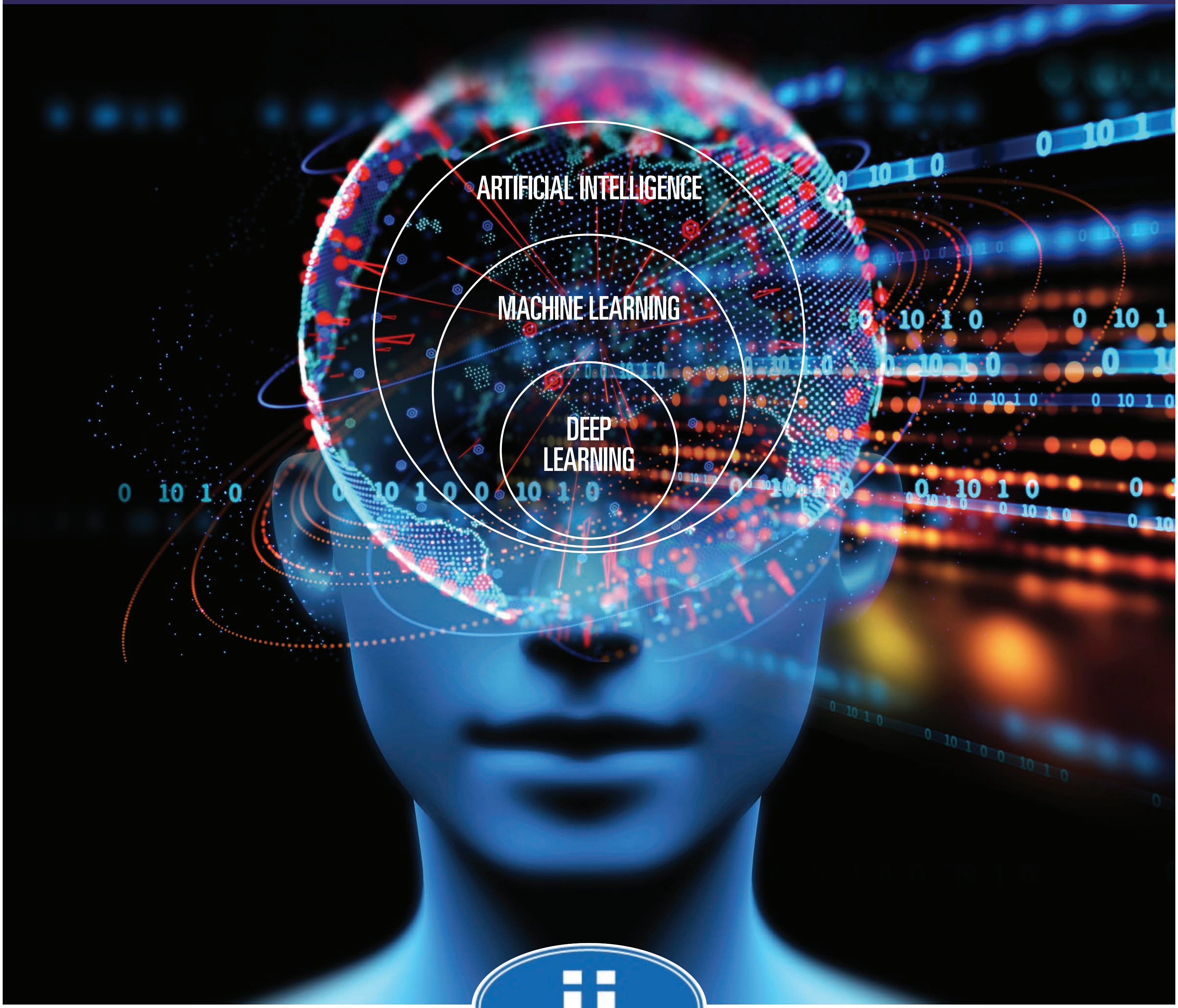
IJIS TECHNOLOGY AND ARCHITECTURE COMMITTEE (ITAC)



IJIS Institute

Artificial Intelligence in Justice and Public Safety

WHITE PAPER

Acknowledgements

This document is a product of the IJIS Institute, a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity. The IJIS Mission is to drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

IJIS Technology and Architecture Committee

Tom Carlson
Tom Carlson Consulting

Collin Evans
Analysts International Corporation

Jim Harris
National Center for State Courts

Bob Kaelin
MTG Management Consultants L.L.C.

Dave McClure
Justice Policy Center

Steve O’Connor
NG9-1-1 and Communications Center Operations

Anil K. Sharma
IBM

Iveta Topalova
Microsoft

Gerald L. Ward
MTG Management Consultants L.L.C.

Cory Woods
County of Nevada

Additional Contributors

Abhijeet Chavan
Tyler Technologies

Chris Thomas
Marquis Software

Fred Roesel
Marquis Software

Comments and Questions

Your comments and questions are welcome. Please contact the IJIS Institute at **info@ijis.org** or 1-703-726-3697.

Table of Contents

Table of Figures

1 | Introduction

The IJIS Institute's Technology and Architecture Committee (ITAC) provides information to industry and government practioners regarding technologies, architectures, and standards that enable the successful adoption of the technology and sharing or enterprise use of information. Artificial Intelligence / Machine Learning / Deep Learning are a collection of related technologies that provide great benefits to the criminal justice (i.e., Law Enforcement, Corrections, Courts), homeland security, and public safety domains (i.e., Fire, Emergency Management Services). ITAC developed this position paper on these technologies to benefit our practitioners in these domains.

