Artificial Intelligence in the Criminal Justice System

Demystifying artificial intelligence, its applications, and potential risks

This technology brief is the first in a four-part series that explores artificial intelligence (AI) applications within the criminal justice system. This first brief frames AI, defines common AI terms, and offers a mental model for identifying AI use cases within the criminal justice system. While this brief provides examples of how AI might bring significant benefit to the criminal justice system, it also highlights risks that decision makers should consider when developing or deploying AI tools. Additional briefs provide greater consideration of AI in law enforcement, the criminal courts system, and corrections.

Key Takeaways

- AI will transform our personal, industrial, commercial, and civil realities in the years to come—enabling and challenging individuals involved in the justice system as well as in criminal activity.

- AI tools have the potential to improve efficiency, reduce costs, and expand capabilities across many criminal justice use cases; however, technical feasibility and operational realities need to be considered.

- AI systems carry inherent risk that decision makers need to understand. For example, AI technologies raise ethical and civil liberties questions that the criminal justice system and society at large will have to wrestle with in the years ahead.

AI will bring changes to nearly every industry over the next decade. In fact, AI is already impacting our daily lives and is being built into the background of many of our daily activities—from facial recognition technologies that unlock our smartphones, to algorithms that recommend movies we might like, to virtual chatbots that handle our customer service inquiries.

For the criminal justice system, AI presents opportunities along with significant risks. AI tools have the potential to improve efficiency, reduce costs, and expand capabilities across many criminal justice use cases. Yet many criminal justice leaders have misconceptions about the capabilities and the level of investment required to create or deploy AI solutions for specific use cases.

Resources for Considering AI in Criminal Justice Applications

This document explores AI within the criminal justice system. Additional briefs address specific application areas.

Figure 1: Implementing AI impacts all stakeholders in the criminal justice community. Briefs in this series frame AI within the community and focus on AI applications in law enforcement, criminal courts, and corrections.
What is Artificial Intelligence?

AI is often misconstrued as a single technology. In reality, AI is a broad discipline encompassing a wide range of methods that seek to create machines that mimic human intelligence. Recent well-publicized advances and media hype have led many to view AI as a new technology. Yet, as far back as the 1950s, researchers like Alan Turing and John McCarthy were working on systems that could mimic human intelligence. The field has had many notable historical achievements with advances—such as the calculator, spell check, and search engines—that are no longer recognized as AI but were once applications on the cutting edge of machine intelligence.

Despite the long history of AI research, recent advances have created an exponential growth in AI applications, research, companies, and misinformation. This brief is not a comprehensive guide to the various domains or underlying computational methods that enable AI applications. However, the criminal justice community should be aware that terms like AI, machine learning, and deep learning are not always interchangeable. Figure 2 highlights common AI terms and their relationship.

The question for the criminal justice community is not, “Is AI ready for deployment today?” Rather, the question is, “How can we be proactive co-creators of an intelligent criminal justice future that balances the risks and opportunities of this new technology?”

Common AI Terms and Their Relationship

The term intelligent system often refers to a system of multiple machines that work together to perceive, learn about, and respond to their environment. Intelligent systems use AI.

Artificial intelligence is a field within computer science that often describes the creation of machines that mimic human intelligence through perception and action in pursuit of a goal. There are many different technical approaches to creating AI.

Machine learning is one of several approaches to creating AI. Unlike explicitly programmed systems (known as rule-based AI or expert systems), machine learning algorithms use known examples—called training data—to “learn” to classify an object or to predict an outcome. There are many types of machine learning methods—including supervised learning, unsupervised learning, reinforcement learning, decision trees, some types of regression, and deep learning; regression algorithms and decision tree algorithms are also often classified as AI or machine learning.

Deep learning algorithms are a type of machine learning that uses artificial neural networks. While deep learning is a powerful approach to creating AI, deep learning algorithms are less transparent than other approaches. For many deep learning algorithms, it is not possible to explain how a particular set of inputs resulted in the algorithmic output.

A Deeper Look at the “Black Box” of AI

Many of the most common AI methods are not “black boxes.” Algorithmic outputs for many AI methods can be explained; however, this is not the case for some deep learning algorithms. Deep learning is a type of AI that has been growing in popularity over the last decade and is powering many AI systems in use today. Yet, explaining how inputs to deep learning algorithms lead to specific outputs is not always possible. Due to the complexity within deep learning systems, even their creators often cannot explain how these systems arrive at specific results. This creates a black box problem for many deep learning-powered AI systems.

