MITRE | Intelligence After Next

IAN SPECIAL SERIES: Artificial Intelligence

AI-1

ARTIFICIAL INTELLIGENCE APPLICATION APPROACHES FOR LAW ENFORCEMENT

by Eric Bloedorn, Travis Carlisle, Eric Hughes, and Jeffrey Parsons

Recent dramatic improvements in generative artificial intelligence (AI) capabilities have captured worldwide attention, and AI has become a major issue across the intelligence community (IC). While there is much to gain from AI in all its forms, there are myriad challenges and issues the IC must understand and address. As part of our ongoing Intelligence After Next paper series, we have created a special series to cover key topics in AI specifically in the context of the IC. This paper represents the first of the series.

Artificial Intelligence for Law Enforcement—A Challenging Environment

Law enforcement (LE) is one of the most challenging environments for the application of AI due to the complexities of laws, policies, and practices that must be complied with, as well as the intense public scrutiny that comes with technological advancements in this field. Nonetheless, AI has the potential to provide significant benefits in the LE domain, including enhanced analysis and optimization of information, improved efficiency and effectiveness, and increased compliance with legal and regulatory requirements.

Moreover, by partially automating administrative tasks, AI can help reduce the burden of paperwork and allow practitioners to focus on higher-value tasks.

As AI technology continues to evolve rapidly, the LE community has a vested interest in adopting these innovations incrementally, ensuring that human oversight and accountability remain paramount. The adoption of AI should not aim to replace the human element in policing and investigation; instead, the use of AI should seek to enhance the ability of LE to conduct its mission more efficiently and effectively. This concept is not new. In 1986 Dr. Robert E. Uhrig advocated for AI to be used as "expert systems" supporting complex decision-making processes by "capturing and disseminating human expertise and knowledge" to facilitate the safe and effective operations of nuclear power plants. He observed, "artificial intelligence is not a substitute for human intelligence, but rather a technology that complements and amplifies human capabilities."[1] Ultimately, the successful integration of AI into law enforcement holds significant promise in enhancing LE's ability to carry out its mission of protecting the American people.

To address these challenges, a phased approach to AI integration is recommended, starting with simpler, low-intrusive applications and gradually advancing to more complex and potentially intrusive uses. Early AI applications can assist in tasks like data analysis, real-time language translation, and administrative automation. Over time, more advanced uses, such as identifying previously undetectable patterns or criminal tradecraft, facial recognition, and semi-autonomous systems, could be adopted, provided legal and ethical frameworks are in place. This incremental adoption will allow law enforcement agencies to build trust with the public and ensure AI is used responsibly, in alignment with legal standards and ethical guidelines, while enabling law enforcement to keep pace with emerging technologies and evolving threats.[2]

As AI technology continues to evolve rapidly, the LE community has a vested interest in adopting these innovations incrementally, ensuring that human oversight and accountability remain paramount.

AI Applications for LE

Despite these challenges, there are several potential opportunities for additional experimentation and use of AI that can mitigate technical and legal barriers to LE application and align with the Department of Justice's (DOJ) Artificial Intelligence Strategy[3] and one of the Federal Bureau of Investigation's (FBI) three AI focus areas—the governance and ethical use of AI within the LE community.[4]

Criminal and national security threat actors will leverage AI wherever it benefits them. To effectively counter the resulting threats, LE will need to apply AI in a way that not only complies with laws and policies but also incorporates practical, proven approaches, ultimately fostering public trust. This eventual adoption of AI has the potential to significantly enhance the capabilities of LE agencies, improving efficiency and effectiveness across a spectrum of tasks, as listed below in Table 1. These AI applications vary in their level of technical difficulty and perceived investigative intrusiveness, impacting their implementation, societal, and judicial acceptance. However, the concept of "least intrusive methods" has long been a foundational principle in LE, guiding actions to minimize interference with privacy and civil liberties while maintaining public safety. The application of AI is an extension of this principle, as it can enhance existing legally authorized methods without introducing new levels of intrusion.

