their mayor has decided not to renew the contract, holding that the city paid $9 million a year and stating concerns with little evidence of its reliability and "over susceptibility to human error" (Mohtasham, 2024). In a report provided to the Inspector General's Office in Chicago, it noted that 85.6% of the reports from Soundthinking did not result in the report of a crime, or law enforcement case being generated by the Chicago Police Department (Ferguson & Witzburg, 2021). Conversely, the Illinois Policy Institute has criticized the mayor's decision, stating that removing the product severely limited policy decisions for the Chicago Police Department, as they argued that the measure of the success of the technology should not be measured by lack of law enforcement reports or crimes reported, but instead by the crimes prevented by the technology (Vallas, 2024). Further, the Illinois Policy Institute noted that 125 lives had been saved by the use of the technology (2024).

The City of New York partnered with a company called Evolv that seeks to replace metal detectors by promoting a "frictionless approach" of having individuals walk through security much like a metal detector (Del Valle, 2024). However, unlike a metal detector, technology allows a person to not have to remove items from their person and allows people to continue moving in a continuous manner. The company states that it uses artificial intelligence designed to only alert if the system detects anomalies that may indicate a firearm or a weapon. While the technology sounds great in theory, it is not flawless as it has a tendency to false report the presence of a weapon (Del Valle, 2024). In other cases, technology fails to detect weapons. One school district in New York removed their product following an incident where a student brought a knife to school and another student was stabbed (Clayton, 2023). The company in 2024 agreed to a settlement with the Federal Trade Commission to resolve claims the company mislead customers by making claims of the technology's capabilities (Guariglia & Quintin, 2024). Within the settlement agreement, the company did not admit fault, but were ordered to no longer make claims that the technology can "detect weapons," "ignore personal items", or "the ability to detect weapons while ignoring harmless personal items" (*Federal Trade Commission v. Evolv Technology Holdings*, 2024). Further, the settlement agreement requires the company to provide a notice to the customers and allow the customers to cancel their contracts (*Federal Trade Commission v. Evolv Technology Holdings*, 2024).

Additionally, several states and other school districts in Florida have adopted a product called ZeroEyes that scans security camera feeds to detect firearms

(Stone, 2023; WCTV Staff, 2023; Hildreth, 2024). The technology detects when a weapon has been brandished by an individual and sends an alert to the ZeroEyes Command Center, alerting a command center staffed by veterans and law enforcement to confirm whether a weapon has been brandished, providing a "human in the loop" confirmation process. The command center then contacts local authorities. However, this technology cannot detect a weapon that is concealed or in the holster.

The United States Department of Homeland Security conducted a study on the technology in 2023. Within the DeepZero Gun Detection Platform Technology Report, evaluators' responses highlighted the system's ease of use and the ability to track a subject with a firearm to provide on-going situation awareness. However, the evaluators were concerned about the seconds between when the notification to review occurs to when officials are alerted, especially in an active shooter situation:

> Some evaluators noted that while DeepZero can alert first responders within seconds of a brandished weapon, it does not guarantee threat prevention. ZeroEyes gets the first alert notification and initiates the dispatch, if necessary, but takes three to five seconds to notify first responders of the incident. Evaluators wonder if these critical seconds before ZeroEyes alerts first responders may result in the system taking too long to be as effective in detection and alerting. ZeroEyes developers point out, however, that there is a trade-off between timeliness and their false positive rate: they cite the additional review by a human as crucial to low false positives (NUSTL, 2023, p. 18).

During Florida's 2025 Legislative Session, SB 562 (2025) and HB 491 (2025) were filed in response to the City of Daytona Beach placing ZeroEyes in public spaces (Reed, 2025). The House Bill was amended to prevent government entities from using "artificial intelligence in conjunction with any camera, video recording, live-streaming device, or similar technology to detect concealed firearms in a public place" (CS/HB 491, 2025, pp. 1-2). The House bill passed its respective chamber, but the Senate bill died in committees.

Facial Recognition Technology

According to a 2022 Pew Research poll on the use of facial recognition technology by law enforcement, 46% of respondents said it would be a "good idea" for society, while 27% believed it would be a "bad idea," and 27% were unsure (Rainie et al., 2022). Additionally, 70% of respondents agreed that a positive match from facial recognition should not be enough to justify an arrest, especially with the possibility of the program being wrong. The poll also broke down responses by race, with 48% of Black respondents expressing concern that the technology would be used to monitor Black and Hispanic neighborhoods more than others. Furthermore, 28% of Black respondents believed it would lead to more false arrests (2022). While law enforcement's use of artificial intelligence can be beneficial, there is certainly room for improvement on its perceived level of trust and implicit biases through more transparency in usage.

> Facial recognition technology uses a photo or still from a video feed of a person—often called a probe or live photo—and converts it into a template, or a mathematical representation of the photo. A matching algorithm can then compare the template to one from another photo and calculate their similarity. (GAO, 2021, p. 3)

At its core, facial recognition is a tool that still requires human interaction to determine the value of the data produced by the system. However, there are concerns regarding privacy, misuse, inaccuracy of the data due to racial bias, and failure to disclose usage by law enforcement. Further, a major concern with this technology is what database is being used to compare the image. For example, if someone were to use technology to compare a picture against a group of mugshots, it is likely the results would be someone who has a mugshot. These systems are designed to compare against only the data it is provided in set databases (Garvie, 2022).

The National Institute of Standards and Technology (NIST) conducted a study in 2019 to evaluate 189 algorithms of facial recognition technology (Boutin, 2019). NIST uses several different methodologies to test the programs, one-to-one is "biometric verification in which submitted feature data is compared with that of one, claimed, identity." (NIST, n.d.-a) In this case, a single image is compared to another image in a one to one match up. In one-to-many comparisons, the single image is compared against a large database of images to find a match (NIST, n.d.-b). In comparing one-to-many comparisons , the study found that there were high numbers of false positives amongst women and African Americans, particularly African American women. In one-to-one matching , American Indians offered high false positives (Boutin, 2019).