The organization of this paper is as follows:

- **Section 2** provides a basic understanding of these new and emerging technologies as concepts;
- **Section 3** presents ongoing work within the public sector space with respect to this new technology;
- **Section 4** presents a small number of use cases in the criminal justice, homeland security, courts, and public safety domains;
- **Section 5** discusses benefits of this new technology;
- **Section 6** presents possible deployment/implementation options to include cloud and on-premise options;
- **Section 7** discuss data and information needs that should be considered with respect to this new technology;
- **Section 8** provides issues and considerations of this new technology in the criminal justice, homeland security, courts, and public safety domains;
- **Section 9** discusses ITAC's position regarding this new technology.

2 | Artificial Intelligence / Machine Learning / Deep Learning: What are they?

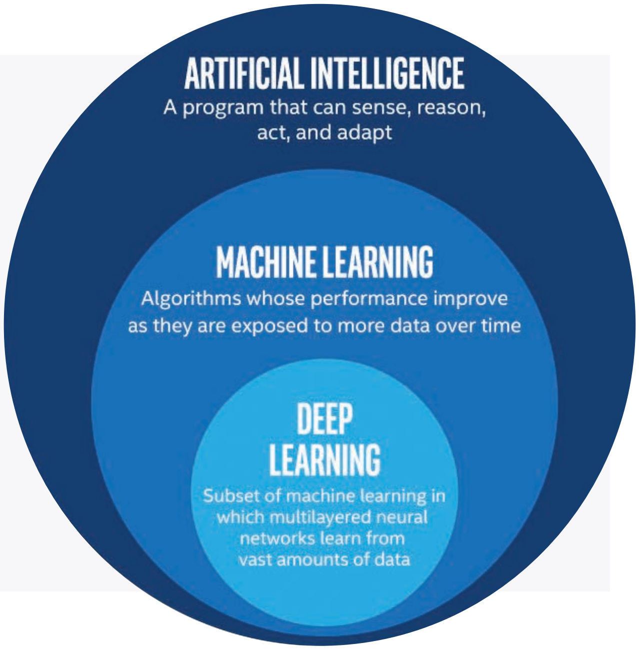
Artificial Intelligence (AI) is the theory and development of computer systems that perform tasks normally requiring human intelligence. This specifically refers to actions based on information presented to them over time. In other words, learning from the data that the system processes. These actions include logical deduction and inference, creativity, visual perception, decision-making, the ability to make decisions based on past experience or insufficient or conflicting information, and the ability to understand spoken language (Lexico.com: Artifical Intelligence n.d.).

Machine Learning (ML) is a method of data analysis that automates analytical model building. It is a branch of AI where systems can learn from data, identify patterns, and make decisions with minimal human intervention (“Machine Learning: What It Is and Why It Matter.” SAS. Accessed November 5, 2019.).

Deep Learning (DL) is a subset of machine learning where artificial neural networks, algorithms inspired by the human brain, learn from large amounts of data (Singh, 2017).

Figure 1

Artificial Intelligence / Machine Learning / Deep Learning: Interrelationship (Singh, 2017)


ARTIFICIAL INTELLIGENCE
A program that can sense, reason, act, and adapt
MACHINE LEARNING
Algorithms whose performance improve as they are exposed to more data over time
DEEP LEARNING
Subset of machine learning in which multilayered neural networks learn from vast amounts of data

3 | Current Activities in the Government Market

As one might expect, there is significant interest in the Government marketplace for AI/ML/DL technologies.

- In 2016, the Obama Administration formed the National Science and Technology Council (NSTC) Subcommittee on Machine Learning and Artificial Intelligence and directed the creation of a National Artificial Intelligence Research and Development Plan, which establishes objectives for federally funded AI research: The National Artificial Intelligence Research and Development Strategic Plan (National Science and Technology Council, 2016);
- A 2018 report highlighting AI initiatives taken by the U.S. government;
- A White House report on Trump administration initiatives, including prioritizing funding for AI research and development (R&D), removing barriers to AI innovation, training the future American workforce, and more;
- FY 2019 NDAA to Authorize $10M for AI National Security Commission;
- FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems;
- OMB research guidance directed agencies to focus on emerging technologies, including machine learning and autonomous systems.
- The Federal Government's investment in unclassified R&D for AI and related technologies has grown by over 40% since 2015, in addition to substantial classified investments across the defense and intelligence communities (The Trump Administration, 2018);
- The President's Management Agenda calls for using automation software to improve government services and maximize Federal data sharing with the American public, which will support non-Federal AI research applications.
- The General Services Administration (GSA) is conducting pilot programs that leverage AI, including a tool to predict regulatory compliance scheduled for production in cloud.gov this year.
- Federal Bureau of Investigation (FBI) Criminal Justice Information Systems released an RFI for the current and prospective use of AI in the Next Generation Identification (NGI) System in the context of automatically identifying fingerprint alterations.

The AI/ML/DL technologies are being assessed for use in many domains as they represent a new set of automation and problem solving approaches.

4 | Select Use Cases in Justice and Public Safety

Justice and public safety organizations in the United States are embracing AI to improve quality, meet demands for better public safety, and serve as a force multiplier. The public safety community lacks many resources, primarly for staff and funding. Investing in AI can provide relief for resources and significant benefits to the communities served.