Table 1: AI Applications for Law Enforcement by Level of Difficulty and Intrusiveness[5]

Low Difficulty, Low Intrusiveness	**Data Analysis and Pattern Recognition:** AI algorithms excel at analyzing large data sets, identifying patterns and trends that might go unnoticed by human analysts. This can aid in resource allocation and identifying potential hotspots for crime.
	Administrative Tasks Automation: Automating routine administrative tasks such as report generation, data entry, and scheduling can free up valuable officer time for core duties.
	Real-Time Language Translation: AI-powered translation tools can facilitate communication between law enforcement and individuals who speak different languages, improving interactions and fostering trust.
Moderate Difficulty, Moderate Intrusiveness	**Facial Recognition and Biometrics:** AI-powered facial recognition systems can assist in identifying suspects, missing persons, or individuals with outstanding warrants. However, concerns about privacy, accuracy, and potential bias necessitate careful implementation and oversight.
	Social Media Monitoring and Sentiment Analysis: Analyzing social media content can provide insights into potential threats, public sentiment, and emerging trends. Balancing public safety with individual privacy rights remains a challenge.
	Body-Worn Camera and Surveillance Footage Analysis: AI can expedite the review of footage, flagging relevant incidents or behaviors for further investigation, while minimizing the manual effort required.
High Difficulty, High Intrusiveness	**Predictive Policing Algorithms:** Advanced AI models aim to predict future crime locations and potential offenders. Ethical concerns regarding fairness, transparency, and the potential for self-fulfilling prophecies demand careful consideration.
	Autonomous Vehicles and Drones for Surveillance: While offering enhanced surveillance capabilities, autonomous vehicles and drones raise concerns about privacy, oversight, and potential misuse.
	AI-Powered Interrogation and Deception Detection: AI-based lie detection systems, although promising in theory, face significant technical and ethical hurdles, with potential impacts on due process and individual rights.

Adoption of AI in the LE community risks lagging behind the private sector and the IC.[6] This reflects the unique U.S. federated model of policing compared with other countries. The United States, with about 18,000 separate law enforcement agencies (federal, state, local, and tribal),[7] faces significant challenges in adopting new technologies, protecting citizen rights, maintaining public trust, and ensuring budget resources are available to meet LE needs. These challenges are best categorized as data standardization, developing legal precedence, and the high threshold for transparency required in LE. In this context, the methods used to incorporate AI solutions are crucial to enhancing the LE community's ability to fulfill its mission.

> LE is one of the most challenging environments for the application of AI due to the complexities of laws, policies, and practices that must be complied with, as well as the intense public scrutiny that comes with technical advancements in this field.

Data Standardization

Well-structured, accessible data is the lifeblood of AI. Rephrased for the LE community, this concept is more simply understood as "garbage in, garbage out." LE organizations collect and examine vast quantities of data through their investigations. This data is obtained through diverse sources such as witnesses; legal process; open-source information; local, state, federal, tribal, and foreign partners; and confidential sources. Each data source is burdened with unique restrictions on its use, whether legal limitations required by Grand Jury secrecy (e.g., Federal Rules of Criminal Procedure 6(e))[8] or limited use necessary to protect sources and methods. Furthermore, data obtained from various providers inevitably is in non-standard formats. Finally, most LE organizations retain their data in case management systems that were not designed with data optimization as a priority. Each of these factors limits the ability of LE to fully leverage the advantages of AI.

Legal Precedence

The impact of future legal rulings on the incorporation of AI into LE is less certain. Legal guidance has historically trailed in addressing the balance between LE tactics and privacy as technology evolves.