The NIST allows ongoing submissions by developers to have their facial recognition programs tested by Face Recognition Technology Evaluation (FRTE) and Face Analysis Technology Evaluation (FATE). The FRTE program reviews submissions on one-to-one identification, 1:N identification (one-to-many), Face in Video Evaluation (FIVE), and twin comparisons which compare fraternal twins (NIST, n.d.-a). Face in Video Evaluation (FIVE) reviews the capability of facial recognition software in video recordings (NIST, n.d.-c). The FATE-MORPH program studies face morphing, quality of probe image, and age estimations (NIST, n.d.-d). Developers can submit their ongoing work to NIST for review of a company's algorithms (NIST, n.d.-a). This on-going testing helps developers to have their products reviewed independently.

Facial recognition technology has been used in the state of Florida for more than 20 years. In 2001, the Pinellas County Sheriff's Office used a Community Oriented Policing Services program (COPS) grant to create the Face Analysis Comparison & Examination System (FACES, now FACESNXT), which allows criminal justice agencies in Florida and federal agencies such as the IRS and Customs and Border Patrol to better identify suspects (Congressional Research Service, 2020; Pinellas County Sheriff's Office, n.d.). The program uses mugshots and driver's license photos that agencies can use as a database. The Pinellas County Sheriff's Office requires a memorandum of understanding between the sheriff's office and other outside agency users that all facial recognition usage policies be open to the public (Pinellas County Sheriff's Office, n.d.).

A popular facial recognition technology currently used by many law enforcement agencies across the nation is Clearview AI, which has a database containing billions of images available for use. Clearview AI states on its website that they have partnered with 3,100 agencies in the United States, including the Federal Bureau of Investigation and the Department of Homeland Security (Clearview AI, 2022). The company has a controversial approach to obtaining these photos through data and web scraping from social media (Hill, 2020). The proces s of web and data scraping itself is a normal function used by many companies; however, in this case, the company has been accused of violating terms of service for social media companies (CBS News, 2020). Meta (Facebook and Instagram), in their current privacy policy, states that Meta can "preserve, use and share your information" with third party entities in compliance with court orders (Meta, 2025).

In 2020, Clearview AI was sued by the ACLU in Illinois for violation of the Illinois' Biometric Information Privacy Act (BIPA) Section 740 Illinois Compiled Statutes 14/15. The law prohibits an entity from "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" unless the entity notifies an individual in writing as to the specific reason and time frame for retention and obtains a written release from the individual. Further, the law restricts and entity cannot "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information" (Section 740 Illinois Compiled Statutes 14).

As a result of the lawsuit, Clearview AI would only provide services to the federal government and to law enforcement outside the state of Illinois (Foody & O'Brien, 2022). Further, several states and cities in the

United States have banned the usage of Clearview AI after raising concerns over the accuracy and potential for racial bias by the technology (MacMillan, 2024). However, officers who work in areas where the ban exists on the use of Clearview AI by asking the neighboring jurisdiction to run the program on their behalf (MacMillan, 2024).

A 2024 murder prompted police officers in Ohio to use Clearview AI in footage captured by a city surveillance camera of the suspect. The footage was processed through Clearview AI and a suspect was identified by law enforcement (Daniel, 2025). The police secured a search warrant for the suspect's residence, where police located a gun which they believed was the murder weapon. The defense filed a motion to suppress, as it was argued that there was insufficient probable cause to justify the search warrant (2025). Law enforcement did not notate the use of Clearview AI, and the information was not independently verified the suspect's identity prior to execution of the search warrant. The judge ruled to suppress the evidence (2025). The case is currently ongoing as of 2025, as the Ohio Attorney General has filed a "friend of the court" brief in April 2025 supporting law enforcement usage in the case while it is being appealed to the appellate court. The attorney general's office has stated that the search was for the apartment and not the suspect (Daprile, 2025). Further, the attorney general has stated that the lack of disclosing technology in the probable cause affidavit is "negligent at worst" and "nowhere near deliberately false or misleading" (Daprile, 2025).

Within Clearview AI's Terms of Service, the independent verification section states that search results should be used as a lead and should be reviewed by more than one person within the organization (Clearview AI, 2025). The terms of service state: "The Clearview Platform is not designed or intended to establishing the identity of an individual, and Users shall not use it as such" (2025, appx. 1). Finally, the terms of service state that "search results produced by the Clearview Platform are not intended or permitted to be used as admissible evidence in a court of law or any court filing" (2025, appx. 1).

Several states have moved to limit or require additional reporting of facial recognition technology usage by law enforcement. In 2024, Maryland passed the most comprehensive and strict legislation for the use of facial recognition technology by law enforcement with Senate Bill 182 (2024). The legislation went into effect on October 2024, and it requires the Maryland State Police to develop model statewide policy and it prohibits use by any local agency who contracts out any facial recognition technology unless the technology abides by the statewide model policy (SB 182, 2024). According to the bill, the usage of facial recognition technology is limited to certain types of offenses, the technology cannot be used in real time, and it restricts the databases of mugshots or driver's license used to compare images (2024). However, the bill allows for outside provider databases to be used if the law enforcement agency has entered into an agreement. Additionally, the bill allows for the law enforcement agency to discontinue to the use of an external database if the third party provider if "commits a material breach of the provisions governing the methods by which images in the database are collected" (2024). Further, there is a requirement of disclosure by the state government , who must comply with the Maryland Rules of Evidence regarding the discovery of the name of the system used and the results generated using the technology to generate leads for each system used and for each database searched (2024). Finally, the law states that evidence produced using this technology can be used to *develop* probable cause; however, it cannot be used *solely* to establish probable cause (2024).

Unfortunately, facial recognition technology has been the source of false arrests in cases nationwide as individuals. As a result, the technology should never be the sole evidence to establish probable cause, but instead an investigative lead only. As reported by the Washington Post, one of the concerns raised is the usage of facial recognition technology is the lack of disclosure of the use of this technology by law enforcement (MacMillan et al., 2025). Legislatures could explore establishing policies which create standardization to ensure consistency in

disclosure and usage and further forbid the use of the technology to be the sole basis of establishing probable cause.

