NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

I'VE GOT MY AI ON YOU: ARTIFICIAL INTELLIGENCE IN THE LAW ENFORCEMENT DOMAIN

by

Eric M. Baker

March 2021

Co-Advisors: Erik J. Dahl
Anthony Canan

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2021	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE I'VE GOT MY AI ON YOU: ARTIFICIAL INTELLIGENCE IN THE LAW ENFORCEMENT DOMAIN	5. FUNDING NUMBERS
6. AUTHOR(S) Eric M. Baker	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

Artificial Intelligence (AI) systems provide a unique problem for users in the law enforcement domain. On one hand, AI systems provide an opportunity for optimizations and faster workflows, especially in the environment of growing data. On the other hand if left unchecked, AI systems have the potential to negatively affect the community served by law enforcement. This research focuses on three types of AI systems currently used by law enforcement: facial recognition, predictive risk assessments, and predictive policing. By looking at these three types of AI systems, this research attempts to evaluate the effectiveness of the technology while maintaining the privacy, fairness, transparency, and accountability expected by the public. These three case studies show how AI systems can have a negative impact on individuals identified via AI systems and the need for further research into effective measures to regulate the technology. Additionally, the European Union is currently working on potential frameworks for responsible implementation of AI systems, which provide a template for future efforts in the United States.

14. SUBJECT TERMS artificial intelligence, machine learning, AI	15. NUMBER OF PAGES 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

I'VE GOT MY AI ON YOU: ARTIFICIAL INTELLIGENCE IN THE LAW ENFORCEMENT DOMAIN

Eric M. Baker
Intelligence Systems Analyst, Texas Department of Public Safety
BS, University of Texas, 2010

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2021**

Approved by: Erik J. Dahl
Co-Advisor

Anthony Canan
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Artificial Intelligence (AI) systems provide a unique problem for users in the law enforcement domain. On one hand, AI systems provide an opportunity for optimizations and faster workflows, especially in the environment of growing data. On the other hand, if left unchecked AI systems have the potential to negatively affect the community served by law enforcement. This research focuses on three types of AI systems currently used by law enforcement: facial recognition, predictive risk assessments, and predictive policing. By looking at these three types of AI systems, this research attempts to evaluate the effectiveness of the technology while maintaining the privacy, fairness, transparency, and accountability expected by the public. These three case studies show how AI systems can have a negative impact on individuals identified via AI systems and the need for further research into effective measures to regulate the technology. Additionally, the European Union is currently working on potential frameworks for responsible implementation of AI systems, which provide a template for future efforts in the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
ALPR	automated license plate reader
AUC	area under curve
BWC	body worn camera
CCPA	California Consumer Protection Act
CCTV	closed-circuit television
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
CTC	criminal, traffic, and civil
EFF	Electronic Frontier Foundation
EU	European Union
FACE	Facial Analysis, Comparison, and Evaluation
FBI	Federal Bureau of Investigation
FIPP	Fair Information Practice Principles
FRT	facial recognition technology
GDPA	General Data Protection Act of 2018
GDPR	General Data Protection Regulation
GIS	geographic information system
HIPPA	Health Insurance Portability and Accountability Act
LAPD	Los Angeles Police Department
LEFG	Law Enforcement Forecasting Group
MLA	machine learning algorithm
NIST	National Institute of Standards and Technology
OCR	optical character recognition
OIG	Office of the Inspector General
PSA	Public Safety Assessment

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Law enforcement is facing a common problem found in the twenty-first century: an expansive growth of data and limited personnel to extract useful trends and analyses from it.[1] The development of artificial intelligence (AI) systems, such as facial recognition and machine learning, present useful tools to address this issue. However, AI systems provide a unique problem for users in the law enforcement domain. On one hand, AI systems provide an opportunity for optimizations and faster workflows, especially in the environment of growing data. On the other hand if left unchecked, AI systems have the potential to negatively affect the community served by law enforcement. These negative effects come in the form of bias and inaccuracies within the systems and secondary effects that are not initially obvious when using AI systems.[2] This begs the question, "How does law enforcement usage of artificial intelligence systems impact the communities they serve?"

This thesis looks at three current uses of AI systems in the law enforcement domain: facial recognition, predictive risk assessments, and predictive policing. These cases are examined by their effectiveness, fairness, privacy, transparency, and accountability to determine how law enforcements' usage impacts their respective communities. When looking at each type of AI system through these criteria, it becomes clear that there are significant considerations to have when using these systems. Without proper policies and regulations in place, AI systems can lead to unjust arrests, unfairly target specific classifications of people, or just may not meaningfully enhance law enforcement operations. Other considerations, such as the Fourth and Fourteenth Constitutional Amendments that provide protections against unreasonable search and seizure and establishes due process, need to be taken into account due to the potential of AI systems to undermine constitutional protections afforded to individuals.

---

[1] John Hollywood et al., *Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group* (Santa Monica, CA: RAND, 2018), https://doi.org/10.7249/RR1987.

[2] Osonde Osoba and William Welser, *The Risks of Artificial Intelligence to Security and the Future of Work*, PE-237-RC (Santa Monica, CA: RAND, 2017), https://doi.org/10.7249/PE237.

These factors do not mean AI systems are doomed or should not be used in the law enforcement domain. However, these findings point to the need for additional research to be conducted into responsible ways for this technology to be used by law enforcement in ways that do not negative impact their communities. Additionally, this is an emerging technology with new development and discoveries on a regular basis. As such, the government is in a perpetual game of cat and mouse, which has led to some municipalities banning the technology outright. Rather than banning the technology, frameworks should be developed to ensure AI systems are used in a responsible manner. The European Union is currently developing a framework with the intention to prevent many of the negative components of AI systems.[3] This work can potentially serve as a starting ground for similar policies and regulations for law enforcement in the United States.

[3] High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI: High-Level Expert Group on Artificial Intelligence," European Commission, 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

ACKNOWLEDGMENTS

Attending the Naval Postgraduate School has been an experience I will never forget, and it would not have been possible without the encouragement and support of many people along the way. First, I would like to thank my wife for her continuous support and encouragement throughout this process. She was always there to push me when I needed it and to listen to me when I needed to talk. Second, I'd like to thank my parents for instilling the values I have in me and being the reason I've gotten into law enforcement and homeland security in general. Their confidence in my abilities has carried me further than my own.

This experience would not have been possible without the support of my command staff at the Department of Public Safety. I know there many times when my absence was a burden and I am grateful for this opportunity to further my education.

Last, but certainly not least, I would like to thank all the staff at the Center for Homeland Defense and Security. The past eighteen months provided many challenges, but all the staff were able to accommodate and maintain the program in a remote environment. I realize this was not an easy task, but it was done with our health and safety in mind.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Artificial intelligence (AI) systems are becoming an ever-present fixture in our society. Whether people realize it or not, it is quite likely the average person interacts with some form of an AI system on a regular basis. AI systems power facial recognition software used to automatically unlock mobile devices, virtual assistants found in household devices, and can even be used to diagnose medical conditions. It is no longer a far-fetched concept only seen in science fiction movies. Currently, AI systems offer convenience, have the potential to enhance workflows, and are becoming increasingly easy to incorporate into everyday activities. There are many potentially positive outcomes when leveraging the capabilities of AI systems, regardless of the industry.

The law enforcement domain in the United States faces many problems that, on face value, are excellent applications for AI. In general, law enforcement is facing growing amounts of data with few personnel that possess the ability to derive analytical insights from data trends. Additionally, many law enforcement agencies strive for data-driven polices, especially in areas to enhance their impact to the communities they serve or to target specific crimes that plague the community. AI and its ability to derive trends from vast datasets provide an opportunity for law enforcement to boost their capabilities and overall service to the community. However, if law enforcement is to leverage this technology, how can citizens be sure AI will actually be beneficial and used in a just manner? This thesis will review current uses of AI systems in the law enforcement domain in an effort to assess their overall effectiveness.

A. PROBLEM STATEMENT

Artificial intelligence has the potential to enhance the workflows, productivity, and effectiveness of individuals and groups that elect to implement the technology. However, potential optimization and enhancement carry the risk of repercussions from AI usage. The risk from technical issues can emanate from the algorithm's design, biases from the data used to train the algorithm, or policy gaps that do not consider the potential effects of this technology.

The public sector has implemented AI systems before, but they are often embroiled in a cloud of controversy due to privacy concerns or legal challenges. This was the case with the COMPAS algorithm implemented by the state of Wisconsin that predicted the risk of releasing offenders on bail.[1] Ultimately, the state of Wisconsin allowed usage of the COMPAS algorithm, and the Supreme Court denied an appeal by the plaintiff.[2] Aside from privacy concerns, other problems include unintended bias against specific populations or potentially misleading outputs. If domestic law enforcement agencies intend to incorporate this new technology into their workflows, these problems can give rise to widespread unintended effects, some negative.

Some existing system design models identify critical considerations regarding the overall process of AI systems, such as algorithmic transparency, which underscores the importance of auditability, transparency, and intelligibility, or the discretion continuum that models when automated decision making by machine learning algorithms (MLAs) would be appropriate.[3] These system design models provide a foundation for the responsible implementation of AI systems in the law enforcement community. Still, law enforcement agencies are generally unwilling or unable to implement this type of new technology due to a lack of policy or oversight to manage the associated risks.[4]

---

[1] *State of Wisconsin v. Eric L. Loomis*, No. 2015AP157- CR (Wis. Ct. App. July 13, 2016); Tim Brennan, William Dieterich, and Beate Ehret, "Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System," Criminal Justice and Behavior 36, no. 1 (October 20, 2008): 21–40, https://doi.org/10.1177/0093854808326545.

[2] Brief for the United States as Amicus Curiae, *Eric L. Loomis, Petitioner v. Wisconsin*, No. 16–6387 (May 2017).

[3] Alexander Babuta, Marion Oswald, and Christine Rinik, *Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges,* Whitehall Report 3–18 (London: Royal United Services Institute, 2018), 17–22, https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical; Emily Berman, "A Government of Laws and Not of Machines," Boston University Law Review 98, no. 5 (October 2018): 1333–55; Auditability refers to the ability of the system processes to be examined. Transparency references either the policies or general availability of a system to be examined by a third party. Intelligibility refers to the ability of an average adult to review and understand the processes implemented by an AI system.

[4] Hollywood et al., *Addressing Emerging Trends to Support the Future of Criminal Justice*, 11.

B. RESEARCH QUESTION

How does law enforcement usage of artificial intelligence systems impact the communities they serve?

C. LITERATURE REVIEW

New law enforcement technologies generally encounter privacy concerns and considerations when they are first implemented. Sacca and Zoufal tell us a great deal about privacy issues regarding emergent technologies, specifically body-worn cameras (BWCs) and closed-circuit television (CCTV).[5] For example, Zoufal focuses on the ability to mitigate privacy concerns by building privacy protections into the system itself.[6] When discussing BWCs, Sacca argues the lack of policies and laws are one of the main contributing limitations to accountability and transparency with BWCs.[7] Even more concerning, Sacca discusses a survey conducted by *USA Today* in which one-third of surveyed police agencies did not have policies in place for BWCs.[8] Their conclusions highlight the same implementation problems facing MLAs and AI within the domestic law enforcement community. Mitigation controls and policies need to be implemented in some fashion to safeguard privacy as required.

Researchers and policymakers concur that the inclusion of MLAs and AI into the decision process requires the consideration of fairness, accountability, and transparency to account for privacy and constitutional concerns appropriately.[9] These conversations fall typically on one of two ends of a spectrum: Either they are incredibly technical and discuss intricacies of specific technical processes, or they are incredibly vague, with generic

---

[5] Donald R Zoufal, "'Someone to Watch Over Me?' Privacy and Governance Strategies for CCTV and Emerging Surveillance Technologies" (master's thesis, Monterey, CA, Naval Postgraduate School, 2008), https://calhoun.nps.edu/handle/10945/4167; Giacomo Sacca, "Not Just Another Piece of Equipment: An Analysis for Police Body-Worn Camera Policy Decisions" (master's thesis, Monterey, CA, Naval Postgraduate School, 2017), https://calhoun.nps.edu/handle/10945/56797.

[6] Zoufal, "Somebody to Watch Over Me," 179.

[7] Sacca, "Not Just Another Piece of Equipment," 86.

[8] Sacca, 85.

[9] Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (Washington, DC: International Association of Privacy Professionals, 2018), 22, https://iapp.org/media/pdf/resource_center/FPF_Artificial_Intelligence_Digital.pdf.

definitions for fairness, accountability, and transparency. Among the former, researchers have identified specific problems with certain algorithms and datasets. As an example, Lucas Dixon effectively demonstrated unintended bias by an AI systems using a dataset from Wikipedia.[10] His team quantifies the amount of bias and even provides a technical solution to account for this bias.[11] However, the process was extremely technical and solution is dependent on the user's ability to understand complex mathematical formulas. This type of information is not easily translated into effective policy, nor is it easily understood by those outside of the subject matter.

On the other side of the spectrum, policymakers and advisors, such as Data & Society and the Future of Privacy Forum, reference the need for "algorithmic accountability," or privacy framing, using fairness, accountability, and transparency, but provide no resources for domestic law enforcement agencies to refer to for further guidance.[12] Both ends of the spectrum provide excellent points and perspectives of the same problem. However, neither takes a proactive step further to provide recommendations to reduce bias with this new technology. As a result, few, if any, implementation guidelines exist for the domestic law enforcement domain, which is likely a significant contributing factor for the slow adoption of this new technology.[13]

Researchers commonly ask, "Is a given MLA or AI ethical?" This question is extremely valuable and should be considered by domestic law enforcement agencies before adopting such technology. Sandvig et al. show multiple ways in which the design and application of MLAs and AI can be unethical by highlighting previous failures in the private industry regarding face detection in commercial cameras, as well as a thought

---

[10] Lucas Dixon et al., "Measuring and Mitigating Unintended Bias in Text Classification," in *Proceedings of AAAI/ACM Conference on AI, Ethics, and Society* (New Orleans, LA, USA: ACM Press, 2018), 68, http://dl.acm.org/citation.cfm?doid=3278721.3278729.

[11] Dixon et al., "Measuring and Mitigating Unintended Bias in Text Classification."

[12] Robyn Caplan et al., *Algorithmic Accountability: A Primer* (Washington, DC: Data & Society Research Institute, 2018), 10–11, https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf; Future of Privacy Forum, The Privacy Expert's Guide to Artificial Intelligence and Machine Learning, 22.

[13] Hollywood et al., *Addressing Emerging Trends to Support the Future of Criminal Justice*, 7–8.

experiment for a new video surveillance system.[14] These findings should caution law enforcement about the increased risk of unethical outcomes accompanying the use of this technology. Domestic law enforcement needs to ensure specific groups will not be targeted because of inadvertently biased AI systems. Ultimately, experts have demonstrated certain ways in which the design and application of MLAs and AI can be unethical in their usage. However, the big picture concerns how domestic law enforcement agencies can identify potential ethical concerns with this technology and how those concerns can be mitigated.