The National Institute of Justice (NIJ) recently published an article by Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs" (Rigano 2019), which describes NIJ-supported research to "address criminal justice needs, such as identifying individuals and their actions in videos relating to criminal activity or public safety, DNA Analysis, gunshot detection, and crime forecasting" (Rigano, 2019). The article lists these use cases for AI:

"Intelligence analysts, for example, often rely on facial images to help establish an individual's identity and whereabouts. Examining the huge volume of possibly relevant images and videos in an accurate and timely manner is a time-consuming, painstaking task, with the potential for human error due to fatigue and other factors."

"The U.S. Department of Transportation is also looking to increase public safety through researching, developing, and testing automatic traffic accident detection based on video to help maintain safe and efficient commuter traffic over various locations and weather, lighting, and traffic conditions."

"AI algorithms are being used in medicine to interpret radiological images, which could have important implications for the criminal justice and medical examiner communities when establishing cause and manner of death."

"The discovery of pattern signatures in gunshot analysis offers another area in which to use AI algorithms. Using a well-defined mathematical model, the Cadre (Research Labs) scientists are working to develop algorithms to detect gunshots, differentiate muzzle blasts from shock waves, determine shot-to-shot timings, determine the number of firearms present, assign specific shots to firearms, and estimate probabilities of class and caliber — all of which could help law enforcement in investigations." (Rigano, 2019)

These use cases and others discussed in the article show how AI can be used as a force multiplier for public safety. Another example includes a Nevada Highway Patrol (NHP) project described in a recent govtech.com article.

An Israeli startup working with NHP "is training artificial intelligence on the region's traffic woes, closely scrutinizing two corridors in hopes of helping highway patrol officers work smarter."

"Coordinating with NHP, the Nevada Department of Transportation and Regional Transportation Commission of Southern Nevada, [the startup] has deployed a cloud-based platform aimed at optimizing traffic management systems and emergency response."

"The [startup's] platform, which draws on everything from social media to crowdsourcing apps like Waze, refines and synthesizes information including speed, braking and acceleration data, then puts it to work predicting potential highway trouble spots."

"Since the system went live around late-September, officials have charted a 12 percent improvement in NHP response times, and a 23 percent drop in secondary collisions — often more serious than primary collisions — all because accidents are being cleared faster." (Douglas, 2018)

4.1 | Artificial Intelligence / Machine Learning in Cyber Security

AI/ML have the potential to change the game for cybersecurity. AI/ML-based approaches allow for the analysis of massive quantities of risk data to speed response times and augment under resourced security operations. AI/ML provide instant insights to filter through thousands of daily alerts, drastically reducing incident response times.

AI/ML-based systems can play an important role in cybersecurity, cyberthreat intelligence, and analytics to detect, contain, and mitigate advanced persistent threats, as well as fight against and mitigate malicious cyberactivities (e.g., organized cybercrimes and state-sponsored cyberthreats). For example, AI/ML systems can automatically scan for unknown malware or zero-day exploitation based on certain features and behavior, rather than specific signatures (Sikos, 2019).

In an AI/ML-based system, the system is trained by consuming billions of data artifacts from structured and unstructured sources, such as blogs and news stories. Through ML and DL techniques, the AI improves its knowledge to “understand” cybersecurity threats and cyber risks.

The AI/ML system gathers insights and uses reasoning to identify the relationships between threats, such as malicious files, suspicious IP addresses, or insiders. This analysis takes seconds or minutes, allowing security analysts to respond to threats significantly faster. The AI/ML system eliminates time-consuming research tasks and provides curated risk analysis, which reduces the time security analysts take to make critical decisions and launch an orchestrated response to eliminate the threat.

4.2 | Facial Recognition

Facial recognition (FR) technologies employ AI to improve recognition and eliminate bias. FR tools allow an image angle adjustment, which then allows for more consistent and accurate matching to be validated by a criminal justice professional. In criminal justice applications, source materials for FR tools are often low quality or at odd angles, making normal recognition difficult. In these cases, source images are adjusted to normalize the image, which allows FR technology to more accurately match the image. Angle adjustment, when carefully audited, increases viable ratings to similar images and typically includes alignment, rotation, and clarity improvements. AI enables the tools to learn and enhance classification results and angle adjustment through feedback on results.

Employing AI in criminal justice FR tools yields automated processes that are consistent, repeatable, and documented, improving the processes used by criminal justice practitioners. This enhances the quality of investigations and allows for more effective justice from the prosecution and defense perspectives. FR rules out individuals just as often as it identifies them. Beyond investigations, FR can be used to improve public safety through automated identification of safety personnel, guests, visitors, and inmates where movements or access must be managed. Section 4.3 expands on one example of this use type. Other examples include using FR to scan visitors into courtrooms to identify potential threats and eliminate incidents that prevent the fair implementation of the justice process.

When FR is used in investigations or as a tool that narrows a target audience, the FR solution must record the source image, all angle adjustments, the adjusted image, statistical data on the candidate pool, and matching results. This allows for auditability and a comparison dataset used by AI to improve the tools.

Agencies applying FR must also have clear policies on technology and AI to improve tools and results. AI applications within any FR tool must be clearly documented and understood by users, and all capabilities and limitations must be made clear to the subsequent justice practices that utilize the FR tool results.

4.3 | Risk Assessment in Prisons

There is an incredible demand for dynamic, real-time risk assessment in correctional institutions. However, the industry faces considerable difficulty in realizing these goals (Baird, et al. 2013). Most corrections agencies use assessment tools that are based on self-reported data, even though these tools are unlikely to ever allow for real-time analytics. ML techniques offer the most promise for these ambitions, especially when combined with real-time visual information processing.