The Florida Department of State's General Records Schedule provides the minimum retention schedule for records for Florida's government. The schedule defines for facial recognition image records to include "but is not limited to, facial images, renderings and associated data generated or received for automated comparison with images of known individuals to make identifications or exclusions. The series may also include user logs, query results, submitter and/or examiner information, and conclusions" (Florida Department of State, 2023, p. 11, Item #221). The schedule states that these records should be retained until "obsolete, superseded, or administrative value is lost" (Florida Department of State, 2023, p. 11, Item #221).

Automatic License Plate Readers (ALPRs)

One technology that is rapidly being deployed and being used by countless communities, private sector organizations, and law enforcement agencies is automatic license plate readers (ALPRs) Flock Safety, which uses ALPR technology to help to solve crimes by taking the information of a license plate and running the information against law enforcement "hit lists" and the National Crime Information Center (Flock Safety, 2023). However, what sets this technology apart is the ability to obtain vehicle information even in the absence of a license plate. For example, if an officer does not have a plate number, but instead has a vehicle description, then the officer can search for specific vehicle identifiers. In the example provided by Flock Safety, an officer can search for a "white F-150 with a ladder in the back" (Flock Safety, 2025a, para. 4). This allows for far more opportunities to find a suspect's vehicle but also goes beyond simply searching for license plates. This technology has quickly gained popularity, as the company website states are currently over 5,000 agencies, 6,000 communities, and 1,000 businesses participating in the program, according to the company's website (Flock Safety, n.d.).

The standard for data collected remains with Flock Safety for 30 days, law enforcement can hold this data for much longer or much less time depending on the laws governing the data. According to Flock Safety's Evidence Request Policy, if an agency seeks to hold onto the data longer than the 30 days and is not otherwise prescribed by law, the company requires the agency to obtain approval from an elected official or governing body and hold the data up to one year (Flock Safety, 2025a). The policy defines an elected or governing body as:

1. Democratically elected bodies include, but may not be limited to: state, local, county, city, and town governments.

2. Democratically elected officials include, but may not be limited to: state and local elected officials, elected sheriffs. (Flock Safety, 2025b, Frequently Asked Questions)

However, as mentioned before, the data can fluctuate depending on the law where the technology operates. Some states have access for less than 30 days, and some states have access for years. New Hampshire's data retention is the most restrictive, as Section 261:75-b, New Hampshire Revised Statutes, requires the data collected to be deleted within three minutes of the capture "unless an alarm resulted in an arrest, a citation, or protective custody, or identified a vehicle that was the subject of a missing person or wanted broadcast, in which case the data on the particular number plate may be retained until final court disposition of the case."

In Florida, Section 316.0777, Florida Statutes, provides that ALPRs are allowed for the "the purpose of collecting active criminal intelligence information or active criminal investigative information." Further, in Section 119.011 (3)(a), Florida statute defines that active criminal intelligence information "shall be considered 'active' if it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities." The issue of records retention of the data collected by ALPR is addressed

in Section 316.0778, Florida Statutes, which requires the Department of State in consultation with the Florida Department of Law Enforcement to develop a retention schedule for the maximum amount of time in which data may be retained.

In reviewing the Florida Department of State's General Records Schedule, "images of licenses plates and any associated metadata" shall be retained "until obsolete, superseded, or administrative value is lost, but no longer than 3 anniversary years unless required to be retained under another record series" (Florida Department of State, 2023, p. 14, Item #217). Conversely, when looking at the retention schedule for body camera or in-car camera footage, the data retention time frame is much shorter at 90 days (Florida Department of State, 2023, p. 19, Item #224) and 30 days (Florida Department of State, 2023, p. 19, Item #192), respectively. Further, the record retention limit may be extended if it becomes a different record series, such as Criminal Intelligence, Criminal Investigative Records, or if the data collected is related to a crime (Florida Department of State, 2023). In cases of body-worn cameras and in-car cameras, the footage can be held longer for criminal investigative or criminal intelligence records.

In 2024 (and currently ongoing as of 2025), two plaintiffs sued the City of Norfolk, Virginia, after the city installed 172 Flock Safety cameras. The plaintiffs argue that their Constitutional rights have been infringed by conducting warrantless search of the movements of individuals. The City of Norfolk filed a motion to dismiss the case (Hughes, 2025). However, the judge in the case stated that "a reasonable person could believe that society's expectations, as laid out by the Court in *Carpenter* (2018), are being violated by the Norfolk Flock system" (*Schmidt et al. v. City of Norfolk et al.*, 2025, p. 18).

Virginia Governor Glenn Youngkin in 2025 signed House Bill 2724 (2025) into law, which addresses the use of automatic license plate readers (ALPR) in criminal investigations where there is reasonable suspicion a crime occurred. Further, allowable uses of ALPRs are in active cases of a missing or endangered person and to obtain information on a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate (HB 2724, 2025). The bill also requires law enforcement agencies who use ALPR systems to provide information annually, including the number of cameras used by the agency; a list of all state and federal databases that the information was compared against; the total number of times the system was accessed; race, ethnicity, age, and gender of the driver of any motor vehicle stopped based on a notification from the system; and whether the agency allows any other law enforcement agency to use the system or has been granted access (HB 2724, 2025). Further, the Virginia State Police are required to collect and to aggregate this data statewide. The bill also requires the Division of Purchases and Supply of the Department of General Services to determine what systems can be used and to set system standards for the usage of such technology for the state.

In June 2025, the City of Austin (TX) announced it would be letting its contract with Flock Safety expire after citing concerns regarding the usage of ALPR cameras related to data sharing with Immigration and Customs Enforcement (ICE) for immigration crimes (Rendon, 2025). The City of San Marcos Police Department (TX) followed suit after a city council meeting. Originally, the meeting was to discuss the current Flock contract and expansion of the program to multiple new cameras around the city (Rendon, 2025). However, following responses from the community, the City of San Marcos Police Department created new standards which stopped the automatic sharing of ALPR data with other law enforcement, set acceptable use standards including what crimes and instances in which other agencies could request the data, removed multiple cameras from around the city, set up new auditing and internal controls to require a case number and reason code for entry of a new vehicle (San Marcos Police Department, n.d.).