An important distinction to make when using AI systems concerns what is considered ethical versus what is deemed to be legal. There are currently few legal rulings on the usage of AI systems. One of the most prominent cases is State of Wisconsin v. Loomis, which ruled that AI systems can be used to assist with recidivism indicators, provided a disclaimer is used.[15] However, at what point does the usage of AI systems become an invasion of privacy, especially if done by domestic law enforcement agencies? The growing usage of body-worn cameras and facial recognition technology in the domestic law enforcement domain offers some insight into public expectations regarding new technology, and potentially provide policy recommendations to adopt for AI systems. However, these similar yet distinct technologies lack guidance on accountability, fairness and, transparency issues that arise from AI systems interpretation of data.

Perhaps a lack of focus in the United States contributes to these limitations. The research into AI systems is relatively new but is primarily focused on the European Union (EU), as the EU has implemented the General Data Protection Regulation (GDPR). Countries in the EU have either adopted the GDPR or updated their data regulations, such as the United Kingdom and the General Data Protection Act of 2018 (GDPA).[16] These data regulations provide general guidance on how data can be used and when consumers must be informed. The GDPA also provides the right for individuals to know what

---

[14] Christian Sandvig et al., "Can an Algorithm Be Unethical?," in *65th Annual Meeting of the International Communication Association* (San Juan, Puerto Rico: ICA, 2015), http://social.cs.uiuc.edu/papers/pdfs/ICA2015-Sandvig.pdf.

[15] *State of Wisconsin v. Eric L. Loomis*.

[16] Henry Ashton and Matt Hancock, "Data Protection Act 2018," § 2018 Chapter 12 (2018), https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm.

information the government or organizations maintain on them.[17] Specifically relating to law enforcement, the GDPA contains requirements to maintain accountability with data practices and usages.[18] Although provisions and regulations address law enforcement's usage of data, no existing standard assesses how law enforcement can best use MLAs and AI to limit bias and achieve fairness, which could harm citizens.[19]

The United States of America has no federal data policy regulation comparable to the GDPR established by the EU. Some states, such as California, have implemented state-level data regulations, but they are only applicable to residents within California and commercial entities within California state boundaries.[20] Until such a policy that incorporates law enforcement's usage of data is agreed upon and established by the federal government, regulation of AI systems rests with individual agencies. Due to the lack of current case-law or precedent, many agencies will be risk-averse when implementing these new technologies.

D. DEFINITIONS

As previously mentioned, researchers and policymakers agree that AI systems require considerations of privacy, transparency, accountability. In order to evaluate the impact of law enforcement's usage of AI systems, it is also beneficial to assess the effectiveness of the system, equality of individuals before the law, and the underlying fairness of the AI system. Throughout this thesis, these five criteria will be used while assessing various types of AI systems currently used in the law enforcement domain. To provide a common understanding of the identified criteria, they have been defined below.

---

17 Ashton and Hancock, 2.

18 Babuta, Oswald, and Rinik, *Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges*, 29.

19 Babuta, Oswald, and Rinik, 33.

20 "California Consumer Privacy Act of 2018, California Civil Code," § 1798.100 (2018).

1. Effectiveness

A large benefit of AI systems is the ability to be a force multiplier in the workforce. In this thesis, effectiveness is defined as the ability of an AI system to positively impact the workload of a law enforcement agency. If usage of the system is detrimental to the agency or causes difficulties, it would reflect poorly in the effectiveness rating. For example, if an AI system is plagued with accuracy issues, it would be evaluated as "low." If studies have shown that an AI system assisted with enhanced performance, it would be evaluated as "high."

2. Privacy

Americans have a reasonable expectation of privacy, as interpreted by the Fourth Amendment. Granted, there are limitations to this expectation, but those limits have not been codified in regards to data and AI systems. In this thesis, privacy refers to the capabilities of an AI system to "identify, profile, and directly affect" people without their knowledge or consent.[21] For example, if data regarding law-abiding systems is used by law enforcement without the individuals' consent, privacy would be evaluated as "low." If law-abiding citizens have the ability to opt-out of AI systems that may use their data, then privacy would be evaluated as "high."

3. Fairness

Fairness within an AI system has been an ongoing debate within the data science community because there are many ways to define it, and it can vary in different circumstances.[22] For the purposes of this thesis, fairness refers to the likelihood of an AI system to evaluate an outcome without being impacted by some form of bias. For example, an AI system would be considered unfair if it regularly classified black men as more likely to commit crimes than white men, given the only difference is race. This example denotes

---

[21] Michael Deane, "AI and the Future of Privacy," Medium, September 7, 2018, https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4.

[22] Sahil Verma and Julia Rubin, "Fairness Definitions Explained," in *Proceedings of the International Workshop on Software Fairness* (ICSE '18: 40th International Conference on Software Engineering, Gothenburg, Sweden: ACM, 2018), 1–7, https://doi.org/10.1145/3194770.3194776.

a racial bias present in the AI system and would be rated "low" in the fairness category. An unfair AI system used by law enforcement will have a negative impact on the community. If an AI system does not exhibit any bias, it would be evaluated as "high."

4. Transparency

David de Ferrani et al. define transparency in "How to Improve Governance: A New Framework for Analysis and Action" as "the availability and increased flow to the public of time, comprehensive, relevant, high-quality and reliable information concerning government activities."[23] Actions that align with this definition are the disclosures of budget and policies to the public for review and awareness.[24] For the purposes of this thesis, this definition equates to the ability of the general public to have access to and review any policies governing the usage of AI systems by law enforcement. Transparency provides insight into how law enforcement is using technology and informs the public regarding its usage. For example, if law enforcement is unwilling to provide information regarding their usage of AI systems, transparency would be considered "low." If information regarding an AI system or its policies is publicly available, it would be evaluated as "high."

5. Accountability

From the same work, Ferranti et al. define accountability as "the responsiveness on the part of government to citizens' demands concerning the type of public services the public sector should provide."[25] Regarding law enforcement projects, this equates roles such as Inspector Generals or auditors that can review information to ensure systems are being used properly. Ideally, the oversight provided by those roles will help determine resources are being used effectively to serve the community and ensure compliance with any established policies or procedures. This is an extremely important aspect with regards to AI systems in the United States because there are no federal regulations on this

---

[23] David de Ferranti et al., *How to Improve Governance: A New Framework for Analysis and Action* (Brookings Institution Press, 2009), 7.

[24] de Ferranti et al., 7.

[25] de Ferranti et al., 7.

technology or a modern data privacy act to ensure information is used in an appropriate manner. For example, if law enforcement does not regularly audit the usage of their system or if the AI system simply isn't able to be audited, accountability would be rated as "low." If law enforcement regularly audits user activity within the AI system, accountability would be evaluated as "high."

E. RESEARCH DESIGN

This thesis will use an inductive case study format as described by Jack Levy, which aims "to describe, explain, interpret, and/or understand a single case as an end in itself."[26] Facial recognition, predictive risk assessment, and predictive policing AI systems have been identified as specific cases to be studied. Within each type of AI system, at least one specific case will be assessed. As previously described and seen throughout the literature review, effectiveness, privacy, fairness, transparency, and accountability will be used as the primary assessment criteria. These categories are instrumental to the responsible usage of AI systems, as they speak to the impact of AI systems in the social and political realms, as well as the practicality to law enforcement agencies and legality of the technology.

The provided criteria will be evaluated primarily using qualitative metrics, as it is challenging to ascertain quantitative metrics for topics such as privacy and fairness. However, each criterion will be evaluated with a value of "low," "medium," or "high," depending on how well that topic is addressed for that category. After analyzing all options by the identified criteria, this thesis intends to provide policy option recommendations for responsible utilization of MLAs and AI by law enforcement agencies.

Information to assess these policy options will be acquired through publicly available documents and scholarly research into the topic of AI systems. Currently, little prescriptive policy work exists in the United States. However, the European Union is currently developing policy guidance that will further inform this thesis and potential

[26] Jack S. Levy, "Case Studies: Types, Designs, and Logics of Inference," *Conflict Management and Peace Science* 25, no. 1 (February 2008): 4, https://doi.org/10.1080/07388940701860318.

policy options.[27] Where applicable, this thesis will also use current federal legislation, as well as any policies implemented at law enforcement agencies employing this technology. Although the subject of AI systems is highly technical in nature, the intent of this thesis is not to be technical but to determine the best path for responsible implementation of AI technology through policy. Any policy recommendations identified through this process should be specific enough to address the defined criteria, but elastic enough that they do not become obsolete as the technology evolves.

Potential challenges with this research design include the ever-changing nature of this technology. On a regular basis, new information regarding this technology is made available, whether it involves advancements in the technology itself or the creation and/or approval of new regulatory measures for the technology. An example of this limitation is the growing number of municipalities working towards an outright ban of facial recognition systems within their jurisdictional authorities.

F. THESIS OUTLINE

This chapter demonstrated the need for further research into the provided research question. As law enforcement agencies incorporate AI systems into their processes, there exists a need to examine the impact on the communities they serve. Five criteria have been provided and define for the evaluation of three different types of AI systems. Chapter II provides a technology overview of many AI systems in use by law enforcement today. The overview is not technical in nature, but provides enough information for a general understanding of how the technology works. Chapters III through V provide case studies and analysis on facial recognition, predictive risk assessment, and predictive policing AI systems. Each chapter concludes with an evaluation based on the five defined criteria. Chapter VI reviews the analysis of each case study while discussing the generalized impact of law enforcement's usage of AI systems. It concludes with a look at an AI framer European Union has developed.

---

[27] European Commission, *On Artificial Intelligence - A European Approach to Excellence and Trust,* COM(2020) 65 Final (Brussels: European Commission, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN.

II. ARTIFICIAL INTELLIGENCE SYSTEMS

This chapter will provide a brief overview of AI systems currently used by law enforcement agencies across the United States. Specifically, this chapter discusses automated license plate readers, facial recognition, and predictive analytic AI systems. Although technical details are not provided, a brief non-technical overview of the technology is given, and a discussion on some of the challenges law enforcement agencies may have when utilizing these systems.

In 2012, the Bureau of Justice Assistance Law Enforcement Forecasting Group (LEFG) outlined the benefits for law enforcement agencies to possess an analytic function, primarily through intelligence-led policing.[28] However, the LEFG identifies potential problems law enforcement agencies should prepare for, such as the unprecedented growth of available information.[29] The LEFG argues this growth of data as reasoning to further invest in analytical resources in the law enforcement domain.[30] Approximately six years later, in 2018, the RAND Corporation worked with the Bureau of Justice Assistance to assess the impact technology can have on law enforcement processes.[31] A significant finding of this assessment involved the challenges of big data and analytics, namely the general lack of understanding of new technology in most law enforcement agencies and the risks posed by implementing these new technologies. These risks range from accuracy issues experienced with AI systems, biases that unfairly impact one group of people over another, to due process concerns when using predictive policing.

As anticipated by the LEFG, law enforcement agencies face a data and technology problem, namely large amounts of data with limited expertise in data analytics. To handle this influx of available data, law enforcement agencies need to leverage technology to

---

[28] Law Enforcement Forecasting Group, *Increasing Analytic Capacity of State and Local Law Enforcement Agencies: Moving Beyond Data Analysis to Create a Vision for Change,* 2010-DB-BX-K003 (Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice, 2012), 5, https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/LEFGIncreasingAnalyticCapacity.pdf.

[29] Law Enforcement Forecasting Group, 15.

[30] Law Enforcement Forecasting Group, 15.

[31] Hollywood et al., *Addressing Emerging Trends to Support the Future of Criminal Justice*, xi.

assess their growing datasets. There are many types of technology available to help with the influx of data, but this thesis focuses on artificial intelligence (AI) specifically. AI encompasses a growing capability that can potentially assist law enforcement with this predicament of increasing volumes of information that need to be analyzed; however, there are risks that agencies should know.

A. TECHNOLOGY OVERVIEW

In general terms, AI is split into two main categories: Narrow AI and General AI.[32] General AI refers to the type of intelligent behavior one would expect from an average person in a wide variety of tasks.[33] This is typically the type of AI that is portrayed in science fiction movies. Most experts agree that General AI will not be achieved for decades.[34] However, Narrow AI is widely used today in a variety of scenarios and sectors. In fact, the digital assistant on your mobile devices such as Siri or Alexa would be considered Narrow AI.

Narrow AI encompasses applications to specific use cases, such as self-driving vehicles, facial recognition, or other narrowly defined tasks.[35] These problems are typically solved through statistical analyses, machine learning algorithms, or rule-based logic. Most of the applications in this thesis will encompass machine learning algorithms, which can be categorized into supervised machine learning and unsupervised machine learning.[36] Supervised machine learning generally provides a training data set that contains the data itself and the outcome. In supervised machine learning, the desired result is a

[32] National Science and Technology Council, *Preparing for the Future of Artificial Intelligence (*Washington, DC: Executive Office of the President, 2016), 7, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

[33] National Science and Technology Council, 7.

[34] National Science and Technology Council, 7.

[35] National Science and Technology Council, 7.

[36] Field Cady, *The Data Science Handbook* (Hoboken, NJ: John Wiley & Sons, Inc, 2017), 89.

reliable algorithm to estimate the output.[37] Unsupervised machine learning only requires raw data, and the algorithm is expected to find underlying patterns in the data itself.[38]

B. CURRENT USAGE IN LAW ENFORCEMENT

Usage of AI systems by law enforcement is not a foreign concept by any stretch of the imagination. As of 2020, there are many vendors that offer various types of tools to aid law enforcement operations via AI systems. These vendors' capabilities range from enhancing license plate readers, facial recognition systems, and predictive policing applications. While these capabilities do not represent the complete potential of AI systems, they provide some of the most common and current use cases for law enforcement in the United States.

1. Automated License Plate Readers

Automated license plate readers (ALPR) are currently used throughout the nation as a force multiplier by law enforcement agencies. ALPR technology allows law enforcement agencies to automate the process of running license plates through specific "hotlists" to determine if the vehicle is associated with any alerts, wanted individuals, or bulletins.[39] This is accomplished through the usage of high-speed cameras that capture images of license plates, optical character recognition (OCR) via types of AI systems to detect the characters of the license plate, and "hotlists" that contain license plate information of interest to law enforcement.[40] If the ALPR system is able to identify license plates that match the provided "hotlists," alerts are delivered to officers for confirmation and action. This ALPR process vastly improves the investigative capabilities of law enforcement by automating the process of detecting vehicles of interest throughout an

---

[37] Cady, 89.

[38] Cady, 89.

[39] David J Roberts and Meghann Casanova, *Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide*, Summary, 239605 (Alexandria, VA: International Association of Chiefs of Police, 2012), 1, https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf.

[40] Roberts and Casanova, 1–2.

officer's day in a passive manner. No action is required of the officer until a "hotlist" vehicle is detected.