- The 1967 Supreme Court Case Katz v. United States established that the FBI's warrantless wiretapping of public phone booths to listen to a suspect's conversations violated the Fourth Amendment's protection against unreasonable searches and seizures. The Court ruled that individuals have a "reasonable expectation of privacy" in their phone conversations, even in public spaces, thereby requiring law enforcement to obtain a warrant for such surveillance activities.[9]
- More recently, the 2018 Supreme Court Case Carpenter v. United States ruled that law enforcement agencies must obtain a warrant before accessing an individual's cell phone location data from wireless carriers.[10] The Court held that the Fourth Amendment protects this data because it provides a detailed and invasive record of a person's movements over time, thus requiring a higher standard of privacy protection. This landmark decision recognized the significant privacy concerns posed by modern technology and set a precedent for digital privacy rights in the age of widespread data collection.[11] This ruling specifically rebuked the government for "fail[ing] to contend with the seismic shifts in digital technology."[12]

Although the Carpenter decision does not directly address the use of AI, legal scholars have interpreted that it "hints that Fourth Amendment protections also turn on the nature of *policing* that produces the information at issue. … Carpenter recognizes, perhaps more so than any other

Supreme Court decision, that dramatic technological changes will rewrite the Fourth Amendment constraints on the government's powers."[13] This history of legal rulings aiming to balance LE tactics with citizen privacy rights must be considered as LE seeks to properly adapt AI into its methods.

Transparency

The LE community's authority is based on the trust and acceptance of its methods by the communities it polices. This principle dates to the founding of modern police methods by Sir Robert Peel in London in 1829. His initial principle of ethical policing recognized that "The ability of the police to perform their duties is dependent upon public approval of police … actions."[14] This 200-year-old statement is still relevant and especially applicable to the adoption of AI capabilities by LE. Unlike the private sector and IC, the methods employed by LE in its investigations are measured by the trust of the courts and a jury of a defendant's peers. This degree of scrutiny requires the use of AI by LE be transparent and public. When an LE official testifies to a conclusion in a court of law, their answer must be understandable, reasonable, and acceptable by the public. Simply stating "AI told us it was so" will not suffice for a suitable explanation.

> "The ability of the police to perform their duties is dependent upon public approval of police existence, actions, behavior and the ability of the police to secure and maintain public respect."
>
> – Sir Robert Peel, founder of the London Metropolitan Police.

Phased AI Implementation

Adopting AI in phases enables organizations to build and develop initial experiments and applications incrementally, paving the way for more sophisticated applications in the future. This strategy allows teams to establish best practices, address legal and technical hurdles, and create a solid foundation for future advancements. LE organizations will need to be committed to advancing the responsible use of AI, adhering to the guidelines set forth by the U.S. government and DOJ regarding ethical and legal considerations. AI applications must be designed to meet these standards, ensuring they align with national priorities and values while protecting individual rights and promoting public trust. In all phases, AI use must be compliant with applicable policy and investigative authorities conforming to federal, state, local, and tribal AI safeguards.

Initial Phase

This phase would start with AI applications that have limited legal and technological complications but have significant potential to enhance analysis and investigations. This includes applications that are in place today. This initial phase will identify necessary changes to information technology (IT) infrastructure to establish proper ethical standards for AI adoption, in addition to initial policy and legal challenges. Additionally, these early AI experiments and applications will begin the process of familiarizing the LE community with AI and developing lessons learned to be incorporated into future developments. Examples of initial AI applications include:

- Application of assisted metadata "tagging" to draft investigative or intelligence documents, such as investigative case classifications, crime indicators,[15] criminal intelligence requirements, intelligence gaps, and key intelligence questions, using standard formats and drawing on structured data sets
- Preparation of draft investigative reports, such as case openings, closings, or summaries, utilizing standard formats based on identified predicating documents
- Preparation of draft affidavits and/or legal process utilizing standard formats based on identified predicating documents

- Preparation of draft criminal intelligence products, such raw and finished analytical products, based on identified facts and predicating documents

Mid-Term Phase

The development of experiments and applications in the mid-term phase would build on the progress from the initial applications and legal guidelines to more fully realize the benefits of AI capabilities. This phase would continue to evolve architectural improvements, including data conditioning and cleaning, in conjunction with policy modifications needed to fully realize AI's potential, while beginning to formalize legal guidelines. These applications will be designed to serve as an assistant to the investigator or analyst by efficiently identifying patterns, commonalities, or sophisticated insights not obvious to human review.

> The ultimate objective of this phased process will be to incrementally adopt increasingly advanced AI technology into LE systems to allow the workforce to more efficiently and effectively exploit data to accomplish the core mission of protecting the American people.