GOVERNMENT OVERSIGHT INTO TECHNOLOGY

One of the most significant areas in which artificial intelligence usage by law enforcement could improve drastically is by offering more transparency, not only in usage of the technology by law enforcement, but also with how technology works to remove any misconceptions and how it impacts public safety. It is vital to bring stakeholders together to find proper solutions to maximize trust, cooperation, and involvement. Several cities and states around the country have attempted to find ways to provide better transparency and oversight of artificial intelligence as presented several times in this paper.

During President Trump's first administration, he signed Executive Order 13960 (2020), requiring federal agencies, including federal law enforcement, to provide case use inventories of all forms of AI used by the agency. Through H.R. 6395 (2021), the National AI Advisory Committee (NAIAC) in which the committee is tasked with advising the president on AI and emerging technology including a subcommittee on law enforcement. Through President Biden's Executive Order 14074 (2022), the National AI Advisory Committee (NAIAC) sought to address the use of artificial intelligence usage in policing which focused on transparency and accountability. Additionally, in the Bipartisan House Task Force on Artificial Intelligence (2024), one recommendation highlighted the need for transparency for users affected by decisions made using artificial intelligence in "enforcement and judicial decision-making" (2024).

On the state level, the Virginia General Assembly passed and Governor Youngkin signed into law House Bill 1496 (2024), which requires all state, county, and local law enforcement to report the usage and procurement of surveillance technologies to the Department of Criminal Justice Services annually (HB 1496, 2024). In 2025, the Virginia General Assembly passed and the governor signed into law House Bill 2725, which reauthorized HB 1496 and amended the language to require law enforcement in Virginia to report third-party services or subscriptions providers that "allow access to any form of surveillance technology or data" (HB 2725, 2025).

Overwhelmingly, transparency in the usage of artificial intelligence products in policing is key. There is a delicate balance of trust between the community and law enforcement which must be upheld. Within the Final Report of the President's Task Force on 21st Century Policing in 2015 recommended that "[l]law enforcement agencies should consider the potential damage to public trust when implementing crime fighting strategies" (President's Task Force on 21st Century Policing, 2015). As such, those who work with artificial intelligence should understand there are limitations to this technology and the goal for every law enforcement agency is to maintain trust through transparency and oversight.

CONCLUSION

As with each of the technologies presented above, there is optimism and hope that emerging technology can provide incredible benefits to law enforcement and communities, alike. However, as noted, there are limitations to what technology can do in its current capacity. Further, the issue of transparency cannot be understated as the technology has its flaws, and human oversight is needed to keep a "human in the loop" to ensure proper oversight. Understanding the limitations to the technology's current capabilities, undue enhanced value should not be added to evidence simply due to the output from an algorithm. It is crucial for that this technology should only augment, not replace human judgement.

To ensure the success of the technology and protect the public, guardrails should be explored. State legislatures could explore requiring each law enforcement agency to provide an inventory of its usage of artificial intelligence and emerging technology that is used to collect and document evidence annually for ongoing policy maintenance to ensure the most transparency is available for the public. Additionally, state legislatures could explore setting acceptable use standards for AI by government operators as this would provide standardization in the use of

the technologies. By offering more transparency and enforcing standards through oversight strikes a proper balance that ensures citizens' rights are protected while also not completely restricting emerging technology. Additionally, state legislatures could explore requiring law enforcement to list in the report or probable cause affidavit, any use of artificial intelligence which may have influenced the case. The world is now at a pivotal point with emerging technology, and states can set a foundation. While the hope for technology is to improve humanity, we should ensure that humanity remains at the forefront of the justice system.

RECOMMENDATIONS

Policymakers

- State lawmakers should explore requiring each law enforcement agency to provide an inventory of its usage of artificial intelligence and emerging technology that is used to collect and document evidence to the state attorneys general, the state legislatures, and governors' offices annually for ongoing policy maintenance.

- State legislatures should explore setting acceptable use standards for artificial intelligence for government operators and should enforce proper standards through adequate governmental oversight.

- Review how data is collected by artificial intelligence and set data retention standards.

- State legislatures should explore requiring each law enforcement agency to disclose the use of AI or similar emerging technologies if its use influenced an investigation and would not be covered by current statutory obligations, by *Brady v. Maryland* (1963), or by its progeny otherwise.

- The criteria for state agencies' usage of Facial Recognition technology should be established legislatively.

- Evaluate the need for curriculum and uniform training standards for users including law enforcement officers, crime analysts and support staff, including resources necessary to facilitate training for non-governmental technology providers.

Law Enforcement

- Law enforcement agencies should work with their community and technology stakeholders to be transparent about the proper usage of such technologies within their communities.

- Policies and procedures of law enforcement agencies should be accessible to the public.

REFERENCES

Adams. I. (2025). *Automation and artificial intelligence in police body-worn cameras: Experimental evidence of impact on perceptions of fairness among officers.* Journal of Criminal Justice. Vol. 25. https://doi.org/10.1016/j.jcrimjus.2025.102373

Axon. (n.d.). *Maintain evidence integrity while preserving privacy.* Retrieved July 30, 2025, from https://www.axon.com/products/redaction

Bipartisan House Task Force on Artificial Intelligence (2024). *Guiding principles, forward-looking recommendations, and policy proposals to ensure America continues to lead the world in responsible AI innovation.* https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. *Big Data & Society, 6*(1), 205395171986170. https://journals.sagepub.com/doi/10.1177/2053951719861703

Boutin, C. (2019, December 19). *NIST study evaluates effects of race, age, sex on face recognition software.* NIST. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Bradbury, S. (2024, August 30). *Aurora police ended AI review of body cameras. Unprofessionalism plummeted when it was in use, new research shows.* The Denver Post. https://www.denverpost.com/2024/08/29/aurora-police-body-cameras-ai-review-truleo-unprofessionalism/

Brady v. Maryland, 373 U.S. 83 (1962). https://www.oyez.org/cases/1962/490

Carpenter v. United States, 585 U.S. 296 (2018). https://www.oyez.org/cases/2017/16-402

Carter, M. (2023, September 27). *Decision to halt program analyzing Seattle police bodycam video under scrutiny.* Seattle Times. https://www.seattletimes.com/seattle-news/law-justice/decision-to-halt-program-analyzing-seattle-police-bodycam-video-under-scrutiny/

Clayton, J. (2023, May 23). *AI scanner used in hundreds of US schools misses knives.* BBC. https://www.bbc.com/news/technology-65342798