For ALPR systems, AI is used explicitly in the OCR portion of the process. For these systems to be successful, image analysis and character recognition need to be fast so that information can be shared back to law enforcement in near real-time. Continuous improvement of OCR capabilities is achieved by advancing AI systems for faster and more reliable detection and character classification.[41]

2. Facial Recognition

Facial recognition technology (FRT) has been around longer than many may expect. FRT was initially developed in the 1960s by Woodrow Bledsoe.[42] This process worked by manually recording measurements between facial features, which were later stored in databases for easy comparisons to other measurements.[43] Since the 1960s, FRT has become a biometric identifier, meaning it is an "automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual."[44]

Currently, FRT is used heavily by law enforcement agencies and is an integral part of the Federal Bureau of Investigation's (FBI) Next Generation Identification program, which currently allows law enforcement to submit photos to be searched against over thirty million criminal mug shot photos.[45] Additionally, some vendors provide FRT access at a low barrier to entry when considering cost or technical set up. In the early 2020s, there are

---

[41] Riel D. Castro-Zunti, Juan Yépez, and Seok-Bum Ko, "License Plate Segmentation and Recognition System Using Deep Learning and OpenVINO," *IET Intelligent Transport Systems* 14, no. 2 (February 1, 2020): 125, https://doi.org/10.1049/iet-its.2019.0481.

[42] Divyesh Dharaiya, "History of Facial Recognition Technology and Its Bright Future," readwrite, March 12, 2020, https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/.

[43] Dharaiya.

[44] John D. Woodward Jr. et al., *Biometrics: A Look at Facial Recognition* (Santa Monica, CA: RAND Corporation, 2003), 1, https://apps.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf.

[45] "Next Generation Identification (NGI)," Federal Bureau of Investigation, accessed September 4, 2020, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

two vendors worth noting, Amazon Web Services and Clearview AI, due to their ease of use and potentially controversial nature, which will be discussed in the next section.

Regarding FRT, AI systems have played a large contributing factor in the rapid development and dependability of the FRT over the past ten years. Breakthroughs in AI systems technology, such as neural networks, have allowed FRT to become more efficient and accurate than before.[46]

3. Predictive Analytics

In "A Review on Predictive Analytics in Data Mining," the authors define predictive analytics as a process that utilizes "various techniques from machine learning, statistics, data mining, modeling and artificial intelligence for analyzing the current data and to make predictions about the future."[47] In the law enforcement domain, predictive analytics can be used on "criminal, traffic, and civil (CTC) incident datasets" to predict where and when future incidents are most likely to occur based on previously collected data.[48]

Perhaps the most notable usage of predictive analytics in the criminal justice system is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm. This algorithm is in use by courts to assess an offender's likelihood to recidivate based on "more than 100 factors, including age, sex, and criminal history."[49] Although

---

[46] Stephen Shankland, "Boosted by AI, Facial Recognition Eases Our Path Through an Increasingly Digital World," CNET, March 28, 2019, https://www.cnet.com/news/huge-leaps-in-ai-have-made-facial-recognition-smarter-than-your-brain/.

[47] V. Kavya and S. Arumugam, "A Review on Predictive Analytics in Data Mining," International *Journal of Chaos, Control, Modelling and Simulation* 5, no. 1/2/3 (September 30, 2016): 1, https://doi.org/10.5121/ijccms.2016.5301.

[48] Abish Malik et al., "Proactive Spatiotemporal Resource Allocation and Predictive Visual Analytics for Community Policing and Law Enforcement," *IEEE Transactions on Visualization and Computer Graphics* 20, no. 12 (2014): 1863, 1871, https://doi.org/10.1109/TVCG.2014.2346926.

[49] Sam Corbett-Davies et al., "Algorithmic Decision Making and the Cost of Fairness," in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,* KDD '17 (Halifax, NS, Canada: Association for Computing Machinery, 2017), 1, 10.1145/3097983.3098095.

there is a substantial amount of concern and controversy over the COMPAS algorithm usage, the Wisconsin State Supreme Court upheld its use.[50]

Predictive analytics is also currently used by law enforcement to help determine optimized patrol routes to deter crime. Agencies like the Los Angeles Police Department, the New York Police Department, and the Chicago Police Department all have some form of predictive analysis to assist with their staffing assignments and strategies.[51] This is accomplished through AI systems that are either procured, such as PredPol, or developed internally with subject matter staff. These AI systems can analyze enormous data sets to determine correlations between identified data elements, such as date/time, location, and crime type.[52]

C. POTENTIAL ISSUES WITH AI SYSTEMS

There are potential issues that law enforcement agencies need to consider before using any type of AI system. Some of the potential problems that warrant attention are potential accuracy, privacy, and constitutional issues. Law enforcement should consider these issues because there can be ramifications that impact the agency itself or even the individuals subject to these AI systems.

1. Potential Accuracy Issues

Osonde Osoba and William Welser IV make an excellent argument that "most algorithms have only probabilistic guarantees of accuracy" because it is nearly impossible to have a perfect dataset or process that can account for nearly every outcome.[53] Inaccuracies in AI systems can come from many places and are not simply limited to the algorithm used to derive conclusions. Issues regarding the outcome can also stem from

---

[50] *State of Wisconsin v. Loomis,* No. 2015AP157- CR (Wis. Ct. App. July 13, 2016).

[51] Tim Lau, "Predictive Policing Explained," Brennan Center for Justice, April 1, 2020, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[52] Lau.

[53] Osonde Osoba and William Welser*, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence* (Santa Monica, CA: RAND Corporation, 2017), 3–4, https://www.rand.org/pubs/research_reports/RR1744.html.

underlying collection procedures, poorly defined algorithms, or an outright over-reliance on the AI system itself.[54] These accuracy problems can lead to potential bias issues within AI systems. The website "Towards Data Science" refers to algorithmic bias as "the lack of fairness that emerges from the output of a computer system."[55]

Accuracy and bias can emerge from multiple places within an AI system. When trained on a dataset, non-obvious historical biases found in the training dataset may continue to enforce those biases.[56] Bias can also come from the methodologies used by developers writing the software of the AI system. Whether or not it is intentional, software developers' choices can impart bias in the system's outcomes.[57]

These inaccuracies and biases can lead to unfairness by disproportionately affecting certain groups of people. As an example that will be explored further, multiple court systems have used a predictive risk assessment AI system to evaluate offenders' likelihood to recidivate. Studies have indicated that black offenders are typically assessed at a higher risk than white counterparts.[58] Accuracy and bias issues can be troublesome if experienced while in use by law enforcement agencies, resulting in wrongful arrests of individuals based on inaccurate AI system returns.

2. Potential Privacy Issues

The Fair Information Practice Principles (FIPPs) are comprised of eight principles central to the Privacy Act of 1974 and are central to many laws at the state and federal

---

[54] Osoba and Welser, 4.

[55] Richmond Alake, "Algorithm Bias In Artificial Intelligence Needs To Be Discussed (And Addressed)," Medium, April 28, 2020, https://towardsdatascience.com/algorithm-bias-in-artificial-intelligence-needs-to-be-discussed-and-addressed-8d369d675a70.

[56] Matthew Guariglia, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing," Electronic Frontier Foundation, September 3, 2020, https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing.

[57] Sandvig et al., "Can an Algorithm Be Unethical?," 2.

[58] Jeff Larson et al., "How We Analyzed the COMPAS Recidivism Algorithm," ProPublica, May 23, 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

level.[59] These eight principles are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.[60] These principles intend to provide privacy protections to the individuals whose data is contained within databases and used by various data systems, including AI systems.

However, Solon Barocas and Helen Nisenbaum make the argument that with the introduction of big-data analytics, machine learning, and artificial intelligence, there are limitations that can be expected to privacy, especially in terms of consent and anonymity.[61] For example, with enough data, AI systems can infer information about people without obtaining consent from the individual for the information. An example used by Barocas and Nisenbaum to highlight this point is purchase history at Target. Using enough data, Target could infer when women were pregnant based on their purchase history, regardless of whether the customer had consented to share that type of information.[62] In a similar fashion, when only anonymous records are kept, generally, there is enough information to identify that individual without relying on personally identifiable information.[63]

3. Potential Constitutional Issues

One of the largest constitutional issues to keep in mind with AI systems is due process. Due process as described in the Fifth Amendment to the Constitution states the following:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of war or public danger; nor shall any person be subject for the same

---

[59] Hugo Teufel III, "Privacy Policy Guidance Memorandum," official memorandum (Washington, DC: U.S. Department of Homeland Security, December 29, 2008), 1–2, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

[60] Teufel III, 3–4.

[61] Solon Barocas and Helen Nissenbaum, "Big Data's End Run Around Procedural Privacy Protections," *Communications of the ACM* 57, no. 11 (November 2014): 31–33, https://doi.org/10.1145/2668897.

[62] Barocas and Nissenbaum, 32.

[63] Barocas and Nissenbaum, 32–33.

> offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.[64]

Similarly, the Fourteenth Amendment references due process in Section One by stating, "nor shall any State deprive any person of life, liberty, or property, without due process of law."[65] Cornell Law School interprets due process outlined in the Constitution as limitations put upon the state that must be followed before depriving a citizen of life, liberty, or property. Simply put by Cornell Law School, "it is not always enough for the government just to act in accordance with whatever law there may happen to be. Citizens may also be entitled to have the government observe or offer fair procedures, whether or not those procedures have been provided for in the law on the basis of which it is acting."[66] This interpretation puts the onus on government entities to implement fair procedures before taking action that may inhibit a citizen's life, liberty, or property. How does this relate to AI systems?

In AI systems, there is the concept of "black-box" algorithms. These are algorithms where the operations performed on inputs are not directly observable or interpretable by the user.[67] This process has been compared to using canines to search for narcotics or illicit goods. It is unknown how the canine can detect the material, but they are trained to perform the task with high accuracy and repeatability.[68] However, unlike highly trained canines, algorithms do not go through an intense accreditation certification to verify their capabilities. This issue of due process relating to AI systems was at the center of the Loomis v. Wisconsin (2016) case regarding the usage of the COMPAS algorithm. In this case, the

---

64 "The Bill of Rights: A Transcription," National Archives, November 4, 2015, https://www.archives.gov/founding-docs/bill-of-rights-transcript.

65 "U.S. Const. Amend. XIV," § 1, accessed September 13, 2020, https://constitution.congress.gov/browse/amendment-14/.

66 Peter Strauss, "Due Process," Cornell Law School Legal Information Institute, accessed September 13, 2020, https://www.law.cornell.edu/wex/due_process.

67 Margaret Rouse, "What Is Black Box AI?," WhatIs, accessed November 21, 2019, https://whatis.techtarget.com/definition/black-box-AI.

68 Emily Berman, "A Government of Laws and Not of Machines," *Boston University Law Review* 98, no. 5 (October 2018): 1319–20.

courts decided other factors were considered to refuse Loomis' parole, and thus his due process rights were not violated.[69] However, in Kansas v. Walls (2017), an opposite verdict was found. In this case, the courts found the defendant was denied their due process rights when the district court refused to provide the full automated assessment that was relied upon for determining probation requirements.[70] Without the foresight to provide guidance on AI systems, there is the real possibility to infringe on protected constitutional rights.

D. SUMMARY

This chapter provides an overview of different types of AI systems available to law enforcement and a non-technical review of how these systems work. AI systems are commonly found in automatic license plate readers, facial recognition, and predictive analytics. When using these systems, some risks should be considered by law enforcement. Although this is not an all-encompassing list, there are potential risks regarding the system's accuracy, the privacy of the individuals subject to the system, and the constitutional rights of individuals subject to the AI system.

[69] Aleš Završnik, "Criminal Justice, Artificial Intelligence Systems, and Human Rights," ERA Forum, *Journal of the Academy of European Law* 20, no. 4 (February 2020): 573, https://doi.org/10.1007/s12027-020-00602-0.

[70] Završnik, 574.

III. CASE STUDY 1: FACIAL RECOGNITION

The first case study addressed in this analysis is the usage of facial recognition artificial intelligence systems by law enforcement agencies. As of 2016, it is estimated that more than one in four law enforcement agencies have access to facial recognition AI systems.[71] Deployments of this technology can range from tight integration with other services, such as live video streaming, to an outright ban of the technology altogether. In fact, with the lack of federal guidance on data protection, privacy, and AI systems in general, many local municipalities have made efforts to regulate the technology within their jurisdiction. This has been a growing approach from 2018 to 2020, with cities like San Francisco, CA, Oakland, CA, Portland, OR, and Boston, MA implementing some form of restrictions on the technology, citing the need to protect their constituents' privacy and civil liberties.

Some cities implementing bans on facial recognition technology also have additional sections addressing surveillance technology. The City of San Francisco defines surveillance technology as "any software, electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory, or similar information specifically associated with, or capable of being associated with, any individual or group."[72] According to this definition, it is reasonable to conclude that AI systems, in general, and not those solely limited to facial recognition, will be subject to similar policies in these cities.

This chapter will examine the usage of facial recognition AI systems by law enforcement agencies, as well as recent regulations implemented to address growing

---

[71] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Washington, DC: Center on Privacy and Technology at Georgetown Law, 2019), 25, https://www.perpetuallineup.org/.

[72] "Acquisition of Surveillance Technology, San Francisco, CA, Administrative Code," § 19 (2019), sec. 19B.1, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

concerns regarding the technology. This chapter will conclude with an analysis of five criteria: effectiveness, privacy, fairness, transparency, and accountability.

A. OVERVIEW

Law enforcement agencies currently utilizing facial recognition AI systems commonly use it in one of four ways:

1. Stop and Identify. When an individual is unwilling or unable to identify themselves, the responding officer takes a picture of the individual for processing in the facial recognition system.[73]

2. Arrest and Identify. When an individual is arrested, part of the booking process is the collection of biometric data, such as fingerprints and a mugshot. In this case, the mugshot is archived in the facial recognition software to be used for future queries.[74] It can also be shared with other law enforcement agencies for similar purposes, such as the FBI.[75]

3. Investigate and Identify. If the face of a suspect is available on a piece of evidence during an investigation, a photo of the face is run through facial recognition to provide any available leads.[76] If there are no matches, the photo is archived for future use, similar to a mugshot.[77]

4. Real-time Video Surveillance. If law enforcement is searching for a specific individual, a "hot list" can be created to search through live video feeds.[78] If a potential match is found, the system alerts users to the possible match.

---

[73] Garvie et al., *The Perpetual Line-Up*, 11.

[74] Garvie et al., 11.

[75] Federal Bureau of Investigation, "Next Generation Identification (NGI)."

[76] Garvie et al., *The Perpetual Line-Up*, 11–12.

[77] Garvie et al., 11–12.

[78] Garvie et al., 12.