Understanding the black box of deep learning systems, a field known as Explainable AI, is an active area of research for many government agencies including DARPA and NIST, private companies, and academic institutions.

AI’s black box problem poses additional risks to the use of these systems within criminal justice settings. In particular, black boxes prevent AI systems from ensuring transparency in the decision-making process and create issues when an AI system is challenged or outputs must be explained. For example, if AI systems are used to make sentencing recommendations within the court system, then an inability to explain how an AI system arrived at a recommendation can lead to concerns about fairness. The explainability of risk assessment tools is an important consideration for criminal justice leaders to consider before implementation.

The risks associated with black box AI systems vary by application. For example, deep learning systems power voice-to-text transcription and other natural language processing applications. The risks associated with many voice-to-text applications are likely much lower than the risk associated with pre-trial risk assessment tools. Criminal justice leaders must evaluate the risks and benefits of AI systems on a case by case basis and should be cautious when considering black box AI systems.

AI is not a magical panacea. AI systems are seldom, if ever, a plug-and-play solution. It is important for criminal justice leaders to understand AI’s key limitations and risks.

Factors Driving the AI Hype

Several factors are driving the growth of AI applications. First is the proliferation of “big data” from a variety of sources—phones, internet activity, transactional data, personal fitness trackers, etc. Data are the fuel for AI systems, and there has been an explosion in data generation. Second, advances in a particular subdomain of AI, called deep learning, have opened up applications such as machine vision and natural language processing (NLP) that enable a wide range of new use cases. Lastly, advances in computer processors are increasing the computational power and speed of the hardware that powers AI-enabled systems.

---

13. It is estimated that that 90% of global data available in 2018 data was generated from 2016 to 2018; this was caused by the growth of (1) the “connected” world and (2) the internet of things. Griffith, E. (2018, November 13). 90 Percent of the BigData We Generate Is an Unstructured Mess. Retrieved March 27, 2020, from https://www.pcmag.com/news/36954/90-percent-of-the-big-data-we-generator-is-an-unstructured-mess.
Common AI Types and Criminal Justice Examples

There are several types, or functional categories, of AI that can help criminal justice leaders better understand AI’s emerging capabilities. Although the functionalities shown in Figure 3 are not comprehensive, they serve as a good starting point for exploring potential AI use cases. Example products and vendor technologies are provided for illustrative purposes only.14

AI systems are already helping the criminal justice community and will continue to have greater impact. It is important for criminal justice leaders to understand the different types of AI and how each type might be used in the criminal justice context.

<table>
<thead>
<tr>
<th>Functionalities Enabled by AI</th>
<th>Example Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Language Processing (NLP)</td>
<td>Speech recognition, speech to text, natural language understanding, and natural language generation software all use NLP technology. NLP algorithms enable voice-controlled systems like Alexa and Siri®. Other NLP applications include automatic transcription (sometimes used in the criminal justice system for transcribing interviews), extraction of sentiment from blocks of text, virtual chatbots, and real-time translation or captioning.</td>
</tr>
<tr>
<td>Machine Vision</td>
<td>Although image analysis has deep roots in criminal justice for applications such as fingerprint analysis, advances in deep learning are rapidly advancing machine vision capabilities. Applications such as facial recognition technology,15 license plate readers, video enhancement, autonomous vehicles, and medical imaging all use machine vision technologies. Google is taking machine vision a step further by developing detection software to identify “deepfakes”—videos that have been doctored by AI—to distinguish between real versus fake pictures and videos.16</td>
</tr>
<tr>
<td>Information Analysis/Predictive Analytics</td>
<td>Recommendation engines for online shopping, enhanced weather prediction, and targeted digital advertising are examples of how AI is improving predictive analytics. In criminal justice, these types of technologies have been used to detect and prevent financial fraud by flagging suspicious transactions or anomalous user behavior. In addition, platforms powered by advanced analytics have been used for hot spot forecasting, potential suspect identification, and court risk assessments.</td>
</tr>
<tr>
<td>Robotic Process Automation (RPA)</td>
<td>Deploying RPA requires detailed examination of existing processes and identification of potential points of automation to enable the design, build, and monitoring of successful systems. Examples include automated password resets, automated report generation and distribution, and call routing at customer service centers.</td>
</tr>
</tbody>
</table>

Figure 3: The criminal justice community is currently using AI in a number of applications.