Clearview AI. (2022, March 25). *Clearview AI releases 2.0 version of industry leading facial recognition platform for law enforcement*. https://www.clearview.ai/press-room/clearview-ai-releases-2.0-version-of-industry-leading-facial-recognition-platform-for-law-enforcement

Clearview AI. (2025, January 7). *Terms of service*. Retrieved July 30, 2025, from https://www.clearview.ai/terms-of-service

Committee Substitute for House Bill 1371. Introduced. Florida Legislature. Regular. (2025). https://www.flhouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h1371c1.docx&DocumentType=Bill&BillNumber=1371&Session=2025

Committee Substitute for House Bill 481. Passed Florida House of Representatives. Florida Legislature. Regular. (2025). https://www.flhouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h0491c1.docx&DocumentType=Bill&BillNumber=491&Session=2025

Congressional Research Service. (2020, October 27). *Federal law enforcement use of facial recognition technology.* https://crsreports.congress.gov/product/pdf/R/R46586

CompTIA. (n.d.). *Artificial intelligence (AI) glossary: Terms & definitions for beginners*. Retrieved July 30, 2025, from https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/aiglossary.pdf

Daniel, L. (2025, January 29). Judge throws out facial recognition evidence in murder case. *Forbes*. https://www.forbes.com/sites/larsdaniel/2025/01/29/judge-throws-out-facial-recognition-evidence-in-murder-case/

Daprile, L. (2025, March 14). *Ohio AG Yost sides with Cleveland police in murder case in which officers used AI to justify search*. Cleveland.com. https://www.cleveland.com/news/2025/03/ohio-ag-yost-sides-with-cleveland-police-in-murder-case-in-which-officers-used-ai-to-justify-search.html

Del Valle, G. (2024, March 28). *NYC will test AI gun detectors on the subway.* The Verge. https://www.theverge.com/2024/3/28/24114956/nyc-subway-ai-gun-detectors-evolv-technologies

Ebrahimji, A. (2024, February 24). *Critics of ShotSpotter gunfire detection system say it's ineffective, biased and costly.* CNN. https://www.cnn.com/2024/02/24/us/shotspotter-cities-choose-not-to-use/index.html

Exec. Order No. 13960, 85 Fed. Reg. 78,939 (Dec. 8, 2020). https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-thefederal-government

Exec. Order No. 14074. 87 Fed. Reg. 32,945. (2022, May 31). https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and

Farooq, U. (2023, December 18). *Body cameras were sold as a tool of police reform. Ten years later, most of the footage is kept from public view*. ProPublica. https://www.propublica.org/article/body-camera-videos-police-killings-remain-hidden-from-public

Ferguson, A. G. (2024, July 17). *Generative suspicion and the risks of AI-assisted police reports*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4897632

Ferguson, J., & Witzburg, D. (2021). *The Chicago Police Department's use of Shotspotter Technology.* City of Chicago Office of Inspector General. https://igchicago.org/wp-content/uploads/2023/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf

Federal Trade Commission v. Evolv Technology Holdings, Inc. (2024, November 26). https://www.ftc.gov/system/files/ftc_gov/pdf/EVOLVORDERFILED.pdf

Finklea, K., Harris, L. & Kolker, A. (2020, October 27) *Federal law enforcement use of facial recognition technology.* Congressional Research Service. https://www.congress.gov/crsproduct/R46586#:~:text=Facial%20recognition%20broadly%20involves%20the,algorithms%20work%20to%20compare%20images

Flock Safety. (n.d.). *Flock Safety license plate readers.* Retrieved July 30, 2025, from https://www.flocksafety.com/products/license-plate-readers

Flock Safety. (2025a, February 14). *The Future of Investigations: How Flock's New AI-Powered Tools Are Transforming Vehicular Evidence.* https://www.flocksafety.com/blog/the-future-of-investigations-how-flocks-new-ai-powered-tools-are-transforming-vehicular-evidence#:~:text=Introducing%20FreeForm:%20A%20Smarter%20Way,law%20enforcement%20with%20effective%20tools

Flock Safety. (2025b). *Flock Evidence Request Policy*. Retrieved July 30, 2025, from https://www.flocksafety.com/legal/flock-evidence-policy

Florida Department of State. (2023). *State of Florida: General records schedule GS2 for criminal justice agencies and district medical examiners*. https://files.floridados.gov/media/706718/gs2-june-2023.pdf

Fox 13 News Staff. (2024, June 7). *Polk County Sheriff's Office launches new lab to combat AI threats.* Fox 13-WTVT. https://www.fox13news.com/news/polk-county-sheriffs-office-launches-new-lab-combat-ai-threats

Fox-Sowell, S. (2024, May 30). *Houston mayor calls gunshot detection tech a 'gimmick,' plans to end ShotSpotter contract.* Statescoop. https://statescoop.com/houston-shotspotter-gimmick/

Foody, K., & O'Brien, M. (2022, May 9). *Face-scanner Clearview agrees to limits in court settlement*. AP News. https://apnews.com/article/technology-business-social-media-chicago-lawsuits-fc4f902976aecdd38b1eca48694c8faa

Garvie, C. (2022). *A forensic without the science: Face recognition in U.S. criminal investigations.* Center on Privacy & Technology at Georgetown Law. https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf

Government Accountability Office (2021, August) *Facial Recognition Technology Current and Planned Uses by Federal Agencies*. Report to Congressional Requesters GAO-21-526. https://www.gao.gov/assets/gao-21-526.pdf

Groogan, G. (2024, May 30). *Houston Mayor set to halt ShotSpotter technology.* FOX 26 Houston. https://www.fox26houston.com/news/houston-mayor-set-halt-shotspotter-technology

Guariglia, M & Quintin, C. (2024, December 6) *FTC rightfully acts against so-called "AI weapon detection"company Evolv.* Electronic Frontier Foundation Deeplinks Blog. *https://www.eff.org/deeplinks/2024/12/ftc-rightfully-acts-against-so-called-ai-weapon-detection-company-evolv*

Hildreth, R. (2024, February 5). *Weapons-detecting software utilizing AI technology to make schools safer*. FOX 35 Orlando. https://www.fox35orlando.com/news/sheriffs-office-promises-expansion-of-school-safety-technology