Telephone toll records, social media contacts, internet protocol history, or financial records, for example, could be used to identify patterns in activity and unknown nodes of interest. AI methods could be used to identify new connections; investigative or intelligence gaps in a case file; or trending threats and/or targets appearing in public complaints, investigative results, and confidential informant and criminal intelligence reporting. Examples of mid-term AI applications include:

- Confirmation that the facts included in a document, such as an affidavit or case closing, are consistent with facts included in an identified case file or specific identified records
- Triage of large data sets obtained via consent or legal process responsive to identified prompts
- Application of machine learning (ML) to voluminous public complaint line (i.e., tip line) data to rapidly triage and prioritize credible threats to the public for LE review and interdiction
- Facilitation of safety and compliance in operational plans (OPLAN) by drawing on previous after-action reports, lessons learned, and best practices—all with human review in overall risk assessment and mitigation; generate OPLAN scenario planning and simulations to consider different strategies and identify potential weaknesses or areas of improvement; and optimize resource allocation for planning and execution

Long-Term Phase

The long-term objective will be to quickly identify emerging or unknown criminal activity, threats, or intelligence gaps, with reduced bias and increased effectiveness and efficacy. Once the necessary IT infrastructure and legal concerns have been addressed in earlier phases, AI can be employed to provide an independent analysis[16] of LE organizations' vast data holdings, looking for previously unknown indicators of crimes or threats, including examples such as:

- Identifying instances of known threat actors employing intelligence or criminal tradecraft from analysis across internal LE and publicly available data sets
- Identifying previously unknown criminal tradecraft by detecting new patterns in large data sets
- Generating potential leads for review by investigators and analysts (consistent with LE organizational and DOJ policies and authorized purpose)
- Identifying individuals of interest or topics for investigation through continuous authorized review of LE data

This phased approach will reduce administrative burden and enhance investigative efforts while laying the groundwork for future AI applications. Beginning with applications that are less complicated will permit the incremental understanding of which policies or existing IT structures need to be updated to further adopt more advanced applications. The phased approach will also allow the LE workforce to adapt to the new technology and organically propose new features and lessons learned to inform future innovations. Figure 1 depicts an example investigative scenario illustrating traditional versus AI-augmented investigative methods.

This approach also facilitates education of, acceptance by, and guidance for elected officials and the judiciary regarding the ethical and lawful use of AI. By doing so, it supports the establishment of good legal precedent and safeguards civil rights as AI applications continue to expand. The ultimate objective of this process will be for LE systems to incrementally adopt increasingly advanced AI technology to allow the workforce to more efficiently and effectively utilize data to accomplish the core mission of protecting the American people.