It is difficult to refute the usefulness of this technology for law enforcement, as there are many instances where it has provided vital breakthroughs in investigations, ranging from credit card fraud, road rage, missing persons, to other violent crimes.[79] However, where there are success stories of the technology, there exist failures as well. These failures most often disproportionately affect non-white individuals. As of January 2021, there have been at least three black men that have been arrested based on bad facial recognition matches and have pending litigation on the matter.[80]

Currently, four major cities in the United States have established some ban on facial recognition. Since there are no federal regulations regarding this technology, each municipality decided to regulate this technology within their respective jurisdictions, often citing the need to protect their constituents' privacy and civil liberties. These four cities are San Francisco, CA; Oakland, CA; Portland, OR; and Boston, MA. These bans on facial recognition technology, sometimes called "face surveillance," started receiving attention in 2019, when San Francisco was the first municipality to ban the technology's usage by any city department.

The city ordinances used to ban facial recognition technology typically highlight multiple concerns regarding the technology. Nearly all cities express concerns regarding the potential of unintended bias in the outcome, primarily when law enforcement agencies use the technology. The City of Portland explicitly calls out "concerns around privacy, intrusiveness, and lack of transparency."[81]

All of these city ordinances preclude usage or ownership of facial recognition technology by all city departments, but specifically call out concerns relating to law enforcement's use of the technology. This regulation also extends to information received by other agencies, as well. Many law enforcement agencies included under these city

---

[79] Jon Schuppe, "How Facial Recognition Became a Routine Policing Tool in America," NBC News, May 11, 2019, https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

[80] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[81] "Portland, OR, Ordinance No. 190113" (2020), sec. 1.9.

ordinances are prohibited from requesting data retrieved from facial recognition analysis performed by other agencies not restricted by these ordinances.

Despite these restrictions on facial recognition technology, there are some generally accepted exceptions to these city ordinances. As more devices begin to leverage some form of facial recognition to unlock devices, such as iPhones, city-issued devices used for communication purposes are generally allowed to use facial recognition technology. Social media providers, such as Facebook, automatically integrate facial recognition into photos uploaded to their platform. Although privacy relating to facial recognition is a considerable concern for city municipalities, this practice is still allowed. Lastly, facial recognition technology can also be used to protect individuals' privacy by detecting a face and redacting or blurring the media.

B. EXAMPLES

In February 2019, Woodbridge Police Department responded to a shoplifting call where the suspect attempted to flee after the officers confronted the suspect. While fleeing, the suspect left a falsified Tennessee driver's license and nearly ran over one of the officers.[82] Woodbridge shared the false photo identification with other law enforcement agencies in the area in an attempt to locate the suspect.[83] A partner agency utilized facial recognition on the photo, which came back to Nijeer Parks, who lived over 30 miles away from the incident.[84] Despite having a solid, verifiable alibi, Mr. Parks was detained for ten days at the local corrections center without bail due to prior convictions.[85] In November 2019, the case was dismissed by the courts, citing a lack of evidence.[86]

[82] Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match."

[83] Hill.

[84] Hill.

[85] Hill.

[86] Hill.

In May 2019, Michael Oliver was charged with a felony count of larceny after being accused of stealing a teacher's cell phone and destroying the device.[87] Facial recognition was used to identify Mr. Oliver as a person of interest, and a witness to the incident identified Mr. Oliver during a photo lineup.[88] It wasn't until a review of video evidence that it became obvious that Mr. Oliver was not involved in the incident, and law enforcement dropped the charges in September 2019.[89]

In January 2020, law enforcement served a larceny felony warrant to Robert Williams in Detroit, MI.[90] The main piece of evidence used in his arrest was a facial recognition return taken from surveillance video, depicting a similar-looking man stealing thousands of dollars of merchandise at a high-end retailer. Mr. Williams was detained for over twenty-four hours before being released.[91] Despite being released, he still needs to go through the expungement process to make sure any record of this arrest is not kept on file.[92]

These three incidents are potentially the first three cases in which individuals have been incorrectly arrested based on the usage of facial recognition technology.[93] All three individuals from these incidents were black, which highlights additional concerns about the technology, its reliability, and any bias that may be present in the system. These concerns will be discussed in more depth in the following section of this chapter.

Despite these incidents and potential issues, facial recognition continues to be used by at least one in four law enforcement agencies, as estimated by Georgetown Law Center

---

87 Elisha Anderson, "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit," *Detroit Free Press, July* 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

88 Anderson.

89 Anderson.

90 Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times,* June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

91 Hill.

92 WCPO Statement in Response to New York Times Article Wrongfully Accused by an Algorithm, June 24, 2020, WCPO Press Release (Detroit, MI: County of Wayne, 2020).

93 Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match."

on Privacy and Technology.[94] Currently, it is difficult to determine how useful facial recognition is to law enforcement, as metrics that would help address this question are not required to be published. There is no doubt facial recognition helps law enforcement with identification and investigative purposes, but most agencies using the technology are not transparent on the matter. The FBI Facial Analysis, Comparison, and Evaluation (FACE) Services Unit is arguably one of the largest facial recognition systems currently in use by law enforcement, with access to over 641 million photos comprises driver license photos, mug shots, and corrections photos from over twenty participating states.[95] From August 2011 to April 2019, the FACE program received 153,636 probe photos resulting in 390,186 searches in the system.[96]

C. ISSUES

Despite facial recognition's ability to assist in law enforcement investigations, there are some serious issues with the technology that are worth considering and can have an impact on the overall outcome. Firstly, it is becoming more evident that facial recognition is less effective on minority groups of people.[97] In December 2019, the National Institute of Standards and Technology (NIST) published their third study on vendor based facial recognition platforms. The first two studies covered performance issues in different types of systems, but the third study focused on "accuracy variation across demographic groups."[98] NIST found that individuals with a country of origin listed as Africa consistently have higher false matching rates within their demographic group. At times,

---

94 Garvie et al., *The Perpetual Line-Up.*

95 Gretta L. Goodwin, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains,* GAO-19-579T (Washington, DC: Government Accountability Office, 2019), 5–6.

96 Goodwin, 6.

97 Fabio Bacchini and Ludovica Lorusso, "Race, Again: How Face Recognition Technology Reinforces Racial Discrimination," *Journal of Information, Communication and Ethics in Society* 17, no. 3 (August 2019): 331, https://doi.org/10.1108/JICES-05-2018-0050.

98 Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test Part 3: *Demographic Effects*, NISTIR 8280 (Gaithersburg, MD: National Institute of Standards and Technology, 2019), 1, https://doi.org/10.6028/NIST.IR.8280.

this rate was 100 times more than the baseline rate seen throughout the study.[99] Although not quite as severe, individuals with a country of origin listed as east Asia experienced a higher false matching rate, too.[100] These findings demonstrate accuracy issues encountered with many modern facial recognition systems. Without proper procedures established at law enforcement agencies, reliance on these systems can result in erroneous arrests, as experienced by the three gentlemen discussed earlier.

Secondly, there are limited policies and accountability reports available to the public regarding law enforcement's usage of facial recognition technology. In Georgetown's 2016 study on facial recognition, a total of over 100 agencies were surveyed for information on how their agency uses facial recognition. Of these responses, Georgetown was able to determine of the respondents, 52 agencies have either currently using or have used facial recognition in the past.[101] Of these agencies, four agencies make their usage policies publicly available.[102] Only two responding agencies, the San Francisco Police Department and Michigan State Police, had accuracy requirements in place for procurement.[103] Since the Georgetown study's publication, the city of San Francisco has outright banned the usage of facial recognition, including usage for law enforcement. Michigan State Police was the only responding agency that provided evidence of routine audits on the system to prevent misuse of the technology.[104]

Policies and audits regarding this technology provide an essential measure of accountability for this technology, mainly because most law enforcement agencies do not require formal declarations, such as a warrant, to use the technology.[105] In most cases, there are no updated privacy laws in place that effectively speak to the recent enhancement

99 Grother, Ngan, and Hanaoka, 34–41.

100 Grother, Ngan, and Hanaoka, 34–41.

101 Garvie et al., *The Perpetual Line-Up*, 15.

102 Garvie et al., 51.

103 Garvie et al., 49.

104 Garvie et al., 60.

105 Garvie et al., 37.

of technology.[106] This point leads to the last issue to be discussed regarding agencies that do utilize facial recognition technology: there are few, if any, protections for the individual. If there are any protections granted by courts or legislation, they vary by state. California is the only state to have passed an updated data privacy act, the California Consumer Protection Act (CCPA), and it is only applicable to residents of California. Although this legislation does not directly regulate how law enforcement can use data, it does provide protections to individuals by requiring the business to inform consumers what data is collected on them and how it is used. This is extremely important, as facial recognition vendors are using consumer data to create and train facial recognition systems, with the intent to sell access to law enforcement customers.

D. CRITERIA ANALYSIS

Each AI system is evaluated based on five criteria: effectiveness, privacy, fairness, transparency, and accountability. Each criterion will be provided a score of either low, medium, or high and will be determined by constraints, problems, or successes caused by each policy that is assessed. Based on each criterion's outcome, an average score will be generated for comparison to the other AI systems.

1. Effectiveness—Low

Facial recognition has proven to be a useful tool for law enforcement by providing investigative leads in cases and identifying individuals quickly. However, there are few, if any, policies guiding effective usage of the technology or regular auditing to ensure the technology is not abused by users. Since 2019, multiple people have erroneously been arrested due to inaccurate facial recognition returns. Additionally, facial recognition technology has been shown to be less accurate among certain populations, particularly black individuals. Due to these limitations of facial recognition, whether through policy, legislation, or accuracy, effectiveness has been evaluated as "low."

[106] Garvie et al., 43–44.

2. Privacy—Low

The most considerable privacy concern for law enforcement usage of facial recognition technology is the lack of regulations on the technology. These regulations could come in the form of agency policies or legislative requirements that define proper circumstances for the technology's use or outline court ordered requirements, such as a warrant, before these systems are used. As previously discussed, research has found that, generally speaking, facial recognition technology is commonly used by law enforcement agencies without any of these regulations.

As more agencies expand their facial recognition programs to include driver's license and identification photos, additional privacy concerns are warranted. By using these photos, it could be argued that a "dragnet biometric database" has been created that not only contains criminal actors, but law-abiding citizens as well.[107] Due to the lack of regulation and the general inclusion of law-abiding citizens' data, privacy has been considered "low."

3. Fairness—Low

As previously discussed, studies have demonstrated, facial recognition is not as accurate for specific groups of people, namely black individuals, and they are more likely to experience false match returns from the facial recognition system. This has led to multiple instances where the wrong person was incorrectly identified and subsequently arrested. At times, some facial recognition AI systems have seen inaccurate, false match rates exceeding 100 times that of the baseline evaluations.[108] Although this accuracy issue is likely not intentional, it does impact specific demographics disproportionately and could be considered an unfair practice if left unchecked. Due to this consideration, fairness has been evaluated as "low."

---

[107] Garvie et al., 57.

[108] Grother, Ngan, and Hanaoka, Face Recognition Vendor Test Part 3, 1.

4. Transparency—Low

In this context, transparency relates to the policies in place for the usage of facial recognition at law enforcement agencies. As the Georgetown study shows, very few law enforcement agencies have publicly shared any policies or procedures for transparency when using facial recognition technology. Without documentation publicly available or legislation governing the use of this type of technology, it is nearly impossible for those outside the law enforcement agency to know how facial recognition is used. Of the responsive agencies surveyed by Georgetown, less than eight percent make their facial recognition policy publicly available, and even less had legislative oversight or approval.[109] Due to these factors, transparency has been evaluated as "low."

5. Accountability—Low

Similar to transparency, there are very few agencies with publicly available information regarding their attempts to audit their agency's usage of facial recognition systems. Internal audits are an essential component of accountability, as audits are a primary driver to ensure systems and processes are not abused or improperly used. According to the Georgetown study, ten of the fifty-two responding agencies "indicated that they audit their employees' use of the face recognition system for improper use."[110] However, only one responsive agency provided evidence that audits are conducted regularly to ensure compliance with system use.[111] The lack of proper internal audits on facial recognition system use is considered a lapse in accountability, which has been evaluated as "low."

E. SUMMARY

This chapter evaluated the usage of facial recognition AI systems by law enforcement and some of the challenges with the technology. In its current state, the accuracy rates of facial recognition systems impose challenges, especially since accuracy

---

[109] Garvie et al., The Perpetual Line-Up, 58.

[110] Garvie et al., 60.

[111] Garvie et al., 60.

issues tend to impact certain groups of people. This challenge, coupled with the lack of regulation at either the agency or legislative levels, leads to unique situations, such as the erroneous arrests of individuals due to inaccurate facial recognition returns.

When evaluated across effectiveness, privacy, fairness, transparency, and accountability, the technology is assessed as “low” across the board. Since this is a new technology, it is not unreasonable to expect a lag before any reasonable policies or legislation are drafted and enacted. However, until such regulations are approved and implemented, there are serious concerns regarding law enforcement using and relying on this technology. Possible recommendations to help law enforcement successfully implement this technology will be discussed in a later chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDY 2: PREDICTIVE RISK ASSESSMENTS

The second case study examined in this thesis concerns the usage of predictive risk assessment AI systems. Predictive risk assessments are the output of a trained AI system that evaluates an event's likelihood. This is a growing field in the medical community as there are increasing numbers of AI systems designed to evaluate the likelihood of a patient's diagnosis for certain diseases.

Predictive risk assessments have also been used by the criminal justice systems before to determine the likelihood of an offender to recidivate or how likely an individual is to commit a crime. This type of AI system is most often imagined when the law enforcement domain intersects with the AI and big data domain. For a good reason, too. There have been many science fiction movies and novels regarding this topic, with the most prominent being the 2002 film *Minority Report* with Tom Cruise. In this film, a "pre-crime" unit prevents major crimes before they are committed with the use of "precogs" that can visualize the crime before it happens. In the film, the "pre-crime" used the precogs' abilities to reduce the murder rate to 0 percent, an enviable rate for any law enforcement agency or politician.[112]

In the case of predictive risk assessments, AI takes the place of the "precogs" from *Minority Report* and leverages historical trends and training from skilled users to evaluate subjects. This chapter will evaluate the case of at least one predictive risk assessment that has been used by court systems in the United States to evaluate the likelihood of an offender to re-offend after placed on parole.

A. OVERVIEW

Predictive risk AI systems currently find use in many fields, most notably the medical industry. These systems have enabled doctors to more efficiently diagnose diseases and reduce errors. In fact, this has been a promising tool for the medical community, with multiple studies indicating greater accuracy than medical professionals.

[112] *Minority Report,* directed by Steven Spielberg (United States: 20th Century Fox, 2002), DVD.