Hill, K. (2020, January 18). The secretive company that might end privacy as we know it. *The New York Times*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Holdsworth, J., & Stryker, C. (2024, August 11). *What Is NLP (Natural Language Processing)?* IBM. https://www.ibm.com/topics/natural-language-processing

Holdsworth, J. & Scapicchio, M. (2024, June 17). *What is Deep Learning?* IBM. https://www.ibm.com/think/topics/deep-learning

House Bill 491. Introduced. Florida Legislature. Regular. (2025). https://www.flhouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h0491__.docx&DocumentType=Bill&BillNumber=491&Session=2025

House Bill 1496. Signed. 2024 Virginia General Assembly. (2024). https://legacylis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB1496+pdf

House Bill 2060. Signed. 88th Texas Legislature. Regular. (2023). https://capitol.texas.gov/tlodocs/88R/billtext/html/HB02060I.htm

House Bill 2724. Signed. 2025 Virginia General Assembly. (2025). https://lis.virginia.gov/bill-details/20251/HB2724

House Bill 2725. Signed. 2025 Virginia General Assembly. (2025). https://lis.blob.core.windows.net/files/1074296.PDF

H.R. 4639. Fourth Amendment Is Not For Sale Act. 118th Congress. (2024). https://www.congress.gov/bill/118th-congress/house-bill/4639/text

H.R. 6395. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. 116th Congress. (2021). https://www.congress.gov/bill/116th-congress/house-bill/6395

Hughes, K. (2025, February 7). *Flock camera lawsuit to proceed in Norfolk.* WAVY.com. https://www.wavy.com/news/local-news/norfolk/flock-camera-lawsuit-to-proceed-in-norfolk/

Hunter, D. Bagaric, M., & Stobbs, N. (2020) *A framework for the efficient and ethical use of AI in the criminal justice system*. Florida State University Law Review. Vol. 47:749. https://www.fsulawreview.com/wp-content/uploads/2022/08/ETHICAL-USE-OF-ARTIFICIAL-INTELLIGENCE.pdf

IBM. (n.d.). *What are AI hallucinations?* Retrieved July 24, 2025, from https://www.ibm.com/think/topics/ai-hallucinations

Illinois' Biometric Information Privacy Act (BIPA), 740 ILCS 14/15. (2008). https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57

Katz v. United States, 389 U.S. 347 (1967). https://www.oyez.org/cases/1967/35

Kelly, J. (2025, February 3). *What is Black Box AI?* Invoca Blog. https://www.invoca.com/blog/what-is-black-box-ai

Kobylka, D. (2024, April 22). *State legislators have their sights on biometric and touchless ID*. Multistate. https://www.multistate.us/insider/2024/4/22/state-legislators-have-their-sights-on-biometric-and-touchless-id

Kyllo v. United States, 533 U.S. 27 (2001). https://www.oyez.org/cases/2000/99-8508

MacMillan, D. (2024, May 18). *These cities bar facial recognition tech. Police still found ways to access it.* Washington Post. https://www.washingtonpost.com/business/2024/05/18/facial-recognition-law-enforcement-austin-san-francisco/

Macmillan, D., Ovalle, D., & Schaffer A. (2025, Janurary 13). *Arrested by AI: Police ignore standards after facial recognition matches*. Washington Post. https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/

Manning, C. (2020). *Artificial intelligence definitions*. Standford University. https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

Mass, D., & Lipton, B (2025, July 10). *EFF's guide to getting records about Axon's Draft One AI-generated police reports.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2025/07/effs-guide-getting-records-about-axons-ai-generated-police-reports

Mares, D. (2022). *Gunshot detection: Reducing gunfire through acoustic technology.* Bureau of Justice Assistance. https://www.smart-policing.com/sites/default/files/2022-11/2022-SPI_POP-GunAcoustic_FINAL.pdf

Martineau, K. (2023, April 20). *What is generative AI?* IBM. https://research.ibm.com/blog/what-is-generative-AI

McKinsey & Company. (2024). *What is AI (artificial intelligence)?* https://www.mckinsey.com/featuredinsights/mckinsey-explainers/what-is-ai/

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). *How Americans view data privacy*. Pew Research Center. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Merken, S. (2025, May 25). *Trouble with AI 'Hallucinations' spreads to big law firms.* Reuters. https://www.reuters.com/legal/government/trouble-with-ai-hallucinations-spreads-big-law-firms-2025-05-23/

Meta. (2025, June 16). *How do we respond.* Meta Privacy Policy. https://www.facebook.com/privacy/policy/?section_id=10-HowDoWeRespond

Mugari, I., & Obioha, E. E. (2021). Predictive policing and crime control in the United States of America and Europe: Trends in a decade of research and the future of predictive policing. *Social Sciences, 10*(6), 234. https://doi.org/10.3390/socsci10060234

National Conference of State Legislatures [NCSL]. (2024, September 9) *Artificial Intelligence 2024 Legislation*. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation

National District Attorneys Association. (2024, April 16). *Nation's law enforcement associations continue to oppose the Fourth Amendment Is Not For Sale Act.* https://ndaa.org/wp-content/uploads/Law-Enforcement-Associations-Opposition-Statement-to-FANFSA-April-2024.pdf

National Institute of Standards and Technology [NIST]. (n.d.-a.). *1:1 Verification.* Retrieved July 30, 2025, from https://pages.nist.gov/frvt/html/frvt11.html

National Institute of Standards and Technology [NIST]. (n.d.-b). *Face Technology Evaluations – 1:N Identification*. Retrieved July 30, 2025, from https://pages.nist.gov/frvt/html/frvt1N.html

National Institute of Standards and Technology [NIST]. (n.d.-c). *Face Technology Evaluations – Face in Video Evaluation (FIVE).* Retrieved July 30, 2025, from https://www.nist.gov/programs-projects/face-video-evaluation-five

National Institute of Standards and Technology [NIST]. (n.d.-d). *Face Technology Evaluations – FRTE/FATE*. Retrieved July 30, 2025, from https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile*. https://doi.org/10.6028/NIST.AI.600-1