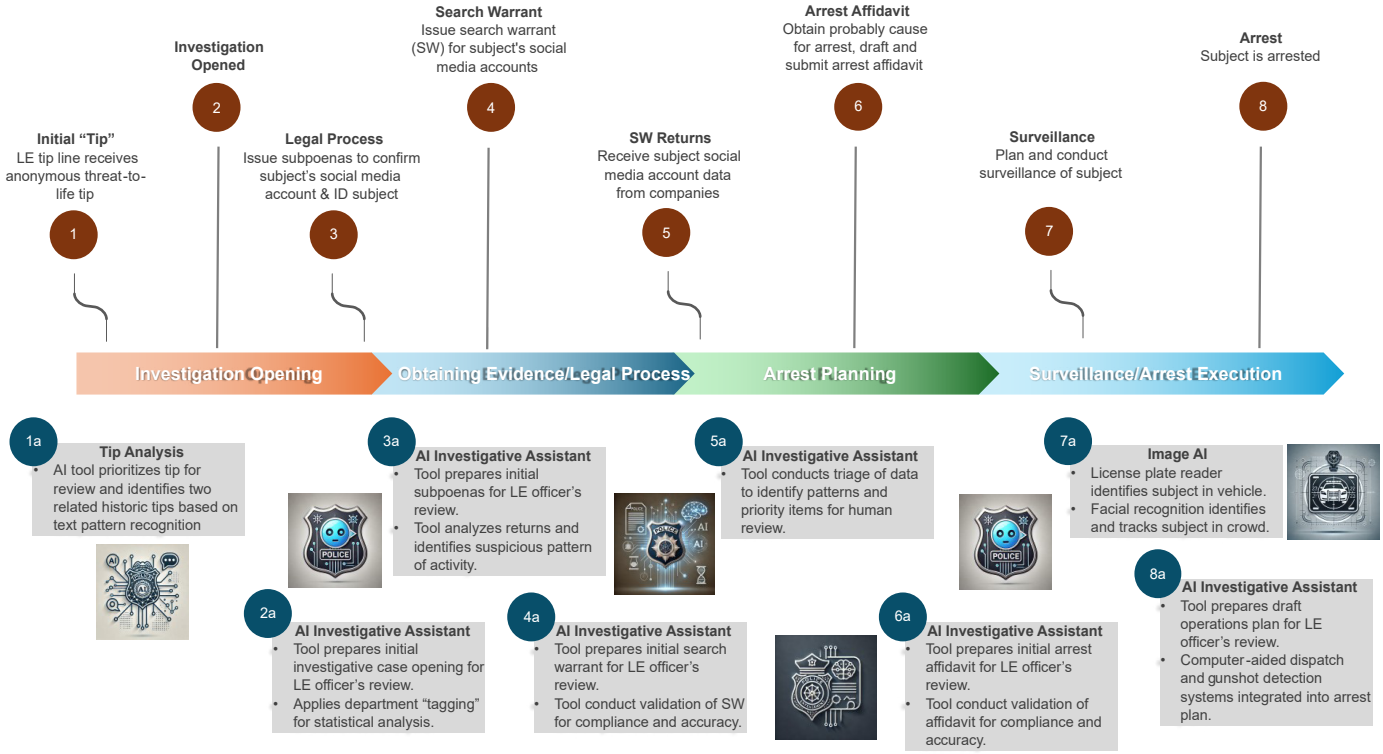

Figure 1: Example Investigative Scenario Depicting Traditional Versus AI-Augmented Investigative Methods

Barriers and Ways to Overcome Them

Assurance of AI[17] will require clearly defined guidelines for LE use, as with any other technology, including:

- AI should be used in a manner that respects individual privacy rights and civil liberties.
- Output from AI should be interpreted/actioned only by trained staff (i.e., humans are always "in the loop").
- AI should never be used to broaden LE collection authorities.
- AI use should conform to established investigative guidelines.
- AI should not modify or eliminate official records.
- Use and policy of AI applications should be transparent to ensure the public's trust.

AI must demonstrate value and trustworthiness. In LE, the volume and velocity of digital and multimedia evidence can overwhelm human review. Unexploited or underexploited data poses an unacceptable risk. AI can be used to locate pertinent content using, for example, improved sorting, filtering, and information retrieval, and to understand content through techniques like information extraction, categorization, and semantic analysis. What is important is for each application to show value over time, starting with narrowly constrained uses and continuously testing and experimenting with broader applications to ensure their trustworthiness. Some examples include:

- The overly broad use of AI systems to analyze and interpret biodata may invade privacy or suppress freedoms of speech and assembly.

  Mitigations: Maintain a minimum level of awareness of where and how AI-enabled systems are being used across the LE organization. Conduct risk and impact assessments. Limit data collection and retention. Use techniques like differential privacy and federated learning. Provide transparency. Strengthen oversight. An example of these mitigations in practice is the FBI's AI ethics council, which "helps the FBI identify, review, and assess new and existing AI deployed and operating in support of agency missions."[18]

- The "black box" nature of some AI systems makes it difficult to understand how recommendations or decisions are reached. This can reduce accountability and trust.

  Mitigations: Have AI-enabled systems and applications use more interpretable models where feasible. Conduct algorithmic audits. Provide and require standardized documentation for transparency into each AI-enabled system's policies and accuracy. Implement human-in-the-loop reviews. Establish robust instrumentation. Continuously monitor and analyze the AI capability in operation (not "approval to operate and done"). As an example of these mitigations, the financial sector regulatory framework of Model Risk Management is a good starting point.[19] This includes "sociotechnical sensors"—ways to measure and report on the impacts of the system to individuals, groups, and society.