14. The Criminal Justice Testing and Evaluation Consortium (CJTEC) does not endorse any specific product or vendor. Mentions of companies and/or products do not represent approval or endorsement by the National Institute of Justice.
Considerations for AI Success

Any successful implementation of AI-enabled technology must consider technical feasibility, which includes both data quality and the systems that house the data, ethical appropriateness that considers the benefits and risks to all stakeholders, and operational achievability to ensure that technology adoption would integrate well within workflows—as Figure 4 shows.

Technical Feasibility

For many new applications, developing an AI system requires a large amount of high-quality data. These data (often called training data) are used to “teach” the AI system and enable machine identification and prediction. Poor quality and insufficient data are often major barriers to AI adoption in many applications.

It is important to distinguish between AI applications specific to criminal justice and those that can be applied more broadly. Criminal justice–specific applications require criminal justice data to develop and train an AI system. For example, creating an AI system that predicts the likelihood of a trial conviction given a certain set of evidence would require a very large volume of court-specific training data.

In contrast, other AI applications are broadly applicable and may not require criminal justice data for training. For example, AI-enabled transcription software has applications in education, healthcare, entertainment, and many other industries. Adapting AI-enabled transcription for criminal justice applications—like using AI to automatically transcribe a deposition—requires less court-specific training data since much of human language is consistent across industries. For applications that primarily use industry-agnostic data, AI systems will likely improve at a faster rate and will be easier for the criminal justice community to adopt. Consequently, criminal justice leaders can benefit from routinely monitoring AI application development in other industries to identify near-term opportunities.

As criminal justice communities and jurisdictions evaluate AI-enabled solutions, leaders and executives must be careful and take ethical concerns into consideration to ensure that any new AI system that is being considered will support the community rather than damage it.

---

Ethical Appropriateness

Technology might enable certain capabilities; however, that does not mean that the use of AI is always ethically appropriate in the criminal justice context. Major ethical issues—such as privacy, fairness, transparency, security, and accountability—are regularly being discussed in the AI community (see Figure 5). Recently, the Department of Defense issued five ethical principles related to AI applications; these principles mention that AI applications should be responsible, equitable, traceable, reliable, and governable. Defining ethical use cases for AI will require ongoing conversations between criminal justice leaders and stakeholders.

Decisions about appropriate use cases may vary by community. For example, in 2019, California banned the use of facial recognition technologies (FRT) by law enforcement. That same year, a federal study confirmed racial differences in the accuracy of FRT by finding that FRT misidentifies people of color more often than white people. Bias—including sampling bias and social bias—is a major concern for prediction or recommendation systems in the criminal justice context. Many international organizations like Institute of Electrical and Electronics Engineers (IEEE) and public-private partnerships like the Partnership on AI are actively collaborating on ethical standards for the use of AI. Criminal justice leaders that decide to implement AI systems should carefully consider the ethical implications of the proposed approach.

Operational Limitations

Even in situations in which technical feasibility and ethical considerations are satisfied, deploying AI tools often requires behavioral changes, process changes, or other operational integration steps. Outside the criminal justice system, many business leaders are finding that overcoming these operational, cultural, and systems integration challenges are far more difficult than solving the technical challenges. The operational limitations that criminal justice leaders are likely to encounter vary widely by application and often depend on the organizational context in which AI tools are deployed. Even seemingly simple operational factors, such as changing existing workflows, can be met with resistance by people who prefer the status quo or prefer data collection practices that do not align with effective AI deployment. Failure to consider operational factors—in addition to the technical and ethical feasibility—will prevent these technologies from having their intended impact in criminal justice settings; these settings include police agencies, courts, prisons, and community-based corrections.

---

18. In this brief we use the term “ethically appropriate” to represent a range of issues related to the appropriate use of AI technology, including privacy, fairness, transparency, security, and accountability. We intentionally decided not to define or determine which use cases were ethical and which were not. Such decisions are highly context dependent and require ongoing conversations with stakeholders.


21. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (December 2019). Retrieved March 27, 2020, from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf From the study: Using the higher quality Application photos, false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals. This effect is generally large, with a factor of 100 more false positives between countries. However, with a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces. With domestic law enforcement images, the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm.

22. Sampling bias occurs when a sample of data over-represents a given characteristic or group of people in the population. For example, if FRVT algorithms are trained on a data set that only includes men, the algorithm will likely be less accurate when identifying women. Similarly, if AI-algorithms are trained on data sets that only include left-handed people, the algorithm may identify future individuals as left-handed because the original data set was not statistically representative. Social bias is a product of the underlying social, historical, or political conditions that exist in a population when a data set is created. If the general population has unfair systematic biases then AI-tools may reflect or reinforce those biases, even if training data sets are statistically representative of the general population.