In 2017, multiple AI systems were more accurate than a panel of pathologist experts when attempting to diagnose breast cancer.[113]

The criminal justice is no stranger to predictive risk assessments either. Plagued by increased workload and decreased staffing, courts have sought after tools to help process all the data used in the court environment. Predictive risk assessments have been used by the courts to help determine the likelihood an offender will re-offend if released. One such AI system is the Public Safety Assessment (PSA) developed by the Laura and John Arnold Foundation and used by the Kentucky court system.[114] Based on specific factors, the PSA has three predictive models used to score pre-trial subjects: Failure to Appear, New Criminal Activity, and New Violent Criminal Activity.[115]

Another predictive risk assessment currently used by the criminal justice system is the COMPAS system developed by NorthPointe Inc. This model has garnered more attention than most due to an investigative journalism article published by ProPublica. Similar to the PSA, COMPAS is an AI system used by the courts to determine the likelihood of an offender to re-offend if released on bail. This chapter will dive deeper into COMPAS more specifically, but the work done by ProPublica highlights some of the major concerns and potential risks of using predictive risk assessments and indicative of present discourse on the topic in general.

B. COMPAS

One of the most prominent implementations of machine learning in the criminal justice environment has been the utilization of Northpointe's product named COMPAS. This product has been used by Broward County , FL, the State of New York, and the State

[113] Babak Ehteshami Bejnordi et al., "Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer," *JAMA* 318, no. 22 (December 12, 2017): 2199–2210, https://doi.org/10.1001/jama.2017.14585.

[114] Matthew DeMichele et al., The Public Safety Assessment: A Re-Validation and Assessment of Predictive Utility and Differential Prediction by Race and Gender in Kentucky (SSRN Journal, 2018), 2, https://www.ssrn.com/abstract=3168452.

[115] DeMichele et al., 18.

of California.[116] Its main function is to assess the likelihood of an offender to re-offend. COMPAS generates two primary risk scores, General Recidivism and Violent Recidivism, that are both based on "criminogenic factors and historical factors."[117] The COMPAS product is widely known due to the legal challenge it faced out of Wisconsin when Eric Loomis filed for an appeal on the basis that usage of this algorithm violated his right to due process.

In 2013, Eric Loomis was charged with five criminal offenses related to a drive-by shooting in La Crosse, Wisconsin. Loomis eventually pleaded guilty to two of the five offenses, and during his sentencing, the Wisconsin Department of Corrections provided a presentencing investigation report that included a COMPAS risk assessment.[118] As mentioned earlier in this paper, the COMPAS is considered to be a black-box algorithm due to the nature of the technology and the fact that the source code is proprietary property. During Loomis' hearing, the COMPAS assessment was utilized to sentence him to six years of imprisonment and five years of probation.[119]

Loomis later filed an appeal with the Wisconsin Supreme Court on the grounds that the use of COMPAS at his sentencing "violates a defendant's right to due process, either because the proprietary nature of COMPAS prevents defendants from challenging the COMPAS assessment's scientific validity, or because COMPAS assessments take gender into account."[120] The Wisconsin Supreme Court affirmed the lower court's decision, arguing two main points. Firstly, the COMPAS information is largely static and based on publicly available information about his criminal history. The data's public availability provided Loomis the opportunity to review and challenge the information used by the

---

116 Keith Kirkpatrick, "It's Not the Algorithm, It's the Data," *Communications of the ACM 60,* no. 2 (January 23, 2017): 21, https://doi.org/10.1145/3022181.

117 Northpointe, Practitioner's Guide to the COMPAS Core (Northpointe Inc., 2015), 1, http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf.

118 "State v. Loomis," *Harvard Law Review,* March 10, 2017, https://harvardlawreview.org/2017/03/state-v-loomis/.

119 *Harvard Law Review.*

120 *State of Wisconsin v. Loomis,* No. 2015AP157- CR (Wis. Ct. App. July 13, 2016).

algorithm.[121] Secondly, the Court concludes that gender usage in the COMPAS algorithm promotes accuracy when predicting recidivism rates, which benefits all justice system components, including defendants.[122]

However, even with this conclusion, the Justices had clarifying comments in their response regarding the usage and reliance on risk-based algorithms, such as COMPAS. Justice C.J. Roggensack points out the difference between consideration and reliance on these assessments, which have very different impacts on the case. Roggensack states, "consideration of COMPAS is permissible; reliance on COMPAS for the sentence imposed is not permissible."[123] Ultimately, if risk-based algorithms were the only factor considered, then the defendant's due process would have been violated. In an effort to highlight the risks of utilizing algorithms similar to COMPAS, Justice Shirley Abrahamson states, "At oral argument, the Court repeatedly questioned both the State's and defendant's counsel about how COMPAS works. Few answers were available."[124] Abrahamson argues that as more and potentially better research tools become available, it is important that their "relevance, strengths, and weaknesses" are considered by the Court. In addition to being upheld by the Wisconsin Supreme Court, the Supreme Court of the United States denied hearing the case, citing "…that determination accords with the sentencing court's heavy emphasis on petitioner's criminal history and the seriousness of the offense… Petitioner would thus be unlikely to benefit from a decision in his favor on the question presented."[125]

Even though the courts do not know exactly how the COMPAS algorithm works, it was considered not to violate Loomis' due process because there was knowledge of the data that was used in the algorithm. Some factors, such as gender, are considered to make the algorithm more accurate. Although the Courts highlighted the risk of over-dependence on COMPAS and similar algorithms, *State of Wisconsin v. Loomis* provides precedence for

---

[121] *State of Wisconsin v. Loomis* at 23.

[122] *State of Wisconsin v. Loomis* at 35–36.

[123] *State of Wisconsin v. Loomis* at 53.

[124] *State of Wisconsin v. Loomis* at 54.

[125] Brief for the United States as Amicus Curiae, *Eric L. Loomis, Petitioner v. Wisconsin,* No. 16–6387 (May 2017).

using black-box algorithms in Court. Even though there was no satisfactory explanation of how COMPAS utilizes data to generate its scores, its usage was still permitted.

This court case has established precedence on using machine learning algorithms and black-box algorithms with no context on how they work. The Court did call for concern when utilizing the COMPAS algorithm and others similar to it and prescribed written warnings when the algorithm is used. Still, it is doubtful how impactful these warnings will actually be.[126] Until additional cases are presented in Court, there is the potential for black-box machine algorithms to assist with the court proceedings and interpretations. If the black box algorithm is wholly accurate and can reliably predict recidivism, then this should not be a problem. But what if the black-box algorithm is not entirely accurate?

The COMPAS algorithm was at the center of the *Loomis v. Wisconsin* trial due to its black-box nature. As discussed above, even though there was no explanation of how the algorithm works, its usage was still allowed. Presumably, since the algorithm's use was permitted, it should be reasonably accurate. According to documentation from 2009 created by Northpoint, the creator of the COMPAS algorithm, there are varying levels of accuracy that are considered satisfactory, which are represented by Area Under Curve (AUC) scores and represent the likelihood of the model's accuracy. Scores above .70 are considered to have "satisfactory predictive accuracy," while measures between .70 and .60 are considered to have "low to moderate predictive accuracy."[127] In Northpointe's study, researchers found their models generally fell within an AUC range of .70 to .80, performed similarly between men and women, and "performed equally well" for white men as African American men.[128] In 2014, ProPublica, a non-profit investigative newsroom, sought to challenge the accuracy of this algorithm.

ProPublica's investigation into the COMPAS algorithm covered over 7,000 individuals arrested during 2013 and 2014 in Broward County, Florida, and followed up in

---

[126] *State of Wisconsin v. Loomis* at 29; *Harvard Law Review,* "State v. Loomis."

[127] Tim Brennan, William Dieterich, and Beate Ehret, "Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System," *Criminal Justice and Behavior* 36, no. 1 (January 2009): 29–30, https://doi.org/10.1177/0093854808326545.

[128] Brennan, Dieterich, and Ehret, 32–33.

2015 and 2016 to see if any arrested individuals were arrested again after their release.[129] ProPublica's investigation found that only 61 percent of the individuals predicted to re-offend did so within the two years of the investigation, and 20 percent of the individuals predicted to recidivate with violent offenses actually did so.[130] Their investigation also found that black individuals were twice as likely to be falsely identified as likely re-offenders. In general, white individuals were more often mislabeled as low-risk than black individuals, as demonstrated in Figure 1.[131] ProPublica's study found that the COMPAS algorithm had an AUC of .636, which means that 63.6 percent of the time, the COMPAS algorithm can predict the likelihood of recidivism accurately and is of "low to moderate predictive accuracy" per Northpointe's scale.

ProPublica's study pointed out potential flaws in the COMPAS algorithm that could point to unintended bias in the outputs. Their research also showed that when compared to follow-up data from Broward County, the algorithm was not as accurate as claimed by Northpointe. Since this is a black-box algorithm, it would be challenging, if not impossible, for defendants to refute the outputs provided by this proprietary machine-learning algorithm.

129 Julia Angwin et al., "Machine Bias," text/html, ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

130 Angwin et al.

131 Angwin et al.

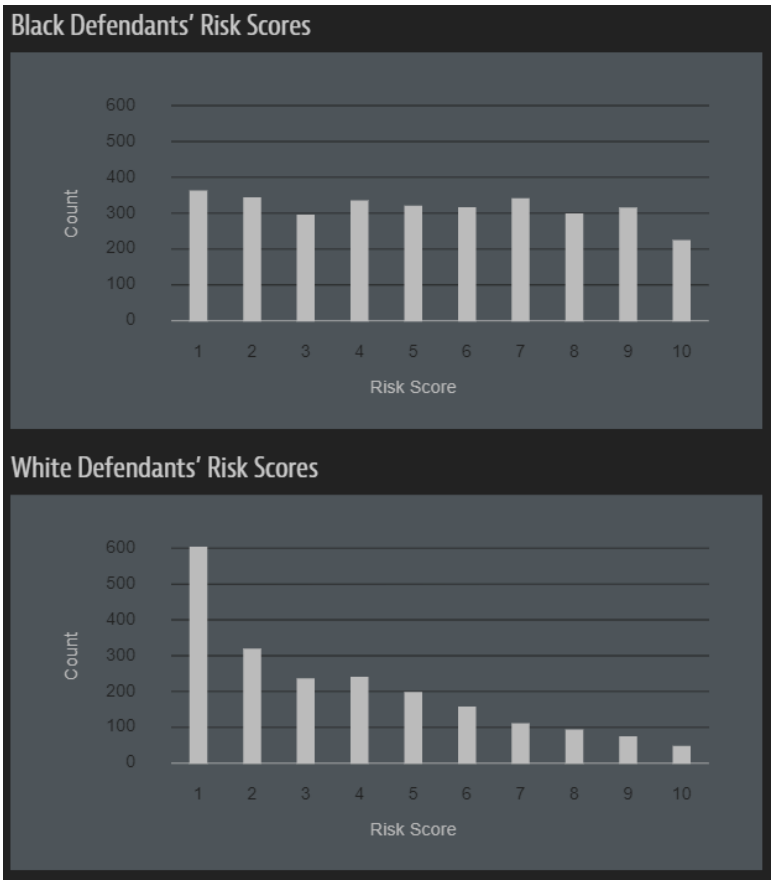

Figure 1. Distribution of scores for white and black individuals evaluated by the COMPAS algorithm.[132]

C. DUE PROCESS

As noted by John Villasenor and Virginia Foggo, the issue of due process as it relates to AI systems has not been directly addressed by the courts. Still, case law can help shed some light on the impact of AI systems on due process.[133] To help facilitate this discussion, Villasenor and Foggo focus on four main themes: "Accuracy and admissibility of information used at sentencing, access by a defendant to information used at sentencing, the scientific validity of AI-based presentencing risk assessment methods, and the extent

[132] Angwin et al.

[133] John Villasenor and Virginia Foggo, "Artificial Intelligence, Due Process, and Criminal Sentencing," *Michigan State Law Review*, no. 295 (2020): 314.

to which such approaches might inadvertently consider impermissible factors such as race."[134]

The 1948 Supreme Court ruling in *Townsend v. Burke* provided the opinion that "this prisoner was sentenced on the basis of assumptions concerning his criminal record which were materially untrue. Such a result, whether caused by carelessness or design, is inconsistent with due process of law, and such a conviction cannot stand."[135] This ruling from the Supreme Court presents the concept that defendants have the due process right to be tried on material that is not "materially untrue."[136] As pointed out by Villasenor and Foggo, multiple court cases throughout the years uphold this finding. However, there are plenty of examples where there are insufficient protections regarding "unreliable or improperly obtained information at sentencing."[137] When applied to AI systems, how does one determine if the information is true or not? There are many factors to consider, from data the system was trained with to the AI system's accuracy. Every component of the AI system has the potential to alter the outcome. To complicate the matter, the burden of proof is generally left with the defendant.

The burden of proof can be even more difficult for the defendant when dealing with proprietary or "black-box" systems where there is no way for an outside observer to determine what happened to the inputs to create the outputs. Villasenor and Foggo argue that there is some guidance from existing court cases, even though they are not concerning AI systems. In *Gardner v. Florida,* the Court convicted Garner of first-degree murder and sentenced him to death.[138] However, the death penalty was based on partial information from the presentence trial and not disclosed to Gardner's council. As a result, the U.S. Supreme Court ruled that Gardner's right to due process was violated by the information's secrecy resulting in the death sentence. Although this seems like a strong stance from the

---

134 Villasenor and Foggo, 314.

135 "Townsend v. Burke.," LII / Legal Information Institute, accessed November 8, 2020, https://www.law.cornell.edu/supremecourt/text/334/736.

136 "Townsend v. Burke."

137 Villasenor and Foggo, "Artificial Intelligence, Due Process, and Criminal Sentencing," 320–21.

138 Villasenor and Foggo, 323.

courts, there isn't clear guidance from the courts on disclosing all facts in a case. In 2006, *United States v. Baldrich* determined that a defendant does not have due process to opinions and recommendations.[139] From *United States v. Eyraud, "*[t]o date, no circuit… has concluded that the Due Process Clause requires full disclosure of all the information relied on by a court at sentencing."[140] This contradicting nature has the potential to be troublesome concerning AI systems.

Villasenor and Foggo posit that the potential secrecy of AI systems is particularly concerning. In many cases, AI systems are proprietary to maintain a competitive edge in the commercial market. Companies supplying AI systems will not be willing to detail their system's inner workings unless ordered by a court. According to the above-mentioned cases, and argued by Villasenor and Foggo, it would be reasonable to expect that all the data and process used by AI systems would be subject to due process laws.[141]

In terms of scientific validity, Villasenor and Foggo argue that the same requirements for expert scientific testimony as outlined in the 1993 case of *Daubert v. Merrell Dow Pharmaceutical, Inc.* should have some applicability to AI systems as well.[142] In this case, the Court identified four factors to determine whether someone could be considered an expert witness. These include "determining whether a theory or technique is scientific knowledge that will assist the trier of fact by examining whether it can be and has been tested, whether it has been subjected to peer review and publication, the known or potential rate of error… and the existence and maintenance of standards controlling the techniques operation, and whether the technique has experience general acceptance within the scientific community."[143] Ultimately, this technology is still too new to have substantial reporting, peer reviews, and testing to have general acceptance. As a result, AI

[139] Villasenor and Foggo, 326.