National Policing Institute. (2021, October 22). *How to think about evaluating acoustic gunshot detection systems.* Data Science Blog. https://datascience.policefoundation.org/2021/10/22/acoustic-gunshot-detection-1/

National Urban Security Technology Laboratory [NUSTL]. (2023). *DeepZero gun detection platform technology report.* Department of Homeland Security. https://www.dhs.gov/sites/default/files/2023-01/22_0818_st_deepzero.pdf

NBC News. (2014, October 22). *Science of strangers: Military research could boost cops' people skills*. https://www.nbcnews.com/news/us-news/science-strangers-military-research-could-boost-cops-people-skills-n230951

Paul, A. (2023, February 10*). Police are paying for AI to analyze body cam audio for 'professionalism.*' Popular Science. https://www.popsci.com/technology/police-body-cam-ai-truleo/

Pinellas County Sheriff's Office. (n.d.). *Florida's facial recognition network*. Retrieved September 18, 2024, from https://www.nacdl.org/getattachment/d215b76f-0de0-4209-99ac-55e10d2582cc/1125_jowell_connectid-2014-fr-presentation.pdf

Phillips, H. (2023, February 16). *Livestreaming body cameras: 5 things to know about PBSO's cutting-edge new tech*. The Palm Beach Post. https://www.palmbeachpost.com/story/news/local/2023/02/16/5-things-to-know-about-pbso-sheriffs-office-axon-body-cameras-livestream-in-palm-beach-county/69905902007/

Police1 Staff. (2024, April 23). *Axon releases Draft One, AI-powered report-writing software*. Police1. https://www.police1.com/police-products/police-technology/software/report-writing/axon-releases-draft-one-ai-powered-report-writing-software

President's Task Force on 21st Century Policing. (2015). *Final report of the president's task force on 21st century policing*. https://www.govinfo.gov/content/pkg/GOVPUB-J36-PURL-gpo64136/pdf/GOVPUB-J36-PURL-gpo64136.pdf

Rainie, L., Funk, C., Anderson, M., & Tyson, A. (2022, March 17) *Public more likely to see facial recognition technology use by police as good, rather than bad for society*. Pew Research Center. https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/

Reed, M. (2025, January 23). *Daytona Beach OKs use of AI gun detection system along Seabreeze Boulevard*. WKMG News 6 & ClickOrlando. https://www.clickorlando.com/news/local/2025/01/21/daytona-beach-police-look-to-use-ai-gun-detection-system/

Rendon, A. (2025, June 17). *Central Texas cities cut license plate reader programs amid community criticism.* Spectrum News 1 San Antonio. https://spectrumlocalnews.com/tx/san-antonio

San Marcos Police Department. (n.d.). *Automated License Plate Readers (ALPR).* Retrieved July 30, 2025, from https://sanmarcostx.gov/4530/Automated-License-Plate-Readers-ALPR

Santos, M. (2023, February 14). *Seattle police stop using AI system to analyze bodycam footage*. Axios. https://www.axios.com/local/seattle/2023/02/14/seattle-police-truleo-artificial-intelligence

Schmidt et al v. City of Norfolk et al, No. 2:2024cv00621 - Document 29 (E.D. Va. 2025). (2024). https://law.justia.com/cases/federal/district-courts/virginia/vaedce/2:2024cv00621/562101/29/

Senate Bill 180. Signed. 2025 Utah Legislature. Regular. (2025). https://le.utah.gov/~2025/bills/static/SB0180.html

Senate Bill 262. Signed. 2023 Florida Legislature. Regular. (2023). https://laws.flrules.org/2023/201

Senate Bill 182. Signed. 446th session Maryland General Assembly. Regular. (2024). https://msa.maryland.gov/msa/mdmanual/07leg/html/sessions/2024.html

Senate Bill 282. Signed. 2025 Montana Legislature. Regular. (2025). https://legiscan.com/MT/text/SB282/2025

Senate Bill 562. Introduced. 2025 Florida Legislature. Regular. (2023). https://www.flsenate.gov/Session/Bill/2025/562/BillText/Filed/HTML

Senate Bill 1444. Introduced. 2025 Florida Legislature. Regular. (2025). https://www.flsenate.gov/Session/Bill/2025/1444/BillText/Filed/HTML

Senate Bill 1444. C1. 2025 Florida Legislature. Regular. (2025). https://www.flsenate.gov/Session/Bill/2025/1444/BillText/c1/HTML

Senate Bill 1680. Signed. 2024 Florida Legislature. Regular. (2024). https://flsenate.gov/Session/Bill/2024/1680/BillText/er/HTML

Senate Bill 1964. Signed. 89th Texas Legislature. Regular. (2025). https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=SB1964

Serrie, J., & Daigle, S. (2023, July 18). *Police departments across America using AI to analyze officers' bodycam video.* Fox News. https://www.foxnews.com/us/police-departments-america-using-ai-analyze-officers-bodycam-video

Sessions, K. (2024, January 26*). Houston Police body cameras will now record at all times, chief says*. Chron. https://www.chron.com/news/houston-texas/article/houston-police-body-cameras-18630451.php

Smith v. Maryland, 442 U.S. 735 (1979). https://www.oyez.org/cases/1978/78-5374

Stofan, J. (2024, April 4). *ShotSpotter alerts and violent crime trending down in Jacksonville early into 2024*. Action News Jax. https://www.actionnewsjax.com/news/local/areas-duval-with-shotspotter-technology-are-seeing-decrease-shootings-compared-last-year/A5DHPHZBTJADTM6EUXQVMNNQL4/

Stone, M. (2023, February 12). *School district deploys cutting-edge campus safety technology.* Hernando Sun. https://www.hernandosun.com/2023/02/12/school-district-deploys-cutting-edge-campus-safety-technology/

Stryker, C., & Scapicchio, M. (2024, March 22). *What is generative AI?* IBM. https://www.ibm.com/topics/generative-ai

United States v. Jones, 565 U.S. 400 (2012). https://www.oyez.org/cases/2011/10-1259

United States v. Knotts, 460 U.S. 276 (1982). https://supreme.justia.com/cases/federal/us/460/276/

United States v. Dionisio, 410 U.S. 1 (1973) https://supreme.justia.com/cases/federal/us/410/1/#tab-opinion-1950134

