Government Business Council

ISSUE BRIEF

Enforcement on the Edge

Artificial Intelligence and Machine Learning in Federal Law Enforcement

TD SYNNEX Public Sector

Red Hat

THE BIG PICTURE

Federal law enforcement agencies are consistently on the lookout for innovation that can help protect American citizens and borders. These activities are becoming increasingly field-based, which in turn demands that rapid analysis of the information gathered must move to the edge too. As artificial intelligence (AI) and machine learning (ML) technologies become increasingly sophisticated and customizable, these agencies are looking to leverage the power of data to help inform decision-making.

WHY IT MATTERS

Artificial intelligence and machine learning tools at the edge can respond faster, save money, and ultimately support the mission of law enforcement by allowing them near-real time analysis of a much larger cache of data. Decisions can be made at both the individual and policy level with a greater degree of certainty based on the information available, with higher accuracy and efficiency.

ARTIFICIAL INTELLIGENCE IN FEDERAL GOVERNMENT

The federal government has recognized the urgent need for a defined and ambitious artificial intelligence strategy, and is beginning to take serious steps towards integrating AI/ML policy and practices within its agencies. Among other initiatives:

The National Artificial Intelligence Initiative Office, established in 2021, sits within the White House Office of Science and Technology and works to support the initiative's six strategic pillars, including improving transparency around how federal agencies are using the technology.[1] The White House is also soliciting public feedback about the design and creation of a National Artificial Intelligence Research Resource (NAIRR).[2]

The National Security Commission on Artificial Intelligence's 2021 final report highlights the wide landscape of potential offered by investments in artificial intelligence, as well as the consequences of not maintaining an advantage over adversaries.[3]

The December 2020 Executive Order promoting the use of trustworthy artificial intelligence within government agencies has led to several agencies, including the Department of Veterans Affairs, to share AI use cases and best practices.[4]

In 2020, the General Services Administration implemented machine learning support for agency regulatory reviews.[5]

ARTIFICIAL INTELLIGENCE WITHIN FEDERAL LAW ENFORCEMENT

This push for innovation using AI and ML has particular resonance for federal law enforcement agencies. From policing small cities to Customs and Border security, the future is in data-driven police work. Federal agencies, including the Department of Justice (DOJ) and Department of Homeland Security (DHS), are leading the way.

DOJ AI/ML PRIORITIES

The DOJ Office of the Chief Information Officer's AI Strategy focuses on:

- **Cultivating an AI-informed and ready workforce.**
- **Fully incorporate AI-specific factors with the DOJ Data Strategy framework.**
- **Develop standardized AI policies and practices across the Department.**
- **Accelerate adoption of technologies where appropriate.**

The DOJ has already invested or expressed interest in a number of AI/ML capabilities, including facial recognition software, machine learning tools to track mobile messaging sites, and biometric tools.

DHS AI/ML PRIORITIES

The DHS Science and Technology Directorate (S&T) released their Artificial Intelligence & Machine Learning Strategic Plan in August 2021, with three key strategic goals:

1. **drive next-generation AI/ML technologies for cross-cutting homeland security capabilities;**
2. **facilitate the use of proven AI/ML capabilities in homeland security missions;**
3. **build an interdisciplinary AI/ML-trained workforce.**

The Plan emphasizes both the force multiplying effect of AI/ML for DHS operations, as well as the need to operate within strict ethical guidelines.

> The potential impacts from AI on the security of the homeland and upon our Department's operational activities—both positive and negative—make it imperative for DHS to take a proactive role in the use of AI systems and to contribute to the national conversation on the secure use of this transformative technology.
>
> **— DHS AI Strategy**[7]

ON THE EDGE: AI/ML IN THE FIELD

One potentially critical arena of AI/ML interventions for federal law enforcement is on the edge. The shift to cloud-based or hybrid cloud data networks that are accessible remotely opens possibilities for improved law enforcement outcomes, from the rapid identification of a criminal, to real-time information about the movements of smugglers, to ability to search cameras or other data in public places for victims of human trafficking.

DATA SHARING

Flexibility about data sharing and access plays a crucial role in responding at speed, particularly for multi-jurisdictional federal agencies. Real-time crime centers (RTCCs) are becoming more popular within cities, relying on open source and cloud technologies that are rapidly deployable and interoperable between tools and agencies, including federal. More broadly, cloud and AI technologies offer the possibility of collaborative or shared databases from which multiple agencies can pull data, even in the field, allowing officers to quickly assess situations and make identifications.

USE CASE

CUSTOMS AND BORDER PROTECTION ON THE EDGE

Enforcing border protection along the waterways that separate the United States and Canada has historically been a high-stakes guessing game. Catching drug runners or smugglers relied on accurately predicting when and where criminal activity would take place, and Border Patrol officers could only search suspicious vessels when they crossed paths.