Many other correctional tasks can be improved by ML. Every correctional facility faces constant decisions about how inmates should be classified, where they should be housed, and what programs they should be enrolled in. The inmate housing and program assignment problems seem particularly well-suited to linear optimization algorithms, and the Philadelphia Adult Probation and Parole Department already published a paper demonstrating some success with these methods. Inmate classification can likely be improved with an ML approach, such as the random forest method employed by Dr. Lawrence Sherman (Berk, et al. 2009), or the highly successful efforts of Dr. Grant Duwe in Minnesota (Duwe and Kim, 2017).

Risk assessment tools trained on neural networks already outperform traditional assessment tools, but these efforts do not yet use the full gamut of information available to correctional agencies. Social network analysis combined with visual information processing could allow an advanced algorithm to detect potential conflicts before an incident occurs by tracking the complex interrelationships among inmates, combined with a level of situational awareness informed by historical data. This might lead to tremendous operational savings and improved safety for staff and inmates within correctional facilities.

A major barrier to ML advancement in criminal justice is the strong need for algorithmic simplicity and transparency. Correctional agencies will not be willing to use a model output that is difficult to interpret, and a private algorithm influencing the offenders' fates could easily become a very serious legal and political issue. This limits the number of ML techniques that could be used in criminal justice, as well as the number of people who may be willing to develop them. Correctional agencies can mitigate these problems by developing their own ML experts or utilizing solution providers to develop customized tools for their population, as well as focusing on the methods with outputs that are easy to interpret.

4.4 | Risk Assessment in Probation and Parole

The corrections community has used risk assessments since the 1920s (Baird, et al. 2013). This first generation consisted of supervising clients and a 'gut feeling.' Subsequent generations incorporated the use of statistics (second generation), as well as evidence-based practices and dynamic risk factors (third generation) (Andrews, Bonta and Wormith, 2006). The current generation (fourth) is more systematic and incorporates additional risk factors and needs.

Risk and needs assessments take static and dynamic factors into account when calculating risk score and determining needs. Risk is usually determined by static (unchanging/historic) factors such as criminal history, age, race/ethnicity, gender, etc. An algorithm is used to calculate the likelihood to recidivate (Eisenberg, et al. 2019). The person can be categorized as low, medium, medium/high, or high-risk to recidivate. This categorization is factored into the supervision plan in contacts and monitoring.

Needs are determined by dynamic (changing/treatable) factors, such as antisocial attitude, criminal associates, education, employment, leisure activities, etc. Assessments identify which needs are high and should be addressed immediately and which are low and can be addressed in the future. Needs also factor into the supervision plan by identifying which treatments or programs to make referrals for (substance abuse, anger management domestic violence counseling, etc.) (Wooditch, Tang and Taxman, 2014).

As mentioned earlier, assessments use algorithms to determine risk level and needs. These algorithms are developed based on research and are proprietary property. The specifics for scoring and grouping are usually not shared with the agency using the assessment, the person being assessed, or the courts (Yong, 2018). This becomes an issue when bias is introduced in the assessments.

Certain variables, such as criminal history, race/ethinicity, etc., have been shown to be biased to different demographic groups (Eckhouse, et al. 2019) (Angwin, et al. 2016). By taking these factors into account, supervision and services for some clients may be at a level that does not match their actual level of risk or need. There are calls for research to address this issue and find a way to decrease or eliminate the bias.

The future of risk and needs assessments may be able to take these factors into account and decrease or remove the bias in the risk and needs assessments. Risk and needs assessments may be able to adjust their scoring methods based on outcomes in the future, as well. If risk to recidivate does not match actual recidivism rates, the assessment may be able to suggest changes to the groupings to reduce the errors with the predicted risk and increase the assessment's accuracy .

4.5 | Automatically Identify Altered Fingerprints

The FBI's CJIS Division identified a growing trend where criminals intentionally alter their fingerprints to defeat identification within the NGI System. Alteration may occur in various ways, including abrading, cutting, applying acid, or performing surgery on fingertips. These techniques obliterate, distort, or imitate fingerprints of other individuals to hide that person's identity, thus avoiding identification in a criminal history record.

Additionally, unintentional alterations of the friction ridge pattern occur. Individuals whose occupations require frequent contact with chemicals or rough surfaces, such as bricklayers, may experience reduced friction ridge detail over time. Certain diseases and medical treatments may also cause fingerprint alterations. Regardless of whether the alterations are intentional or unintentional, accurate identification through the NGI System may be compromised.

Altered fingerprint detection and matching technology have been the topic of numerous scientific papers over the last half decade. Algorithm development efforts included the capability to detect unaltered and altered fingerprints and to match altered fingerprints with their unaltered mates.

The next step in the evolution of fingerprint alteration defensive technology is to use AI to enable the NGI System to detect and match not only the alteration types the algorithm has been coded to detect and match but also new alteration types the algorithm has not previously received. As those who seek to avoid identification continue to evolve their alteration techniques, it is critical that the NGI System maintain pace through the ability to learn in real-time.

The FBI is seeking input from Industry for the current and prospective use of AI in the NGI System related to fingerprint alterations.

4.6 | Courts Domain Use Cases

The court systems today are very paper-oriented. Most, if not all, court processes and interactions are manual, paper-based, and in an unstructured document format. This environment lends itself to the use of AI and ML. Two broad use cases are detailed below.

4.6.1 Document Handling

One use case is through document handling and turning unstructured information into structured data that is automatically organized for staff to use in their processes and to rethink some court processes. ML models may allow courts to handle more cases.