[140] Villasenor and Foggo, 326.

[141] Villasenor and Foggo, 327–28.

[142] Villasenor and Foggo, 328.

[143] Villasenor and Foggo, 328.

systems do not meet the core requirements of a human to provide expert scientific testimony.[144]

Lastly, courts prohibit introducing certain factors such as race, ethnicity, or religion to play a factor during sentencing, even if the defendant's council brings the information forward. Villasenor and Foggo claim that this is a concerning element for AI systems, even if the system is designed to ignore specific data elements that should be ignored.[145] Due to the nature of the historical data used to train the AI system, there is a real possibility for protected factors could still be implied and used in the courts, even if it is unintentional. Villasenor and Foggo use the Iowa Risk Revised (IRR) tool as an example that highlights this potential. As part of the IRR tool's factors, employment status, current convictions, and previous convictions are included in this assessment.[146] However, these factors have been historically impacted by racial discrimination and incidentally include bias based on a protected characteristic.

D. CRITERIA ANALYSIS

Each AI system is evaluated based on five criteria: effectiveness, fairness, transparency, and accountability. Each criterion will be provided a score of either low, medium, or high and will be determined by constraints, problems, or successes caused by each policy that is assessed. Based on each criterion's outcome, an average score will be generated for comparison to the other AI systems.

1. Effectiveness—Low

When used in the real world, the COMPAS algorithm accomplished what it set out to do, assist with case evaluation backlog, with moderate success. As is demonstrated by ProPublica, the accuracy of the system demonstrates the need to not solely rely on the COMPAS algorithm for evaluations. COMPAS was only found to be 61 percent accurate when its recidivism predictions were followed up two years after the initial investigation.

144 Villasenor and Foggo, 328.

145 Villasenor and Foggo, 332–33.

146 Villasenor and Foggo, 332–33.

This accuracy significantly drops to 20 percent when only considering violent crimes. According to the study, the COMPAS algorithm also imparts some bias in its evaluations, causing concern in the overall impact on the court system.

Although these predictive risk assessments provide some insight into the problems they are trying to address, they are not completely accurate and are prone to bias in their current state. As discussed earlier, COMPAS sees moderate successes in their respective domains, but they come with certain risks and caveats that may cause a law enforcement agency pause. As a result, effectiveness has been evaluated as "low."

2. Privacy—Low

There are serious considerations and potential impacts on privacy when using predictive risk assessment AI systems. One of the largest issues is the lack of recent federal regulation on data, to the point where individual states feel the need to legislate their own data regulations, as was previously discussed. AI systems have the potential to reveal protected sets of data by interpreting patterns and connections from other sets of data. Due to the lack of regulations in place at the agency or legislative level, privacy has been evaluated as "low."

3. Fairness—Low

In the COMPAS algorithm reviewed in this chapter, individuals are subject to the same processes conducted. However, these processes are subject to previous data sets and assumptions that may introduce bias and unfair practices. Despite best efforts, protected classes can still manage to find their way into AI systems and disproportionately affect a specific subset of individuals. This can happen through training sets of data that contain historical racial biases, processes that disproportionately impact a particular group of people, or even assumptions made by system administrators or developers that initially developed the AI system.[147] When investigating the COMPAS algorithm's accuracy, ProPublica found that individuals classified as white were regularly evaluated at a lower risk level than their counterparts that were classified as black. ProPublica found that black

[147] Sandvig et al., "Can an Algorithm Be Unethical?"

individuals were 45 percent more likely to receive a higher risk score than white individuals. Due to the lack of consistency across multiple factors, fairness has been evaluated as "low."

4. Transparency—Low

As discussed previously, the lack of regulation does not encourage transparency within AI systems. When businesses implement proprietary systems without some form of regulation, there is no incentive to create transparent systems. These "black-box" systems do not allow outside parties to understand the system's inner workings or provide comprehensible explanations to the processes used to transform data.

Additionally, since private entities own the AI systems discussed in this chapter, the owners have no obligation to allow the general public to audit their processes or data sources for independent verification purposes. This has severe impacts if these systems have a large role in an investigation or trial and significantly complicates, if not makes it impossible, for the results to be challenged in a meaningful way. Due to these reasons, transparency has been evaluated as "low."

5. Accountability—Low

Without regulatory oversight of AI systems, there is no form of accountability when incorporated into a law enforcement agency's usage. There is no way for an agency to evaluate or determine the potential impact an AI system like COMPAS would have on an individual without some form of impact assessment conducted by the agency. Even though AI systems may strip elements of PII, there is still the potential to infer specific people from the data correctly. Due to the lack of regulatory oversight when these systems are implemented, accountability is evaluated as "low."

E. SUMMARY

This chapter evaluated the usage of predictive risk assessment AI systems by the criminal justice system. Although the examples discussed throughout this chapter focused on AI systems used in the courts, many of the concerns are the same if law enforcement agencies implemented similar systems. There are significant concerns when using

predictive risk assessment tools, especially related to an individual's right to due process and accuracy, as discussed throughout this chapter. As has been seen with other AI systems discussed, certain groups of people are disproportionately impacted by the assessments made by predictive risk assessment AI systems. Additionally, there are due process concerns as these systems can infer traits about a person. Still, it is extremely difficult to apply the same standards for verification that are applied to "experts" in the court of law.

When evaluated across effectiveness, privacy, fairness, transparency, and accountability, predictive risk assessments have been evaluated as "low" in every category. Similar to facial recognition, this is a new and emerging technology with very few regulatory guidelines to help inform and scope its usage by law enforcement. Until such regulations are implemented, law enforcement should be wary of using and relying on this technology. In a later chapter, potential recommendations for law enforcement will be discussed in an effort to ensure an effective approach to this technology.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY 3: PREDICTIVE POLICING

The third and last case study addressed in this analysis is the usage of predictive policing AI systems in the law enforcement domain. Although this is fairly similar to the previous chapter on predictive risk assessments, the intent of this case study is to focus on the ability of AI systems to derive trends from large sets of data rather than to predict an outcome. According to the Atlas of Surveillance, there are over 150 agencies across the nation that utilize predictive policing in some form or fashion.[148] Law enforcement agencies use predictive policing systems to determine staffing and resource allocation, areas where crime is likely to occur or to determine where crimes are likely to happen.[149]

Although these tools can be useful and potentially address resource concerns about the growing amount of data, there are significant privacy concerns relating to the type of data collected and the manner in which it is processed. Although this type of AI system has yet to garner the same amount of attention as facial recognition, concerns are mounting. In September 2020, Santa Cruz, CA became the first city in the United States to ban law enforcement's usage of predictive policing and defined it as "software that is used to predict information or trends about crime or criminality in the past or future, including but not limited to the characteristics or profile of any person(s) likely to commit a crime, the identity of any person(s) likely to commit crime, the locations or frequency of crime, or the person(s) impacted by predicted crime."[150]

This chapter will examine the usage of PredPol, a predictive policing AI system that identifies "hotspots" based on trends derived from an agency's records management system. This chapter will also examine some of the larger implications of privacy when a law enforcement agency uses a predictive policing AI system. Lastly, predictive policing

148 Electronic Frontier Foundation, "Search the Data - Atlas of Surveillance," accessed January 10, 2021, https://atlasofsurveillance.org/search?sort=state_desc&technologies%5B86%5D=on.

149 Lau, "Predicitve Policing Explained."

150 "Surveillance Technology," Santa Cruz Municipal Code § 9.85 (2020), 2, https://www.codepublishing.com/CA/SantaCruz/#!/SantaCruz09/SantaCruz0985.html#9.85.

AI systems will be evaluated using the following criteria: effectiveness, privacy, fairness, transparency, and accountability.

A. OVERVIEW

The Los Angeles Police Department (LAPD) is often credited with being the first to develop and use predictive policing used to "anticipate gang violence and to support real-time crime monitoring."[151] Predictive policing finds its beginnings in the theory that crime is predictable, and criminals tend to operate within their comfort zone. A study into predictive policing by RAND describes this as a "blended theory," where criminals and victims follow common life patterns, time and location impact criminal activity, and criminals make "rational" decisions about committing crimes.[152] Using data that speaks to these areas, predictive policing is used to predict or forecast where crimes are most likely to occur. Currently, there are many vendors that offer predicting policing services. Some of the more popular vendors include PredPol, Palantir, and Hunchlab, which offer services such as patrol recommendations, mission planning, and performance analytics[153]

There are growing concerns about predictive policing AI systems, especially regarding privacy expectations for an individual. With the amount of data used in these systems, it is within the realm of possibility to identify individuals with basic demographic information. The level of insight to an individual's preferences, beliefs, and daily activities also has fourth amendment implications, as protected information becomes unveiled due to correlations discovered by predictive policing AI systems.

B. PREDPOL

The RAND Safety and Justice Program defines predictive policing as "…the application of analytical techniques- particularly quantitative techniques- to identify likely

---

[151] Walt L. Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations,* RR-233-NIJ (Santa Monica, CA: RAND, 2013), 4, https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

[152] Perry et al., 3.

[153] "Law Enforcement," PredPol, accessed November 24, 2020, https://www.predpol.com/law-enforcement/.

targets for police intervention and prevent crime or solve past crimes by making statistical predictions."[154] Multiple agencies have used this method to reduce crime within their particular jurisdictions, particularly by proactively reducing violent crime.[155] As technology has advanced, these workflows have been augmented by machine learning and artificial intelligence and packaged by vendors to sell to other agencies. One such vendor that specializes in predictive policing utilizing these techniques is PredPol.

As described on their website, PredPol is a tool that "identifies where and when crime is most likely to occur, enabling you to effectively allocate your resources and prevent crime."[156] Using information reported to the participating agency, PredPol leverages machine learning and artificial intelligence to anticipate where crime is most likely to happen. PredPol uses a proprietary machine-learning algorithm that finds its origins in seismology to predict where crime is most likely to happen. This algorithm is trained from the participating agency's historical information and maps the incidents in a geographic information system (GIS) display to interact with the data. The driving concept behind PredPol is to identify activity "hotspots" to aid law enforcement in personnel allocation in a more strategic and thoughtful manner. If the specified "hotspots" are where the most crime has historically occurred, then that location is where more officers should be patrolling.

154 Perry et al., *Predictive Policing,* xiii.

155 Perry et al., 80.

156 "PredPol Mission," *PredPol* (blog), accessed November 24, 2020, https://www.predpol.com/about/.

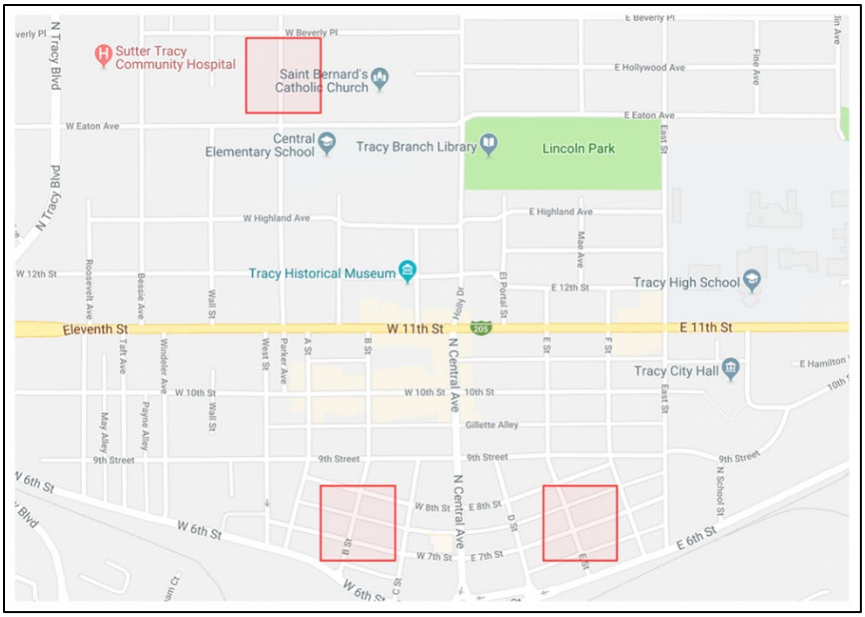

Figure 2. Example of PredPol "hotspot."[157]

On the surface, PredPol makes a sound case for predictive policing and can help automate personnel assignments to areas that need law enforcement officers the most, as identified by the "hotspots" from historical trends. However, according to researchers investigating the impact of predictive policing software, the approach used by PredPol may be flawed. It can potentially lead to enforcing or exaggerating bias found in the original set of data used to identify the "hotspots." While conducting their analysis, Kristian Lum and William Isaac find "that rather than correcting for the apparent biases in the police data, the model reinforces these biases. The locations that are flagged for targeted policing are those that were, buy our estimates, already over-represented in the historical police data."[158] When Lum and Isaac applied the PredPol algorithm to a year's worth of Oakland crime reporting data, they concluded that using a predictive policing algorithm for personnel allocation would "result in the disproportionate policing of low-income communities and communities of colour."[159]

---

157 PredPol, "Law Enforcement."

158 Kristian Lum and William Isaac, "To Predict and Serve?," *Significance*, October 2016, 18.

159 Lum and Isaac, 18.

The Los Angeles Police Department (LAPD) has been a PredPol customer since 2011.[160] In 2019, the LAPD Office of the Inspector General (OIG) conducted a review of "data-driven policing strategies" at the urging of multiple privacy and civil rights advocates, which included LAPD's usage of PredPol. While reviewing PredPol, the OIG found that officers spent "relatively minimal" time in the "hotspots" identified by PredPol. While the targeted crime of vehicle-related crimes targeted by PredPol had a decrease of approximately 3 percent during the review period, the OIG could not confidently conclude the crime reduction was a direct result of the application.[161] Too many reporting and data collection discrepancies prohibited conclusive results.[162] Although the OIG did not recommend suspending or terminating the program, they recommend developing a system to report the usage and effectiveness of data-driven programs to their governing commission and the general public to promote transparency and oversight.[163]

C. PRIVACY

The concept of privacy has evolved over the years, both conceptually and in the courts. In 1890, Samuel Warren and Louis Brandeis spoke to the evolution of a person's rights and how the law has evolved to maintain pace with society's expectations.[164] In their work, "The Right to Privacy," Warren and Brandies recognize the need to codify the right of privacy or "the right to be let alone."[165] Their work also outlines the beginnings of a conception of informational privacy, or the right to control personal information kept in private or shared with others in confidence.[166]

---

160 Mark P Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies" (official memorandum, Los Angeles, CA: Los Angeles Police Department, 2019), 26, http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

161 Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies."

162 Smith, 28–30.

163 Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies."

164 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* IV, no. 5 (December 15, 1890): 193.

165 Warren and Brandeis, "The Right to Privacy."

166 Karl Manheim and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy," *Yale Journal of Law and Technology* 21, no. 106 (December 13, 2019): 118.