- Errors or bias in AI systems used in investigations or as evidence in trials could violate rights to contest decisions made against individuals.

  Mitigations: Ensure public notice of AI use is provided. Prioritize transparency documentation and enable auditing of AI-enabled systems. Review policies on redress. Issue guidance on AI's role in due process. Formulate policies to ensure corroboration of AI products via independent methods. An example of these mitigations is DOJ's published AI Use Case Inventory, publicly available on its homepage.[20]

- Models trained on historical crime data may amplify biases and disparate impacts on marginalized groups.

  Mitigations: Establish clear definitions of bias and fairness in AI-enabled systems. Iteratively assess and mitigate bias risks during both development and deployment. Continuously evaluate model fairness. Implement controls like human-in-the-loop reviews. LE organizations can establish clear and systematic procedures for broad stakeholder engagement from the start through operations. Some tools for participatory design to facilitate responsible AI governance are available, such as from Google and the Partnership on AI in the public interest.[21, 22]

To comply with any AI-focused federal guidance, as well as other U.S. government AI initiatives, LE organizations can take proactive steps. Specifically, they can assess AI applications for potential safety and civil liberty impacts using the approaches outlined here. Those identified as having significant impact can be prepared for public notice where appropriate. Additionally, LE organizations can utilize AI expertise to assess applications of foundation models and generative AI technologies like ChatGPT.

To effectively utilize AI, organizations need to cultivate organizational maturity in AI development and implementation. This requires thinking beyond buying new hardware or hiring AI engineers. For example, LE organizations must establish protocols for safe and ethical AI development and deployment, safeguard against novel attack pathways and vulnerabilities that AI integration may introduce, and formulate policies and monitoring processes for AI system authorization and oversight. It is important to note, however, that these issues need not all be solved before any progress on AI can be achieved. A good roadmap will look for opportunities to make the organization stronger incrementally along these dimensions while simultaneously building capability to support a specific need. Broad categories of topics that should be included in a roadmap for organizational AI maturity include:

- Strategy and resources
- Organization and workforce
- Technology enablers
- Data management
- Ethical, equitable, and responsible use
- Performance and application

Finally, LE organizations can build AI roadmaps that document the value proposition, as well as when, who, and how capabilities will be developed, tested, deployed, and sustained. Reaching the necessary level of AI maturity to meet mission demands and get in front of criminal and adversary AI use will be a multi-step process. The LE community can build on lessons learned from these efforts rather than starting new efforts from scratch. Focusing on both what worked and what barriers still exist will be vital to informing future efforts and guiding where to put resources to address potentially long-lead-time problems like policy or hiring. AI efforts like those that rely on ML models need to have a much larger sustainment tail than traditional software development because they must collect and curate both the feedback and models. LE organizations will need to establish governance processes, as well as standards for developing and documenting AI capabilities, to ensure AI is used correctly and in compliance with laws and policies.

Embracing AI to Protect the Public

While the complexities and challenges of incorporating AI into law enforcement are substantial, these should not serve as a deterrent to its adoption; rather, they highlight the need for a carefully considered, incremental approach. The potential benefits of AI, including enhanced analytical capabilities, improved efficiency, and more effective use of resources, are too significant to ignore, especially as LE faces increasingly sophisticated threats that leverage advanced technologies. By implementing AI gradually and thoughtfully, LE agencies can address the technical, legal, and ethical hurdles that come with these innovations, ensuring that AI enhances rather than undermines their mission.