4.6.2 Courts Support of Self Representation

Many people cannot afford legal representation, which resulted in more self-representation by individuals faced with court proceedings. This is problematic as the individuals must interact with a system designed for lawyers. This leads to inadequate services, slowed processes, and backlogs. ML technologies could help the courts interface with the public by directing people to resources, helping them complete forms, and providing guidance through the court processes. The process described is analogous to online/automated technical support. Guiding people through optionsnand different steps, as well as improving the process, may support increased numbers of successful self-represented proceedings.

4.7 | DNA Analysis

AI can be used to detect patterns in DNA not easily detectable by human examiners. Current research suggests that AI may improve the success of separating and identifying individual DNA donors based on older and smaller amounts of biological material. These improved methods can create leads in new and old criminal investigations (Rigano, 2019). In 2018, a suspect in the "Golden State Killer" case was apprehended after a 20-year investigation, mostly due to an unconventional approach involving a publicly accessible genealogy database (GEDmatch n.d.) (Butler, 2019). This is a game-changer because now it is possible to identify suspects without depending on a prior genetic sample collected by law enforcement. The coupling of AI technology and genealogical databases may yield even greater potential in the future (Bulman, 2014).

4.8 | Gunshot Detection

Scientists are working to develop algorithms to detect gunshots, differentiate muzzle blasts from shock waves, determine shot-to-shot timings, determine the number of firearms present, assign specific shots to firearms, and estimate probabilities of class and caliber — all of which could help law enforcement in investigations (Rigano, 2019).

Gunshot detection algorithms can be effective to identify gunshots, but one 2018 study published in the *Journal of Experimental Criminology* showed that it may also increase the police workload investigating unconfirmed gunshot incidents detected by sensors (Ratcliffe, et al. 2019). This inefficiency should decrease as gunshot detection sensors and algorithms improve.

4.9 | Crime Forecasting

AI increased the potential to predict outcomes in four areas:

1. **Legal outcomes:** AI algorithms can interpret large volumes of legal precedence, social information, and media to suggest legal outcomes, identify criminal enterprises, and identify people at risk.
2. **Recidivism:** AI analysis of existing criminal records can predict recidivism when warrants go unserved, which can assist law enforcement agencies in optimizing limited resources.
3. **Potential victims of physical and financial elder abuse:** This AI technology can inform law enforcement of a likely crime in progress in time to intervene, as well as identify likely victims of elder abuse and financial exploitation.
4. **Potential victims of violent crime:** AI may be used to identify high-risk individuals through analysis of social network risk (Rigano, 2019).

Many software companies offer AI tools to predict crime types and locations for more effective allocation of patrol resources. Past studies show that crime prediction algorithms can be effective in reducing certain types of crimes when properly applied (Dormehl, 2018).

5 | Benefits

Using AI to support criminal justice decision making offers several benefits, not all of which are related to a specific use case. Many advantages can be realized during an initial requirements definition, as well as throughout the operational life of the application. Such capabilities reduce reliance on specialized human resources, allow for the processing of larger volumes of information than might otherwise be impracticable, and support dynamic algorithms that automatically adjust to changes in real-world patterns. These benefits include:

- **Processing Large Volumes of Information.** Although the capacity for computers to collect and store information has grown, the ability for humans to efficiently process that information has remained stagnant. Analyzing criminal justice information often requires specialized human resources that are limited in availability, which requires significant training and investment in Subject Matter Experts (SMEs). Furthermore, examining this information can be extremely tedious when done manually; people are subject to exhaustion, which can lead to errors and omissions in the analysis.

  For example, an investigation may need to review hundreds of hours of video taken in a crowded environment in order to trace a suspect's movements. Although a lot of this information may be immaterial, it must still be analyzed in detail to identify the relevant video frames or sequences. Machines are well-suited to such tasks, often provide useful results more quickly than humans, and require a substantially smaller investment in training than SMEs.

- **Identifying Patterns in Inconsistent Data.** A significant advantage of AI is the ability to process unstructured information that contains substantial variation and inconsistency. This allows the system to produce higher quality outputs from lower-quality inputs. As an example, consider free text information contained in incident reports and court case information. Although this information often contains some structured data, much of the useful information can be found in large blocks of text that may contain considerable variation in spelling, grammar, formatting, and digital representation.

  While traditional algorithms can be constructed to analyze this information, they are often rigid and produce inaccurate results when confronted with data and patterns not anticipated at the time the algorithm was defined. To support such methods, a substantial up-front human effort is often required to define the rules themselves, as well as cleanse and normalize input data. Because algorithms based on AI intelligence are tolerant of immaterial variations in information, the initial human involvement required to create such a system can be reduced.

- **Creating and Adapting Rules Based on Experience.** Traditional analytic systems require humans to define business rules based on experience and understanding of the signals present in the data which, in most cases, are based on predefined/well-defined features of information (e.g., in facial recognition, the eye shape, color, and spacing). Although effective, humans may not consider other parameters that may support a desired output. Further, the up-front effort required to enumerate such rules may be substantial and rely upon specially trained SMEs. This necessary investment may also deter ongoing refinement of the algorithm as new experience is acquired, which can result in lower quality outputs over time.

  Systems based on AI are capable of developing rules independently and further refining those rules based on new information. A given pattern may change with time (e.g., policy changes, additional inputs that were not previously available, or other social trends), and without additional investment, traditional algorithms remain static based on what was known at design and implementation time. AI can automatically adapt to these changes based on experience, largely relieving humans of ongoing review and tuning of the algorithm, while also providing improved outputs over the system's life.