In a day and age when data is thought to be more valuable than oil, informational privacy becomes increasingly important to the person.[167] Not because of the potential value they may be missing from the sale of their data, but because of the information, trends, and insights that can be extracted from mining this set of data. The argument has been made that without regulation, AI systems can undermine privacy values due to the sheer amount of data available on a person and connections that can be inferred between sets of data.[168] In fact, just simple demographic data, it has been shown that approximately 87 percent of the population in the United States can be uniquely identified by their five-digit zip code, gender, and date of birth.[169] About half of the United States population can be identified by place (city/town), gender, and date of birth.[170]

Another point of concern regarding privacy issues is the United States has not passed any wholesale data regulations since the 1974 Privacy Act, which regulates what type of information government entities can store on U.S. citizens.[171] There have been other acts approved by Congress, such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act. Still, they are limited in scope and only apply to a small subset of the American population. Interestingly enough, individual states, such as California, New York, Maryland, Massachusetts, Hawaii, and North Dakota, have taken data rights into their own hands by approving their own data privacy laws.[172]

Without some form of privacy regulations on AI systems, there is the potential for industries, such as the health or law enforcement sectors, to over-reach to the detriment of

---

167 "The World's Most Valuable Resource Is No Longer Oil, but Data," *Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data; Kiran Bhageshpur, "Data Is the New Oil -- and That's a Good Thing," *Forbes,* November 15, 2019, https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/.

168 Manheim and Kaplan, "Artificial Intelligence."

169 Latanya Sweeney, *Simple Demographics Often Identify People Uniquely, Data Privacy* Working Paper 3 (Pittsburgh, PA: Carnegie Mellon University, 2000), 2.

170 Sweeney, 2.

171 Andy Green, "Complete Guide to Privacy Laws in the US," *Inside Out Security (*blog), March 29, 2020, https://www.varonis.com/blog/us-privacy-laws/.

172 Green.

the general populace. Manheim and Kaplan explain, "the aggregation and coordination of disparate databases can reveal everything from buying habits to health status to religious, social and political preferences."[173] This closely resembles Justice Sotomayor's opinion in *United States v. Jones* that revolves around "mosaic theory." In this case, the Court sought to determine if GPS surveillance of a vehicle over twenty-eight days constituted enough surveillance to trigger Fourth Amendment protections. Ultimately, this case would allow for a new approach for Fourth Amendment protections. Prior to this case, Fourth Amendment considerations were made step by step. However, by accepting the concept of the "mosaic theory," the courts allow a more holistic approach to determine Fourth Amendment protections. Justice Sotomayor states, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[174] Although this case was explicitly geared toward GPS surveillance, the concept of "mosaic theory" should apply to AI systems. Ostensibly, this technology, through the connections and associations it is capable of, resembles the "mosaic theory" described by Justice Sotomayor.

D. CRITERIA ANALYSIS

Each AI system is evaluated based on five criteria: effectiveness, fairness, transparency, and accountability. Each criterion will be provided a score of either low, medium, or high and will be determined by constraints, problems, or successes caused by each policy that is assessed. Based on each criterion's outcome, an average score will be generated for comparison to the other AI systems.

1. Effectiveness—Low

So far, it has been difficult to gauge the effectiveness of predictive policing AI systems. As discussed previously, LAPD determined their experience with PredPol was not significant, and it was difficult to discern if the success could genuinely be attributed

[173] Manheim and Kaplan, "Artificial Intelligence," 121.

[174] Orin S Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review* 111, no. 3 (December 2012): 238.

to the AI system itself. In fact, most of the dosage time detected by PredPol was from areas close to areas frequented by officers, such as LAPD facilities, or were driven through in response to other calls.[175] A decrease of 3 percent isn't significant, especially when accompanied by a 41 percent increase in dosage time, or recommending staffing levels.[176]

Although predictive policing AI systems provide some insight into the problems they are trying to address, they are not completely accurate and are prone to bias in their current state. PredPol saw moderate success in their domain, but the usage of the system comes with certain risks and caveats that may cause a law enforcement agency pause. As a result, effectiveness has been evaluated as "low."

2. Privacy—Low

There are serious considerations and potential impacts on privacy when using AI systems. One of the largest issues is the lack of recent federal regulation on data, to the point where individual states feel the need to legislate their own data regulations. AI systems have the potential to reveal protected sets of data by interpreting patterns and connections from other sets of data. Even when PII is stripped from these datasets, there is still a good likelihood that an AI system can accurately identify a person with a handful of data elements.

The ability to identify a person without using PII combined with the "mosaic theory" presents significant privacy concerns regarding the usage of AI systems. This capability offers a situation where AI systems, and their subsequent users (i.e., law enforcement officers), to peer into the lives of individuals at will. Of course, this ability assumes there is enough data for these connections to be made. Still, in the current environment where "data is the new oil," there is certainly enough information readily available for some links to be made. With the evolving understanding of privacy over the past 200 years, the ability to intrude upon an individual's life using information they thought was private could potentially violate Fourth Amendment protections provided by

---

[175] Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies," 28–29.

[176] Smith, 27.

the Constitution. With these considerations in mind, privacy was evaluated as "low" because there are too many privacy concerns and potential constitutional violations caused by this technology's lack of regulation.

3. Fairness—Low

In the PredPol predictive policing AI system reviewed in this chapter, individuals are subject to the same processes conducted. However, these processes are subject to previous data sets and assumptions that may introduce bias and unfair practices. When Lum and Isaac reviewed the PredPol system, it was found that "black people would be targeted by predictive policing at roughly twice the rate of whites. Individuals classified as a race other than white or black would receive targeted policing at a rate 1.5 times that of whites."[177] Although not intentional, historical biases found in the data caused an unfair application of law enforcement presence.

The Electronic Frontier Foundation (EFF) provides a simple take on this issue stating, "Predictive policing is a self-fulfilling prophecy."[178] By this, the EFF is highlighting concerns regarding bias found within datasets used to train the AI system that will ultimately provide policing recommendations. If police units perform a lot of enforcement in a particular area, that area is very likely to remain a recommendation for police enforcement due to historical trends. This has the potential to reinforce bias within the predictive policing AI system and unduly target members of protected classes. The AI system has become unfair to those individuals based on their race. Due to the lack of consistency across multiple factors, fairness has been evaluated as "low."

4. Transparency—Low

As discussed previously, the lack of regulation does not encourage transparency within AI systems. When businesses implement proprietary systems without some form of regulation, there is no incentive to create transparent systems. These "black-box" systems

[177] Lum and Isaac, "To Predict and Serve?," 18.

[178] Guariglia, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing."

do not allow outside parties to understand the system's inner workings or provide comprehensible explanations to the processes used to transform data.

Additionally, since private entities own the AI systems discussed in this chapter, the owners have no obligation to allow the general public to audit their processes or data sources for independent verification purposes. This has severe impacts if these systems have a large role in an investigation or trial and significantly complicates, if not makes it impossible, for the results to be challenged in a meaningful way. Due to these reasons, transparency has been evaluated as "low."

5. Accountability—Low

Without regulatory oversight of AI systems, there is no form of accountability when incorporated into a law enforcement agency's usage. There is no way for an agency to evaluate or determine the potential impact an AI system like PredPol would have on an individual without some form of impact assessment conducted by the agency. Even though AI systems may strip elements of PII, there is still the potential to infer specific people from the data correctly. Due to the lack of regulatory oversight when these systems are implemented, accountability is evaluated as "low."

E. SUMMARY

This chapter evaluated the usage of predictive policing AI systems by law enforcement and many of the challenges associated with these systems, especially regarding privacy and applicability. Even when PII elements are removed from large datasets, there still exists the potential for these systems to accurately associate activities to specific individuals. Additionally, these systems require additional Fourth Amendment considerations, as the "mosaic theory" from *United States v. Jones* should be applicable when these systems are in use, which would impact how and when warrants are required. As documented by LAPD, it was also difficult to determine the impact similar systems have on the agency's ability to reduce motor vehicle crimes.

When evaluated across effectiveness, privacy, fairness, transparency, and accountability, predictive policing AI systems were rated "low." This outcome is extremely

similar to the other two AI systems that were evaluated. Predictive policing AI systems suffer from many of the same problems, such as a lack of regulation at any level to inform how and when these systems should be used. In a later chapter, potential recommendations for law enforcement will be discussed in an effort to ensure an effective approach to this technology.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

Like many other industries, law enforcement strives to enhance their performance and optimize their workflows to better serve their constituents. As anticipated by the Law Enforcement Forecasting Group, the influx of data requires law enforcement agencies to adapt to these new challenges.[179] Advances in technology allow AI systems to become both more powerful and easier to procure. When law enforcement acquires these systems, however, there are serious considerations to be aware of because there can be serious ramifications if not addressed.

Three different AI systems were evaluated by five categories that represent considerations that need to be taken before law enforcement implement an AI system in their agency. These categories cover topics that range from the overall effectiveness of the system, how AI systems can affect those subjected to it, and even potential legal issues that may arise from using an AI system. These five considerations were evaluated for three different types of AI systems: facial recognition, predictive risk assessments, and predictive policing.

Since this is an emerging technology, aspects of AI systems are changing on a regular basis, as well as how local, state, and federal governments are reacting to the technology's potential and pitfalls. Limitations regarding available information for this study will be discussed in this chapter.

Lastly, this is not a problem that solely affects the United States of America. The European Union (EU) is encountering many of the same problems with AI systems. In conjunction with data privacy regulations established, such as the General Data Protection Regulation (GDPR), the EU has formed expert groups to evaluate and generate a potential framework to establish responsible practices for AI systems.[180] The lessons learned from

---

[179] Law Enforcement Forecasting Group*, Increasing Analytic Capacity of State and Local Law Enforcement Agencies,* 5.

[180] High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI: High-Level Expert Group on Artificial Intelligence," European Commission, 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

this expert group are directly applicable to the United States and should be considered as a framework to be established by professionals here as well.

A. FINDINGS

When evaluated by their effectiveness, privacy, fairness, transparency, and accountability, all AI systems discussed throughout this analysis were rated low for each category. Although facial recognition, predictive risk assessment, and predictive policing AI systems accomplish different tasks for law enforcement and provide different outputs, they all experience many of the same problems.

1. Effectiveness

The effectiveness of all systems comes into question for two primary reasons: the accuracy of the AI system and the impact it has on law enforcement. As seen by facial recognition and predictive risk assessment AI systems, accuracy plays a large role in the impact of effectiveness.[181] If an AI system is inaccurate in its assessments, incorrectly identified, innocent people can become suspects in a crime they did not commit.[182] Inaccurate assessments can lead to harsher penalties imposed on people that are not as much of a risk as estimated by the AI system. The accuracy of an AI system can also have an impact on the fairness of a system, as discussed below. If an AI system unfairly impacts a specific group of people, it cannot be considered an effective or useful tool for law enforcement.

Additionally, as was demonstrated by LAPD's internal audit of PredPol, the impact of some of these systems is questionable.[183] An effective AI system should be able to provide a tangible increase in productivity while either maintaining or lowering the required human capital for the project.

---

[181] Grother, Ngan, and Hanaoka, Face Recognition Vendor Test Part 3, 34–41.

[182] Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match"; Anderson, "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit"; Hill, "Wrongfully Accused by an Algorithm."

[183] Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies."

2. Privacy

Each AI system poses a negative impact on privacy for the individual at multiple levels. Depending on how it is applied, facial recognition AI systems can essentially create "dragnet biometric databases" that impact both criminal and law-abiding citizens. If applied in a live video feed, then any expectations of privacy or anonymity in public are essentially eroded by the capabilities of a facial recognition system. Since there are no current limitations or regulations imposed on this type of technology, law enforcement agencies are not required to submit warrants or justification before usage. For this reason, many municipalities have taken it upon themselves by banning the usage of facial recognition by public agencies within their jurisdiction.

Facial recognition AI systems are not the only systems with privacy issues. Both predictive risk assessment and predictive policing AI systems have the ability to chip away at privacy expectations and alter Fourth Amendment expectations. As described by Justice Sotomayer, the "mosaic theory" could be applied to AI systems in a similar manner to GPS surveillance, as the power of data has grown to the point where intimate details of a person's habits and preferences can be accurately inferred.[184]

3. Fairness

Each type of AI system assessed experienced problems with fairness for various reasons. Facial recognition AI systems tend to experience much higher false-positive matching rates for black individuals than other races.[185] Predictive risk assessments, such as the COMPAS algorithm, tend to evaluate minority races as a higher risk of recidivism than white individuals, even when almost all traits are the same.[186] Predictive policing AI systems have the potential to reinforce historical trends in data, which has been found to

---

[184] Kerr, "The Mosaic Theory of the Fourth Amendment."

[185] Grother, Ngan, and Hanaoka*, Face Recognition Vendor Test Part 3*, 34–41.

[186] Julia Angwin et al., "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks.," ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=YxUntiDH12MOMHz5OD1yLBRth4wTzdEG.

affect minority communities more than white communities.[187] One of the biggest concerns expressed by the Electronic Frontier Foundation regarding AI systems is the risk of repeating or exacerbating previous mistakes found in historical datasets.[188] Put succinctly, "Predictive policing is a self-fulling prophecy."[189] While this sentiment was expressed specifically towards predictive policing systems, it is applicable to facial recognition and predictive risk assessment AI systems, too. Historical biases found in datasets used to train AI systems have the potential to reinforce those biases.

With these biases found in AI systems, it is obvious they impact certain groups of individuals more than others. If law enforcement were to rely on these systems in their current state with no guiding policy or legislation, there is little oversight to ensure these systems are used in a fair manner. In fact, since 2019, there have been three black men arrested due to unfair and inaccurate returns from facial recognition systems.[190]

4. Transparency

One of the major roadblocks prohibiting transparency with most AI systems is the notion of the "black-box" environment. The "black-box" environment does not allow outside parties to understand how the system works. This lack of understanding is generally accomplished through proprietary claims from vendors or an inability to explain how an AI system generated results in a manner that is easily understood.[191] Without sharing how an AI system works, there is little room for transparency. To make matters worse, if used by law enforcement, there can be difficulties explaining how conclusions were made when relying on "black-box" systems.

---

[187] Lum and Isaac, "To Predict and Serve?"

[188] Guariglia, "Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing."

[189] Guariglia.

[190] Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match"; Hill, "Wrongfully Accused by an Algorithm"; Anderson, "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit."

[191] Margaret Rouse, "What Is Black Box AI?," WhatIs, accessed November 21, 2019, https://whatis.techtarget.com/definition/black-box-AI.

When surveyed, very few law enforcement agencies were able to supply publicly available policies regarding AI systems in place at their agency.[192] Even few law enforcement agencies had legislative oversight on the technology. Without any oversight or information available to the public regarding AI systems, it is difficult to ensure this technology is used correctly by law enforcement.