Moreover, adopting AI incrementally allows agencies to build trust with the public and maintain transparency, both of which are crucial given the unique responsibilities of law enforcement in a democratic society. A phased approach ensures that the use of AI remains aligned with legal standards and ethical guidelines, fostering public trust and accountability. As criminal and national security threats continue to evolve, failing to integrate AI into LE practices is not a viable option. Instead, LE agencies must actively embrace AI technologies to enhance their ability to protect public safety, adapt to the modern landscape of crime and threats, and uphold justice in a manner that respects civil liberties and privacy.[23, 24]

References

1. R. E. Uhrig. "Toward the Next Generation of Nuclear Power Plants," Forum, 1(3), Fall 1986, p. 26. *Available:* https://www.google.com/books/edition/Forum_for_Applied_Research_and_Public_Po/-0vIhNJm3YIC?hl=en&gbpv=1&dq=%22Artificial+intelligence+is+not+a+substitute+for+human+intelligence%22&pg=RA2-PA26&printsec=frontcover
2. This document includes content generated with the assistance of ChatGPT 4o, a generative AI tool and hosted by OpenAI. ChatGPT 4o was used to assist in writing the executive summary of this paper. The authors have reviewed and edited all AI-generated content to ensure accuracy, following MITRE's generative AI use guidelines
3. U.S. Department of Justice, Office of Chief Information Officer. Artificial Intelligence Strategy for the U.S. Department of Justice. December 2020. *Available:* https://www.justice.gov/d9/pages/attachments/2021/02/04/doj_artificial_intelligence_strategy_december_2020.pdf
4. The three FBI AI focus areas are collecting intelligence about and identifying and tracking adversarial use of AI, protecting AI innovation in the private sector and academia, and governance and ethical use of AI within the LE community. See Artificial Intelligence, Artificial Intelligence (AI) Has Implications Not Just for the Commercial Sector but for National Security and Law Enforcement. FBI.gov. Accessed: September 4, 2024. *Available:* https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence
5. This document includes content generated with the assistance of ChatGPT 4o and Gemini Advanced, generative AI tools hosted by OpenAI and Google. ChatGPT 4o and Gemini Advanced were used to generate the initial draft of Table 1, drawing on prompts and materials in this paper. The authors have reviewed and edited all AI-generated content to ensure accuracy, following MITRE's generative AI use guidelines.
6. K. Finklea. "Law Enforcement Use of Artificial Intelligence and Directives in the 2023 Executive Order," Congressional Research Service (CRS) Insight IN12289, December 2023. *Available:* https://crsreports.congress.gov/product/pdf/IN/IN12289
7. A. Cheatham and L. Maizland. "How Police Compare in Different Democracies," Council on Foreign Relations (CFR) Backgrounder, March 2022. *Available:* https://www.cfr.org/backgrounder/how-police-compare-different-democracies
8. C. Doyle. "Federal Grand Juries: The Law in a Nutshell," Congressional Research Service (CRS) RS20214, May 2015. *Available:* https://crsreports.congress.gov/product/pdf/RS/RS20214/11
9. Supreme Court of the United States. Katz v. United States, 389 U.S. 347, No. 35. 18 December 1967. *Available:* https://supreme.justia.com/cases/federal/us/389/347/#:~:text=Katz%20v.%20United%20States:%20It%20is%20unconstitutional%20under%20the%20Fourth
10. Supreme Court of the United States. Carpenter v. United States, 585 U.S. 296, No 16-402. 22 June 2018. *Available:* https://supreme.justia.com/cases/federal/us/585/16-402/#:~:text=Argued:%20November%2029,%202017.%20Decided:%20June%2022,%202018.%20Justia%20Summary
11. This document includes content generated with the assistance of ChatGPT 4o, a generative AI tool and hosted by OpenAI. ChatGPT 4o was used to assist in writing the summaries of both the Katz and Carpenter Supreme Court cases. The authors have reviewed and edited all AI-generated content to ensure accuracy, following MITRE's generative AI use guidelines.
12. Supreme Court of the United States. Carpenter v. United States, 585 U.S. 296, No 16-402. 22 June 2018. *Available:* https://supreme.justia.com/cases/federal/us/585/16-402/#:~:text=Argued:%20November%2029,%202017.%20Decided:%20June%2022,%202018.%20Justia%20Summary
13. E. Joh. "Artificial Intelligence and Policing: Hints in the Carpenter Decision," Ohio State Journal of Criminal Law, August 2018. *Available:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3238212#:~:text=But%20the%20Carpenter%20decision%20reveals%20the%20Supreme%20Court%E2%80%99s%20first%20set
14. Robert Peel. "Principles of Law Enforcement," in C. Reith, A New Study of Police History, London, UK: Oliver and Boyd, 1956, p. 287.