6 | Implementation Considerations

To be successful in implementing AI, organizations have to consider key challenges associated with deploying this emerging technology. Based on today's experience, these challenges include technology, process, skills, integration, and cost. This section outlines these challenges and some approaches to overcome them.

6.1 | Technology

Implementing AI requires significant computing capabilities and large amounts of storage. Additionally, according to Gartner, a team who is building data science algorithms and solutions uses seven tools on average to build a solution. Among these are multiple data processing tools (e.g., Spark, Hive, etc.) and AI/ML tools (e.g., Spark ML, PyTorch, TensorFlow, etc.). At the same time, agencies have a choice to deploy the solution on premises or in the cloud, which is one of the key decisions when starting the deployment.

Implementing the solution on premises might be driven by the availability of existing infrastructure, as well as compliance requirements more often associated with security and privacy. At the same time, deploying in the cloud brings significant benefits, such as the ability to use compute and storage on demand, as well as the availability of required tools for Platform as a Service (PaaS) services, which reduces the initial capital investment and ongoing operational costs.

Agencies must consider all of the above when building their AI implementation plan.

6.2 | Process

Adopting AI requires deliberate planning and a structured process that should be followed by a multidisciplinary team. Due to technology's emerging nature, the body of knowledge around process and best practices for implementation is fairly limited, and as a result, one of the biggest obstacles to successful implementation.

One of the approaches to overcome this challenge is to start small and follow the lead of other agencies that were early adopters in the same mission area.

6.3 | Skills

Implementing AI requires AI/ML experts, business analysts, and data scientists with deep knowledge of current AI technologies and their limitations. Additionally, it is necessary to supplement these AI specialists with SMEs who can provide context and clarity to the exact mission problem being solved with AI.

According to some estimates, fewer than 10,000 people have the skills necessary to tackle serious AI problems, and competition for them is fierce. Agencies considering the option to build their own AI solutions will need to consider whether they have the capacity to attract and retain workers with these specialized skills.

One strategy to consider is reskilling existing staff in addition to hiring external expertise to assure continuity and reduce the overall impact of this factor.

6.4 | Integration

Integration of the AI initiative is a multifaceted challenge. It starts with technology integration with existing systems to assure that the required data is available and extends into adopting new business models, new team models, and new workflows across all areas and teams.

Implementing a proven change management process to achieve this integration is key to success.

6.5 | Cost

As discussed above, adopting AI requires significant investment in technology, process, and people. Many agencies have challenges justifying this investment especially when they may not have a way to prove the benefits of implementing this emerging technology.

Two ways to overcome these challenges include identifying a clear problem that has a high priority for the constituents and starting small until there are demonstrable positive outcomes.

7 | Data and Information Organization

The correctness and organization of data and information used in AI/ML/DL-based systems are critical as these systems learn and make future decisions based on how the data/information are presented. Two broad types of data to consider here include:

Structured Data: These are typically sourced from other record systems and are common, well-organized data types, such as text, names, dates, biographical information, numbers, addresses, phone numbers, geospatial coordinates, monetary information, time series, etc.

Unstructured Data: These are items such as narrative text, photos, fingerprints, iris prints, videos, etc. They may also have some structured data in the form of annotation or descriptions attached. These are also sourced from other systems.

For both types of data, consideration should be given to:

- the quality of data being used in the AI/ML/DL based system;
- governance needs of the data;
- legal usage considerations and limitations;
- how changes in video and image resolutions affect AI/ML/DL systems; and
- potential impact on bias.

Also, a growing concern involves potential changes in how a data set can be used and how these changes could affect AI/ML/DL-based systems. For example, if an AI/ML/DL-based system has already “seen” some sensitive information, and a new policy/law prohibits the use of this data for the task at hand, then how does the AI/ML/DL-based system “unsee” this information?

8 | Issues and Considerations

8.1 | Ethics and Ethical Use

While the field of AI is in its early stages of development, recent advances in core computing technologies has provided the ability to implement and validate algorithms and applications, which have only been theoretical for many decades. Recognizing the developing and transformative nature of AI, the Defense Innovation Board recently issued a report on the “Principles for the Ethical use of AI” for the U.S. Department of Defense (DoD) (Defense Innovation Board, 2019). The principles in the report include:

1. **Responsible.** Human beings should exercise appropriate levels of judgment and remain responsible for the development, deployment, use, and outcomes of DoD AI systems.

2. **Equitable.** DoD should take deliberate steps to avoid unintended bias in the development and deployment of combat or non-combat AI systems that would inadvertently harm people.
3. **Traceable.** DoD's AI engineering discipline should be sufficiently advanced so that technical experts possess an appropriate understanding of the technology, development processes, and operational methods of its AI systems, including transparent and auditable methodologies, data sources, and design procedure and documentation.
4. **Reliable.** DoD AI systems should have an explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use.
5. **Governable.** DoD AI systems should be designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption, and for human or automated disengagement or deactivation of deployed systems that demonstrate unintended escalatory or other behavior.

Note that the principles can easily be adopted to the public safety, justice, and law enforcement domain.

8.2 | Jurisdictional Rules

Different legal entities and jurisdictions will have different rules with legal implications. For example, certain jurisdictions may have different rules and precedents for establishing "Probable Cause" in a court of law. Some will accept AI and ML guidance, and some will not.

8.3 | Security

AI and ML algorithms can be "gamed." If unsecured people control the input into the system, then they can provide data to the system that results in misleading results. A common example is "Google Bombing," in which a large number of web pages all link two objects together textually, often the name of a politician and a derogatory term. The end result is that a search for the derogatory term leads to results listing the politician. "Google bombing" can also be done on smaller scales for more esoteric topics.