Ethical Considerations for the Use of AI for Criminal Justice Leaders

An overview of ethical considerations is presented in Figure 5. The key questions in each category can serve as a starting point for criminal justice leaders and decision makers as they evaluate potential impacts of AI solutions on the community and other stakeholders. Engaging in ethical use of any emerging technology requires ongoing conversations. Organizations that want to implement cutting edge technology must also lead conversations around ethical use of that technology.

<table>
<thead>
<tr>
<th>Ethical Issues</th>
<th>Key Questions to Consider for AI Tools</th>
</tr>
</thead>
</table>
| **Transparency, or explainability,** in intelligent systems refers to the capacity for humans to understand and interpret a given system's source of data, operation, and functioning. Transparent or explainable systems create a clear understanding of the relationship between input features and output predictions. | ☐ Is there transparency around the data and methods used to create the tool?  
☐ Has the AI tool's business use case been shared with and approved by relevant policy stakeholders?  
☐ Can users understand and explain how system variables impact the system predictions?  
☐ Are tool designs, architectures, and training data open to research, review, and criticism?  
☐ Are confidence estimates provided and useful for statistical predictions?  
☐ How does the AI system handle missing data? How was missing data handled in the design or training process? |
| **Fairness** ensures that all people are treated in an appropriate way that does not discriminate against any specific groups or individuals. Negative bias can lead to the preferential, prejudicial, or malicious treatment of groups and individuals. | ☐ Does the AI system treat all people fairly?  
☐ Do the data that were used to train the system involve any statistical or social biases?  
☐ Did the AI system developers educate themselves and seek out diverse evaluations and perspectives about the different ways that bias can penetrate system decision making? Did the developers create pathways to overcome those biases?  
☐ Was the system designed in such a way that reinforces existing biases within society, or are there features in place that mitigate or eliminate the unfair biases? |
| **Accountability** refers to both the need to justify its decisions and actions through an explanation and the need to identify parties responsible or legally liable for outcomes. Transparency is a possible means to that end. | ☐ Who is accountable for ensuring that the decisions made by AI systems are fair and just?  
☐ Are the AI tool's limitations of use clearly defined? Are there protections or auditing procedures in place to ensure that the AI tool is used only for approved business use cases?  
☐ Is the use of this AI tool legal in the jurisdiction it will be used? Who is legally liable for outcomes?  
☐ Will jurisdictions take responsibility for the post-deployment evaluation, monitoring, and auditing of the AI tool? |
| **Security** of AI systems refers to their resistance to malicious interference or use. | ☐ Does the AI system comply with security regulations?  
☐ How are data collected, stored, and distributed?  
☐ Is there a risk for malicious use of the AI tool?  
☐ Does the system have vulnerabilities that adversaries might exploit?  
☐ Are there sufficient cybersecurity measures in place?  
☐ Does the AI tool support internal auditing and modification for continued robustness and security updates? |
| **Privacy** protects the rights of individuals from unauthorized intrusion. There isn’t a clear, universal definition of privacy; however, privacy is an important consideration in the use of AI and is a critical issue that impacts community acceptance. | ☐ Are privacy rights protected with the use of the tool?  
☐ Does the tool provide users with more or less privacy than the law demands?  
☐ Have the designers and engineers thought about ways to satisfy the tool's purpose while maximizing user privacy? |

Figure 5: Criminal justice leaders and decisionmakers should consider these ethical issues and key questions as they evaluate potential impacts of AI solutions on the community and other stakeholders.
A Design Thinking Approach for Evaluating AI Use Cases

Design thinking is an approach to innovation that places emphasis on deeply understanding the problem, context, and end users before iteratively designing solutions. Design thinking asks the question, “What problem am I trying to solve?” rather than starting with a technology and asking, “Where can I use this new technology?” When evaluating AI’s role in the criminal justice system, a design thinking approach can help prevent the application of AI where it is not needed or not beneficial.

Criminal justice decision makers should first identify problems worth solving and then look at various technologies (including AI) to find the best tool for solving those problems.