15. M. Berzofsky, K. Barrick, T. Scott, E. L. Smith, and C. Barnett-Ryan. Indicators for Crime Estimates Using NIBRS Data. Department of Justice, Bureau of Justice Statistics, and Federal Bureau of Investigation Criminal Justice Services Division, September 2022. *Available:* https://bjs.ojp.gov/content/pub/pdf/iceunibrsd.pdf

16. Independent analysis only done within respective agency policies and procedures still requiring human review and validation.

17. C. Clancy, D. Robbins, O. Eris, L. Booker, and K. Enos. A Sensible Regulatory Framework for AI Security. The MITRE Corporation, McLean, VA, Doc. 23-1943, 2023. *Available:* www.mitre.org/news-insights/publication/sensible-regulatory-framework-ai-security.

18. The "AI Ethics Council helps the FBI identify, review, and assess new and existing AI deployed and operating in support of agency missions. FBI's Privacy and Civil Liberties Unit within the Office of General Counsel is responsible for, among other things, providing legal advice and counsel on compliance with federal law protecting individual privacy, and best practices to achieve an appropriate balance between protecting civil liberties and facilitating FBI activities." See Government Accountability Office (GAO). Facial Recognition Services (GAO-23-105607). 2023, p. 30. *Available:* https://www.gao.gov/assets/830/828859.pdf

19. D. Blackburn. MITRE's Response to the NTIA RFI on Artificial Intelligence Accountability. The MITRE Corporation, McLean, VA, Doc. 22-01891-21, 2023. *Available:* https://www.mitre.org/sites/default/files/2023-06/PR-22-01891-21-MITREs-Response-to-the-NTIA-RFI-on-Artificial-Intelligence-Accountability.pdf

20. Department of Justice. 2023 DOJ AI Use Case Inventory. 14 July 2023. *Available:* https://www.justice.gov/open/file/1305831/dl?inline

21. L. Richardson. "How We're Partnering with the Industry, Governments and Civil Society to Advance AI." Blog.Google. Accessed: September 20, 2024. *Available:* https://blog.google/technology/ai/google-ai-partnerships-government-industry-civil-society/

22. About Us, Advancing Positive Outcomes for People and Society. Partnershiponai.org. Accessed: September 20, 2024. *Available:* https://partnershiponai.org/about/

23. This document includes content generated with the assistance of ChatGPT 4o, a generative AI tool and hosted by OpenAI. ChatGPT 4o was used to assist in writing the conclusion of this paper. The authors have reviewed and edited all AI-generated content to ensure accuracy, following MITRE's generative AI use guidelines.

24. This document includes content generated with the assistance of ChatGPT 4o, a generative tool and hosted by OpenAI. ChatGPT 4o was used to assist in editing and providing suggestions for concise language to this paper. The authors have reviewed and edited all AI-generated content to ensure accuracy, following MITRE's generative AI use guidelines.

Authors

Dr. Eric Bloedorn is the Chief Scientist of the Global Intelligence Division at MITRE. Previously, he developed AI applications for numerous U.S. government agencies. He is now responsible for promoting the responsible and effective use of AI for national security sponsors and is currently focusing on helping assess and improve organizational AI maturity.

Travis Carlisle is the Department of Justice Program Coordinator in Law Enforcement and Domestic Security (LEADS) at MITRE. He previously served in the FBI as a Special Agent and, prior to that, in the U.S. Army as an enlisted soldier and Military Intelligence Officer.

Dr. Eric Hughes is the Chief Engineer of the Global Intelligence Division at MITRE. He is responsible for technical quality and strategy for the division, including application of AI.

Jeffrey Parsons is a Systems Engineering Principal in LEADS at MITRE. He previously served in the FBI as a Special Agent investigating counterintelligence and counterterrorism matters. Prior to the FBI, he served in the U.S. Navy as a Surface Warfare Officer.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

FEBRUARY 2025