Like any computer system, AI systems can be compromised. Compromise can lead to leaks of sensitive information or to algorithm modifications. The opaque nature of AI systems can make it more difficult to tell when results have been compromised. *If you don't know exactly how the results were generated, how will you know when they're wrong?*

8.4 | Bias

AI and ML systems can perpetuate biases. Bias can be introduced either unintentionally or intentionally. Bias endangers desire for fairness at all levels and in all areas of criminal justice.

8.4.1 Bias in Training

AI and ML systems often rely on being trained on large data sets and are only as good as the data they were trained on. If those data sets include biases, then the resulting system will exhibit those same biases. In other words, the resulting system will reflect the training set, for good or ill (Merritt, 2019).

As an example, the Deep Dream images generated by Google's Deep Dream program, tended to morph many things into dogs. The reason being that the training set for the program used many dog photos. "Garbage in, garbage out" applies to AI systems, something that can be hard to see given the opaqueness of most AI systems.

Similarly, if a hiring system is trained on current staff as the desired outcome, then the system will end up biased toward candidates who do not reflect the existing staff. If the staff is biased, so will be the resulting system.

This problem gets worse in a criminal justice environment, where investigative and predictive systems will pick up prior biases by humans (Angwin, et al. 2016).

8.4.2 Bias in Algorithms

Even if a system is trained on unbiased training sets, the algorithms used to analyze that resulting system can reflect the biases of those who have designed or programmed the system. Designers may make decisions as to what is important and what is not, decisions that incorporate personal biases (Lecher, 2019). Alternately, a system may make its own decisions based on its own ideas of what information is important. Those decisions can be inaccurate, but the opaqueness of AI and ML systems make it difficult to see when they occur.

8.4.3 Demonstrating a Lack of Bias

Admission of results from AI may depend on an ability to show lack of bias. If we cannot explain how a system came to its conclusion, then how can we show it came to that conclusion within allowed parameters? Similarly, a system may need to show that it does not rely on factors that it should not be relying on when developing a result.

A court might insist that a system show how it came to a recommendation, while the very nature of the system may prevent it from doing so. “We don’t know how it works, just that it does” is not a good answer to a judge asking about “probable cause.”

Potential legislation may codify this need to show a lack of bias in algorithms. The potential Algorithmic Accountability Act would require some entities to prove that their algorithms are neither biased nor discriminatory (116th Congress, First Session, 2019).

9 | Summary and Looking Forward

AI/ML/DL are emerging technologies with tremendous potential to improve nearly every analytical process used by companies and government agencies. However, as with the adoption of any new technology, there will be challenges to the widespread adoption and acceptance of these technologies. This section contains general recommendations to facilitate the proliferation of AI/ML/DL technologies by using these technologies responsibly, as well as preparing for likely barriers to acceptance in the near future. These recommendations include:

- **Transparency and Explainability** – Any creation of AI/ML/DL technology should assume that the creation process and validity of model outputs will probably need to be explained and justified to stakeholders and government agencies. There has been movement towards algorithmic transparency with H.R. 2231 (The Algorithmic Accountability Act of 2019), but this legislation is tame compared with what will likely follow in the future. Washington state has already passed legislation with HB 1655 (Washington State House of Representatives 2019) and SB 5527 (Washington State Senate 2019) to regulate automated decision-making systems. Legislation similar to this will likely be implemented nationally within a few years. Anyone training an AI/ML/DL system should prepare to publicly report and justify their methodology. “Black box” processes will probably receive increased scrutiny, so alternatives should be considered if a viable alternative is present.
- **Training, Education, and Outreach** – Education initiatives are necessary for the widespread adoption of AI/ML/DL systems to address common misunderstandings in how these systems work and their capabilities. A word of caution to those creating AI/ML/DL systems: AI/ML/DL systems are complex systems that require proper data, careful work, and adequate time, and, contrary to marketing messages, an AI/ML/DL system is not a “magic button” that will miraculously solve all problems. Additionally, these processes are often complicated to the point where operators misuse model outputs because they don’t understand how to properly interpret them. These issues can

be addressed with educational efforts by AI/ML/DL experts to explain how these systems work and how their outputs should be used as an additional responsibility when creating the system itself. Finally, outreach initiatives to stakeholders will assist in mitigating the initial skepticism and resistance to these new technologies to the community at large.

- **Regulatory Uncertainty Preparation** – Companies should also expect a movement towards universal assessment standards and metrics in the near future as a means of comparing the utility of different statistical processes. To prepare for this and uncertain regulatory standards:
    - AI/ML/DL engineers should evaluate their systems with as many assessment metrics as possible.
    - An industry representative organization working with its members could develop a set of assessment standards, which may influence the imminent regulatory mandate.
    - Companies developing solutions could develop multiple AI/ML/DL solution options to a given problem, and then choose the best performing system across many metrics. This will serve to help justify the process as well as prepare for upcoming accountability and assessment standards that will likely be put in place.

References

116th Congress 1st Session. 2019. “Algorithmic Accountability Act of 2019.” *US Senate*. https://www.wyden.senate.gov/download/algorithmic-accountability-act-of-2019-bill-text.

Andrews, D. A., James Bonta, and J. Stephen Wormith. 2006. “The Recent Past and Near Future of Risk and/or Need Assessment.” *Crime & Delinquency* (Sage Publications) 52 (1): 7-27.