United States v. Miller, 425 U.S. 435 (1976). https://www.oyez.org/cases/1975/74-1179

Vallas, P. (2024, February 16). *Vallas: Fixing 4 myths about Chicago's gunshot detection technology*. Illinois Policy. https://www.illinoispolicy.org/vallas-fixing-4-myths-about-chicagos-gunshot-detection-technology/

Vickers, C. (2024, April 7). *How AI risks creating a 'black box' at the heart of US legal system.* The Hill. https://thehill.com/business/personal-finance/4571982-ai-black-box-legal-system/

Warren, D. (2023, July 18) *Rival US lawmakers mobilize to stop police from buying phone data.* Wired. https://www.wired.com/story/fourth-amendment-is-not-for-sale-act-2023/

WCTV Staff. (2023, October 24). *New AI gun detection system installed in Leon County High Schools.* WCTV. https://www.wctv.tv/2023/10/25/new-ai-gun-detection-system-installed-leon-county-high-schools/

Whiting, Z. & Dunmoyer, D. (2024). *Promise and Peril: How Texas Can Lead on Responsible Artificial Intelligence Policy.* Texas Public Policy Foundation. https://www.texaspolicy.com/wp-content/uploads/2024/11/2024-11-BTT-Responsible-AI-Policy-WhitingDunmoyer_FINAL.pdf

APPENDIX A

Acoustic gunshot detector (AGSD)	"ASGD systems triangulate the location of a gunshot by using a series of microphones mounted in areas throughout a city. These microphones pick up on the sound produced by a gunshot, and are subjected to a combination of automated software and human review to determine whether the triggering event was caused by a gunshot" (National Policing Institute, 2021 para. 2).
Artificial Intelligence (AI)	A term coined by emeritus Stanford Professor John McCarthy in 1955, was defined by him as 'the science and engineering of making intelligent "machines" (Manning, 2020, para. 2). "AI is a machine's ability to perform the cognitive functions we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem-solving, and even exercising creativity" (McKinsey & Company, 2024, para. 4).
Automatic License Plate Readers (ALPRs)	"Automated license plate recognition system" means a system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data (Section 316.0777, Florida Statutes).
Biometric Data	""Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs; video or audio recordings or data generated from video or audio recordings; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq" (Section 501.702 (4), Florida Statutes).
Black box problem	The black box "refers to artificial intelligence systems—particularly deep learning models—that make decisions without offering any insight into *how* they arrived at their conclusions" (Kelly, 2025, para. 3).
Body-worn Camera (BWC)	"'Body camera' means a portable electronic recording device that is worn on a law enforcement officer's person that records audio and video data of the officer's law-enforcement-related encounters and activities" (Section 943.1718 (1) (a), Florida Statutes).
Deep learning	"Deep learning is an artificial intelligence function that imitates the workings of the human brain in processing data and creating patterns for use in decision making. Deep learning is a subset of machine learning in AI that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Also known as deep neural learning or deep neural network" (CompTIA, n.d., p. 2). "Deep learning is a subset of machine learning that uses multilayered neural networks, called deep neural networks, to simulate the complex decision-making power of the human brain. Some form of deep learning powers most of the artificial intelligence (AI) applications in our lives today" (Holdsworth, & Scapicchio, 2024 para. 1).

Facial Recognition Technology	Facial recognition broadly involves the automated searching of a facial image (a probe) against a known collection or database of photos" (Finklea, Harris &, Kolker, 2020, para. 10).
Generative AI (GenAI)	"Generative AI refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on" (Martineau, 2023, para. 1). "EO 14110 defines Generative AI as 'the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.' While not all GAI is derived from foundation models, for purposes of this document, GAI generally refers to generative foundation models. The foundation model subcategory of 'dual-use foundation models' is defined by EO 14110 as 'an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts'" (NIST, 2024, p. 1, fn. 1; Exec. Order No. 14110, 2023, pp. 75194-75195).
Hallucination (Confabulation)	"'Confabulation' refers to a phenomenon in which GAI systems generate and confidently present erroneous or false content in response to prompts. Confabulations also include generated outputs that diverge from the prompts or other input or that contradict previously generated statements in the same context. These phenomena are colloquially also referred to as 'hallucinations' or 'fabrications'" (NIST, 2024, p. 6).
Machine Learning (ML)	"Machine learning is a branch of AI that allows systems to automatically process data and analyze for insights without being programmed explicitly. Machine learning is concerned with learning functions and patterns to do things like classification and prediction" (CompTIA, n.d., p. 2).
Natural language processing (NLP)	Natural language processing is a form of machine learning that allows computers to understand and communicate in human language (Stryker & Holdsworth, 2024).
One to One 1:1	"One-to-one verification algorithms compare a photo of someone claiming a specific identity with a stored image (s) of that known identity to determine if it is the same person" (Finklea et al., 2020, para. 10).
One to Many 1:N	"One-to-many identification search algorithms compare the features of a probe photo with all those in the gallery of images" (Finklea et al., 2020, para. 10).

ABOUT THE AUTHOR

Christian Cochran currently serves as Florida State Director for the Foundation's Right On Crime initiative. Cochran's policy and legislation experience came through a unique path, first serving as a Deputy Sheriff in the Florida panhandle and a Reservist in the United States Army Reserve. Cochran had his initial experience with legislation and policy as a two-year fellowship Wounded Warrior Fellow through the United States House of Representatives. This allowed him to spend time helping active-duty military and veterans. He then served as the Deputy Legislative Affairs Director for the Florida Department of Veterans Affairs. Before coming to Right on Crime, Cochran was Government Relations Manager for the Florida Court Clerks and Comptrollers.

Cochran graduated from Florida State University with a M.S. in Political Science, The Citadel Graduate College with an MBA, Liberty University with a M.S. in Criminal Justice Administration: Public Administration and a B.S. from Columbia Southern University in Criminal Justice Administration. He currently lives in Crawfordville, Florida, with his wife, Laura and daughter, Liberty Rose.

Texas Public Policy Foundation

Right On Crime

901 Congress Avenue | Austin, Texas 78701 | (512) 472-2700 | www.TexasPolicy.com