**Question 1:** What is the “job to be done” by the AI system?

The first step for criminal justice leaders is to examine the problem they are trying to solve or the job that needs to be done. In the case of AI, most jobs that need to be done can be broadly segmented into two categories: (1) **performing tasks** and (2) **making decisions**. For task-oriented jobs, AI often aims to improve operational efficiency, improve communication, or reduce costs. For decision making or prediction-oriented jobs, AI aims to improve decision quality in a way that leads to improved outcomes. The answer to this question will be specific to the need within the criminal justice system.

**Question 2:** What level of AI involvement is appropriate?

For each criminal justice related task or decision, the level of AI involvement needs to be considered. Figure 6 highlights four levels of AI involvement: (1) AI should not be involved (i.e., the job should be done by **humans only**), (2) AI **assists humans**, often by increasing the efficiency with which the job is done, (3) AI **augments humans** to perform jobs that would be impossible for a human alone, and (4) AI can create fully automated systems and the human can be removed from the job.

Example uses of AI for criminal justice applications are shown in Figure 6. These uses illustrate varying levels of AI in situations where humans are helped in decision making or performing tasks.

### A Design Thinking Framework for AI Use Cases

**Figure 6:** Examples of AI helping humans make decisions or perform tasks in criminal justice settings.
10 Things Every Criminal Justice Decision Maker Should Know About AI

1. A design thinking approach that starts with a problem to be solved is more likely to succeed than simply adopting AI for the sake of being “cutting edge.”

2. AI tools have the potential to radically improve efficiency, reduce costs, and expand capabilities across many criminal justice use cases; however, capturing these gains will likely require significant investment and time.

3. Despite recent advances in AI methods, deploying AI is not a “plug-and-play” opportunity in most criminal justice applications. High-quality data are a critical prerequisite to successful AI development and deployment in new applications.

4. AI is not a single technology; rather, AI is a suite of computational methods that seeks to mimic human intelligence. Like any toolbox of technologies, each method has strengths and limitations.

5. Risks for AI systems vary by application type; decision makers considering AI solutions should carefully consider the technical, ethical, and operational risks as well as limitations of any proposed solution.

6. As AI technologies become a larger part of our daily lives, the skills of the criminal justice workforce will need to evolve to fully take advantage of these emerging tools.

7. AI will likely enable new forms of criminal activity and the criminal justice community must be prepared to respond.

8. Regardless of the technical readiness of AI systems, implementation may require substantial process or procedural changes. In addition to investing in AI technologies, leaders should also invest in a strategy for the change management efforts required to deploy AI-enabled tools effectively.

9. AI technologies raise questions about risks to ethical and civil liberties, and the criminal justice system and society at large need to stay vigilant.

10. Rates of adoption for AI technologies in criminal justice applications will vary, which presents an opportunity for learning through collaboration.

Future Outlook

AI is here to stay, and advances in technical capabilities will continue. The criminal justice community faces shrinking budgets and a growing sense of mistrust from the community. With these things in mind—and considering ethical appropriateness, technical feasibility, and operational limitations—AI provides important opportunities to improve the criminal justice system. Opportunities to implement AI tools should be met with a clear understanding of the data requirement and use a design-thinking approach to evaluating potential use cases. This series of briefs aims to inform decision makers about what is already happening in the criminal justice ecosystem and what is required to utilize emerging AI technologies in a thoughtful, informed, and unbiased way.

The NIJ continues to support a portfolio of AI research projects in areas such as public safety video and image analysis, DNA analysis, gunshot detection, and crime forecasting. Looking ahead to the future, different countries and states are likely to adopt AI technologies for criminal justice applications at different rates, which presents an opportunity for learning through collaboration. Improving criminal justice outcomes through the use of AI-enabled technologies will require intentional investment, careful consideration, and sustained efforts from criminal justice decision makers. If designed and implemented well, AI-enabled tools have the potential to improve efficiency, reduce costs, and expand capabilities across many criminal justice use cases.

---


Additional References


Published: August 2020

More Information

Steven Schuetz
Senior Science Advisor/Physical Scientist
National Institute of Justice
U.S. Department of Justice
Steven.Schuetz@usdoj.gov
Tel +1-202-514-7663

Jeri D. Ropero-Miller, PhD, F-ABFT
Project Director, CJTEC
RTI International
jerimiller@rti.org
Tel +1-919-485-5685

James Redden
Innovation Advisor
RTI International
jredden@rti.org
Tel +1-919-248-4222

Molly O’Donovan Dix
Director, Strategy and Innovation
RTI International
dix@rti.org
Tel +1-919-541-5866

Suggested Citation


This publication was made possible by Award Number 2018-75-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

http://cjtec.org/