Angwin, Julie, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. *Machine Bias*. May 23. Accessed June 2019. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Baird, Chris, Theresa Healy, Johnson Kristen, Andrea Bogie, Erin Wicke Dankert, and Chris Scharenbroch. 2013. “A Comparison of Risk Assessment Instruments in Juvenile Justice.” *National Criminal Justice Reference Service (NCJRS)*. December. Accessed June 2019. https://www.ncjrs.gov/pdffiles1/ojjdp/grants/244477.pdf.

Berk, Rchard, Lawrence Sherman, Geoffrey Barnes, Ellen Kurtz, and Linday Ahlman. 2009. “Forecasting murder within a population of probationers and parolees: a high stakes application of statistical learning.” *Journal of the Royal Statistical Society: Series A (Statistics in Society)* 172 (1): 191-211.

Bulman, Philip. 2014. “Solving Cold Cases With DNA: The Boston Strangler Case.” *National Institute of Justice Jounral* (National Institute of Justice) (273): 49-51.

Butler, John. 2019. “NIST: National DNA Day and the Birth of Investigative Genetic Genealogy.” *NIST Taking Measure Just a Standard Blog*. April 25. Accessed June 2019. https://www.nist.gov/blogs/taking-measure/national-dna-day-and-birth-investigative-genetic-genealogy.

Defense Innovation Board. (2019). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*. US Department of Defense.

Dormehl, Luke. 2018. *New crime-predicting algorithm borrows from Apollo space mission tech*. Juy 26. Accessed June 2019. https://www.digitaltrends.com/cool-tech/predicting-policing-weather-forecasting/.

Douglas, Theo. 2018. *Las Vegas AI Pilot Improves Highway Patrol Response Times*. January 10. Accessed May 2019. https://www.govtech.com/public-safety/Las-Vegas-Artificial-Intelligence-Pilot-Improves-Highway-Patrol-Response-Times.html.

Duwe, Grant, and KiDeuk Kim. 2017. “Out With the Old and in With the New? An Empirical Comparison of Supervised Learning Algorithms to Predict Recidivism.” *Criminal Justice Policy Review* (SAGE Journals) 28 (6): 570-600.

Eckhouse, Laurel, Kristian Lum, Cynthia Conti-Cook, and Julie Ciccolini. 2019. “Layers of Bias: A Unified Approach for Understanding Problems With Risk Assessment.” *Criminal Justice and Behavior* (SAGE Journals) 46 (2): 185-209.

Eisenberg, Mara J., Joan E. Van Horn, Judith M. Dekker, Mark Assink, Claudia E. Van Der Put, Jan Hendriks, and Geert J. M. Stams. 2019. "Static and Dynamic Predictors of General and Violent Criminal Offense Recidivism in the Forensic Outpatient Population: A Meta-Analysis." *Criminal Justice and Behavior* (SAGE Journals) 46 (5): 732-750.

GEDmatch. n.d. "GED Match Tools for DNA and Genealogy Research." *GEDmatch, Inc*. Accessed June 2019. https://www.gedmatch.com/login1.php.

Lecher, Colin. 2019. *The artificial intelligence field is too white and too male, researchers say*. April 16. Accessed June 2019. https://www.theverge.com/2019/4/16/18410501/artificial-intelligence-ai-diversity-report-facial-recognition.

n.d. "Lexico.com: Artifical Intelligence." *Lexico, Powered by Oxford*. https://www.lexico.com/en/definition/artificial_intelligence.

Merritt, Tom. 2019. *Top 5 ways humans bias machine learning*. January 9. Accessed June 2019. https://www.techrepublic.com/article/top-5-ways-humans-bias-machine-learning/.

National Science and Technology Council. 2016. *The National Artificial Intelligence Research and Development Strategic Plan*. National Science and Technology Council, CreateSpace Independent Publishing Platform.

Ratcliffe, Jerry H., Matthew Lattanzio, George Kikuchi, and Kevin Thomas. 2019. "A partially randomized field experiment on the effect of an acoustic gunshot detection system on police incident reports." *Journal of Experimental Criminology* (Springer Netherlands) 15 (1): 67-76.

Rigano, Christopher. 2019. "Using Artifical Intelligence to Address Criminal Justice Needs." *NIJ Journal* (National Institute of Justice) (280): 37-46.

Sikos, Leslie F. 2019. *AI in Cybersecurity*. Cham: Springer Nature Switzerland AG.

Singh, Niven. 2017. *How to Get Started as a Developer in AI*. December 28. https://software.intel.com/en-us/articles/how-to-get-started-as-a-developer-in-ai.

The Trump Administration. 2018. *Artificial Intelligence for the American People*. May 10. https://www.whitehouse.gov/briefings-statements/artificial-intelligence-american-people/.

Washington State House of Representatives. 2019. "Washington State Legislature." *House Bill 1655. State of Washington 66th Legislature*, 2019 Regular Session. October. https://app.leg.wa.gov/billsummary?BillNumber=1655&Chamber=House&Year=2019.

Washington State Senate. 2019. "Senate Bill 5527. State of Washington, 66th Legislature, 2019 Regular Session." *Washington State Legislature*. October. https://app.leg.wa.gov/billsummary?BillNumber=5527&Year=2019&initiative=#documentSection.

Wooditch, Alese, Liansheng Larry Tang, and Faye S. Taxman. 2014. "Which Criminogenic Need Changes Are Most Important in Promoting Desistance From Crime and Substance Use?" *Criminal Justice and Behavior* (SAGE Journals) 41 (3): 276-299.

Yong, Ed. 2018. *A Popular Algorithm Is No Better at Predicting Crimes Than Random People*. January 17. Accessed June 2019. https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/.