The Northern Border Remote Video Surveillance System (NBRVSS) changed that. NBRVSS has 22 sites of high-resolution cameras and radar strategically placed along the waterways. The custom software detects, monitors, and analyzes traffic patterns and vessel movements, and notifies CBP when it detects anomalies or vessels entering alert areas. Border Patrol ships can then be dispatched to investigate. The cameras can also zoom in on the ships, allowing law enforcement to have a clearer idea of the situation they're entering. This data is shared in partnership with the Canadian border police, substantially improving the efficiency, accuracy, and safety of CBP at the edge.[8]

ON THE EDGE: AI/ML IN THE FIELD

One potentially critical arena of AI/ML interventions for federal law enforcement is on the edge. The shift to cloud-based or hybrid cloud data networks that are accessible remotely opens possibilities for improved law enforcement outcomes, from the rapid identification of a criminal, to real-time information about the movements of smugglers, to ability to search cameras or other data in public places for victims of human trafficking.

BIOMETRICS

Being able to provide rapid and correct identification is a significant opportunity of AI/ML technologies within federal law enforcement. From Customs and Border Patrol, who can use biometric technologies to more quickly process passengers arriving and departing at the border, to handheld fingerprint scanners that can assist law enforcement officers in the field, to the more controversial use of facial recognition software, AI/ML technologies are able to rapidly trawl vast amounts of biometric data to bring information to the edge at speed.

USE CASE

FBI AND THE BIOMETRICS OF CRIME

The FBI's long-piloted Next Generation Iris Identification (NGII) launched in October 2020. The program is an automated biometrics service, using a near-infrared camera to capture and immediately match an iris against a database with a 98 percent accuracy rate. Now, the Bureau is developing an AI tool that will assist in recognizing fingerprints that have been deliberately altered to hide the owner's identity, as well as a full-palm scanner that keeps the palm and fingerprints together as one. Both of these tools would build out the biometric profile of suspected law-breakers, and ensure that law enforcement is able to rapidly match persons of interest with any files already in the system much faster than previously possible.[9]

COMPLIANCE AND ACCOUNTABILITY

But the landscape of artificial intelligence and machine learning also involves risk and the possibility of overreach. There have already been calls from lawmakers to ban some facial recognition technology currently used by federal agencies, citing bias and privacy concerns, including some that have led to wrongful arrests.[10]

In part to address some of these rising issues, the Government Accountability Office (GAO) released an Accountability Framework for federal agencies. The Framework addresses four key principles of governance, data, performance and monitoring, with best practices outlined under each principle. The December 2020 Executive Order on Transparency also mandates that federal agencies "must therefore design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, civil liberties, and American values."[11]

Some federal agencies have already considered accountability within their strategies. The DHS AI/ML Strategic Plan, for instance, incorporates compliance measures around privacy, bias, and trust within the development phase, and specifically references "trustworthy" AI. Maintaining public trust in federal agencies' use of AI/ML technology is key to building the safer future these agencies are looking to create.

HARNESSING THE POWER OF DATA

Artificial intelligence and machine learning technologies are more than simple tools — they open up a new world of possibilities to ensure public safety. From saving victims of human trafficking, to identifying opioid dealers online, to stopping terrorists at the border, harnessing the power of data to identify people and patterns that might be dangerous serves federal law enforcement agency missions of protecting the homeland and the people within it. Equipping officers in the field and on the edge with these technologies is often more cost-effective, accurate, and efficient, letting a program automate the data search and allowing them to focus on making the right decision at the right time. As long as these agencies comply with critical ethical and governance frameworks, AI/ML technologies have the chance to reshape the future of security.

Government Business Council

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights.

Red Hat

TD SYNNEX Public Sector

ABOUT RED HAT

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

Learn more at redhat.com/government.

ENDNOTES

1. https://www.fedscoop.com/naiio-launches-ai-website/
2. https://www.fedscoop.com/national-ai-research-resource-input/
3. https://www.nscai.gov/wp-content/uploads/2021/03/Final_Report_Executive_Summary.pdf
4. https://www.fedscoop.com/trustworthy-ai-use-case-sharing/
5. https://www.fedscoop.com/machine-learning-regulatory-reviews/
6. https://www.dhs.gov/sites/default/files/publications/21_0730_st_ai_ml_strategic_plan_2021.pdf
7. https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf
8. https://www.cbp.gov/frontline/cbp-artificial-intelligence
9. https://www.afcea.org/content/fbi-upgrades-biometric-technologies
10. https://www.rand.org/pubs/perspectives/PEA862-1.html
11. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/