5. Accountability

The lack of policies or regulations on AI systems also has an impact on accountability. In the Georgetown study, ten of the fifty-two respondents claimed to audit employees' usage of AI systems.[193] However, only one of the ten agencies supplied evidence that these audits are genuinely conducted on a regular basis.[194] In an Office of the Inspector General report from LAPD, investigators had a difficult time determining the effectiveness of PredPol due to incomplete or inaccurate system records, which calls into question how accurate some systems are at capturing user activity.[195]

Many law enforcement agencies are not required to submit any formal declarations prior to utilizing AI systems, such as warrants or court orders.[196] Since many of these systems contain information on law-abiding citizens and have the ability to make accurate inferences on those subjected to these systems, it is extremely important to ensure actions within the system are well documented and maintained. Documenting and maintaining actions within the system provides a deeper level of accountability, so long as audits are regularly conducted to ensure there is no misuse of the system.

B. LIMITATIONS

Although this study has shown there are significant concerns with law enforcement usage of AI systems, there are limitations that warrant consideration. Firstly, AI systems

192 Garvie et al., *The Perpetual Line-Up,* 51.

193 Garvie et al., 60.

194 Garvie et al., 60.

195 Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies."

196 Garvie et al., *The Perpetual Line-Up,* 36.

are a relatively new technology to the public sector, including law enforcement. Not only does it take time for iterations of technology to make it to law enforcement, but it also takes even more time to develop, draft, and institute an effective policy that can guide how this technology is used. Although many considerations, such as transparency and accountability, stem from policy and regulatory issues, these concerns may be addressed in the near future as policymakers become familiar with the technology. There may also be law enforcement agencies that have effective policies in place that address these issues as well. This assessment is not targeted towards any specific law enforcement agencies. Rather, the focus is on general issues caused by AI systems within the law enforcement domain. However, conclusions based on this information may quickly become obsolete if agencies draft and implement policy that addresses many of the identified concerns

Secondly, AI systems used by law enforcement can have a significant impact on their operations and efforts to combat crime and terrorism. It is reasonable to expect a lack of responsiveness to inquiries from researchers that may compromise investigative techniques. As such, the assessments throughout this analysis are based on information that has been shared with the public and research institutions. This can have an impact on how widespread the usage of AI systems within the law enforcement community and how impactful these systems are, for better or worse. Unfortunately, this also reinforces transparency issues regarding law enforcement's usage of this technology.

Lastly, the general tone held by the public regarding the usage of AI systems by law enforcement has been more negative throughout the duration of time while research was conducted. Perhaps this is due to the lack of transparency, audits, and effectiveness studies from the law enforcement perspective available for public consumption. There are many anecdotal stories alluding to the usefulness and positive impact had by facial recognition, predictive risk assessment, and predictive policing AI systems. However, there are few, if any, studies demonstrating the positive impact AI systems can have on law enforcement operations.

C. EXAMPLES FROM THE EUROPEAN UNION

The European Union, through the European Commission and the High-Level Expert Group on Artificial Intelligence (AI HLEG), has established a framework that outlines ethical principles, baseline requirements, and assessment methodologies for the implementation of trustworthy AI in the European Union.[197] According to the AI HLEG, trustworthy AI complies with all laws and regulations, adheres to ethical principles, and should be robust from a technical and social perspective.[198] Although the guidelines developed by AI HLEG are intended to be broad enough to span across multiple industries, such as private organizations, research facilities, medical institutions, and government entities, they provide baseline requirements to facilitate the responsible implementation of AI.[199] Specific considerations may be required for homeland security applications, but the AI HLEG guidelines offer the most robust case for this technology.

The AI HLEG utilizes international human rights law, the EU Treaties, and the EU Charter to provide the "foundation" of implementing trustworthy AI in the European Union.[200] Since these fundamental rights, such as protection of personal data and respect for private and family life, are guaranteed by law in EU member states, not only is it important to ensure AI does not violate these rights, but it is also important to determine certain circumstances when they are not applicable, such as specific use-cases within the law enforcement or counterterrorism domain.[201] Regardless, AI HLEG argues it is vital for AI systems to adhere to "the ethical principles of respect for human autonomy, prevention of harm, fairness, and explicability."[202] Without these ethical principles in place, AI systems potentially pose substantial risks to individuals and groups that can be difficult to anticipate. Such risks, especially in the law enforcement and homeland security domain, include infringement on individual liberty, privacy issues, and unfair bias, which can lead to

197 High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI," 2–3.

198 High-Level Expert Group on Artificial Intelligence, 2.

199 High-Level Expert Group on Artificial Intelligence, 5–6.

200 High-Level Expert Group on Artificial Intelligence, 9.

201 "Charter of Fundamental Rights of the European Union, OJ 326/391, 26.10.2012" (2012).

202 High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI,* 13.

discriminatory actions or violations of privacy expectations by derivations from large sets of data.

To achieve the aforementioned ethical principles, AI HLEG recommends the following seven requirements to be implemented into the AI system's life cycle:

Human Agency and Oversight—The requirement of human agency and oversight provides the need to ensure fundamental rights provided by the EU Charters and Treaties are not violated by AI systems. The AI HLEG proposes this can be accomplished by proper training and tools for users of the AI system to comprehend, interact, and challenge the AI system.[203] Human oversight is another mechanism that allows human intervention at nearly every "decision cycle" of the AI system.[204]

Technical Robustness and Safety—Technical robustness and safety provide the requirement that AI systems be developed in a manner that protects against vulnerabilities to the system itself or the data within.[205] Technical robustness also speaks to the need to develop systems that are accurate, reliable, and reproducible.[206]

Privacy and Data Governance—Data quality is extremely important in an AI system, encompassing data integrity, and privacy protection. Due to the nature of AI systems, there is the potential to accurately infer sensitive portions of an individual's life, such as religious views or sexual orientation.[207] If data is not adequately governed, data quality can suffer or be maliciously manipulated, leading to potentially harmful bias in the AI system output.[208]

Transparency—Transparency is the process in which an external party to the process can understand how the AI system provided results. This incorporates the concept of traceability, in which the processes used by the AI system can be mapped out, as well as

[203] High-Level Expert Group on Artificial Intelligence, 15–16.

[204] High-Level Expert Group on Artificial Intelligence, 16.

[205] High-Level Expert Group on Artificial Intelligence, 16.

[206] High-Level Expert Group on Artificial Intelligence, 16–17.

[207] High-Level Expert Group on Artificial Intelligence, 17.

[208] High-Level Expert Group on Artificial Intelligence, 17.

explainability, where the decisions made by the AI system can be explained in a format easily understood by humans.[209]

Diversity, Non-Discrimination, and Fairness—Closely related to privacy and data governance, AI systems should avoid biased datasets, which can originate from "historic bias, incompleteness, and bad governance models."[210] Biases can also originate from the programming within the system, regardless of the data used in the model.[211]

Societal and Environmental Well-being—When developing an AI system, it should be developed and implemented in a manner that does not negatively contribute to the environment or maliciously impact societal expectations.[212] Special considerations should be made for the political environment in which it is implemented, as not to undermine established processes or democratic values.[213]

Accountability—Accountability encompasses requirements to enable independent review of processes in the AI system via audits and impact assessments to determine any risks that may occur while using the system.[214] Auditability and impact assessments allow the AI system to be verified, confirming it is working correctly while allowing system owners to accept or mitigate any risk associated with the system.[215]

A potential recommendation is for a specialty agency or committee, similar to the National Institute of Standards and Technology (NIST), to develop a framework for AI system implementation. Organizations like NIST are well-positioned to provide this framework, as they are generally a coordinated effort between subject matter expertise in a particular domain. NIST was founded in 1901 and is a part of the U.S. Department of Commerce. NIST is responsible for technological standards and research studies in use today, such as the NIST

---

[209] High-Level Expert Group on Artificial Intelligence, 17.

[210] High-Level Expert Group on Artificial Intelligence, 18.

[211] Sandvig et al., "Can an Algorithm Be Unethical?"

[212] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI,* 19.

[213] High-Level Expert Group on Artificial Intelligence, 19.

[214] High-Level Expert Group on Artificial Intelligence, 20.

[215] High-Level Expert Group on Artificial Intelligence, 20.

Cybersecurity Framework and reference materials for forensic science. A commission like this would also emulate the EU model by creating a panel of experts similar to the AI HLEG. These experts will be in the best position to develop the framework needed to preserve the seven main requirements outlined by the AI HLEG. Once developed, this framework would outline implementation requirements for AI systems that can then be shared with agencies that may not have resources to create appropriate policies for this technology.

D. RECOMMENDATIONS FOR FUTURE RESEARCH

Based on the results and limitations of this analysis, there are several avenues for additional research on the topic of AI systems usage in the law enforcement domain. One of the most crucial recommendations for research would be additional work in the policy and legislative arena. If law enforcement is to continue to use AI systems and desire to do so in a responsible manner, then there need to be usable policy recommendations drafted that enable law enforcement to use AI systems but also protect the privacy and constitutional rights of the general public. Finding the balance between law enforcement usage and protection of the individual will take additional research through privacy advocate groups, such as the Electronic Frontier Foundation and law enforcement advocacy groups. Additionally, new details and capabilities regarding this technology are discovered on a regular basis. It is an ever-growing capability that will greatly benefit from sound, fungible policy recommendations.

Research into the effectiveness of AI systems in law enforcement practices will greatly enhance this discussion, as well. Currently, research into this topic is limited, but this research would greatly inform policymakers, as well as law enforcement leaders, about the pros and cons regarding the potential impact this technology may have on their agency. Research like this would likely be difficult, as it would require participation from law enforcement agencies currently utilizing AI systems and potentially their vendors.

Lastly, any one of the criteria used throughout this analysis warrants additional research. This thesis served as a look into potential problems that need to be considered for law enforcement agencies to responsibly use AI systems, but there are additional implications for each of the five categories that can be discussed in greater detail. As alluded to earlier,

since this topic is new and constantly evolving, there will likely be changes that require a reassessment of the five categories.

E. CONCLUSIONS

Several conclusions can be made regarding this analysis of AI systems in the law enforcement domain. The first conclusion is that many types of AI systems have the potential to disproportionately affect certain communities of people. Regardless of the AI system evaluated throughout this analysis, black people were consistently impacted the most. This manifested in poor accuracy in AI systems as well as historical trends embedded in datasets used to train AI systems. Regardless of why certain communities are impacted more, law enforcement should not solely trust the outputs of these systems, or they will risk unfair actions against the community they serve.

The second conclusion from this study is there exists a lack in the regulation of this type of technology within the law enforcement community. Regulation exists in the form of policies governing use, legislation provided by a governing body, or any kind of regular auditing of system usage. The creation and enforcement of these regulations will greatly enhance the transparency and accountability of these systems. The European Union has completed and provided recommendations on a framework to ensure responsible usage of AI systems. This framework should be heavily considered for use in the United States in the future.

The third conclusion from this study is the ever-evolving nature of this technology and the need for law enforcement to maintain technology literacy. New studies regarding AI systems and their impact on individuals are coming out on a regular basis. A lack of familiarity with technology was identified as a weakness by the Law Enforcement Forecasting Group in 2018.[216] If law enforcement does not recruit or invest in individuals that are aware of AI systems and their risks, then those law enforcement agencies are bound to either procure systems that do not fit their needs or utilize them in ways that may be detrimental to the community.

---

[216] Law Enforcement Forecasting Group, *Increasing Analytic Capacity of State and Local Law Enforcement Agencies*.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Acquisition of Surveillance Technology, San Francisco, CA, Administrative Code, § 19 (2019). https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

Alake, Richmond. "Algorithm Bias In Artificial Intelligence Needs To Be Discussed (And Addressed)." Medium, April 28, 2020. https://towardsdatascience.com/algorithm-bias-in-artificial-intelligence-needs-to-be-discussed-and-addressed-8d369d675a70.

Anderson, Elisha. "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit." *Detroit Free Press*, July 10, 2020. https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner. "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks." ProPublica, May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=YxUntiDH12MOMHz5OD1yLBRth4wTzdEG.

Ashton, Henry, and Matt Hancock. Data Protection Act 2018, § 2018 Chapter 12 (2018). https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm.

Babuta, Alexander, Marion Oswald, and Christine Rinik. *Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges*. Whitehall Report 3–18. London: Royal United Services Institute, 2018. https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

Bacchini, Fabio, and Ludovica Lorusso. "Race, Again: How Face Recognition Technology Reinforces Racial Discrimination." *Journal of Information, Communication and Ethics in Society* 17, no. 3 (August 2019): 321–35. https://doi.org/10.1108/JICES-05-2018-0050.

Barocas, Solon, and Helen Nissenbaum. "Big Data's End Run Around Procedural Privacy Protections." *Communications of the ACM* 57, no. 11 (November 2014): 31–33. https://doi.org/10.1145/2668897.

Berman, Emily. "A Government of Laws and Not of Machines." *Boston University Law Review* 98, no. 5 (October 2018): 1277–1356.

Bhageshpur, Kiran. “Data Is the New Oil -- and That’s a Good Thing.” Forbes, November 15, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/.

Brennan, Tim, William Dieterich, and Beate Ehret. “Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System.” *Criminal Justice and Behavior* 36, no. 1 (October 20, 2008): 21–40. https://doi.org/10.1177/0093854808326545.

Cady, Field. *The Data Science Handbook*. Hoboken, NJ: John Wiley & Sons, Inc, 2017.

California Consumer Privacy Act of 2018, California Civil Code, § 1798.100 (2018).

Caplan, Robyn, Joan Donovan, Lauren Hanson, and Jeanna Matthews. *Algorithmic Accountability: A Primer*. Washington, DC: Data & Society Research Institute, 2018. https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

Castro-Zunti, Riel D., Juan Yépez, and Seok-Bum Ko. “License Plate Segmentation and Recognition System Using Deep Learning and OpenVINO.” *IET Intelligent Transport Systems* 14, no. 2 (February 1, 2020): 119–26. https://doi.org/10.1049/iet-its.2019.0481.

Charter of Fundamental Rights of the European Union, OJ 326/391, 26.10.2012 (2012).

Corbett-Davies, Sam, Emma Pierson, Avi Feller, Sharad Goel, and Aziz Huq. “Algorithmic Decision Making and the Cost of Fairness.” In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 797–806. KDD ‘17. Halifax, NS, Canada: Association for Computing Machinery, 2017. 10.1145/3097983.3098095.

Deane, Michael. “AI and the Future of Privacy.” Medium, September 7, 2018. https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4.

DeMichele, Matthew, Peter Baumgartner, Michael Wenger, Kelle Barrick, Megan Comfort, and Shilpi Misra. *The Public Safety Assessment: A Re-Validation and Assessment of Predictive Utility and Differential Prediction by Race and Gender in Kentucky*. SSRN Journal, 2018. https://www.ssrn.com/abstract=3168452.

Dharaiya, Divyesh. “History of Facial Recognition Technology and Its Bright Future.” readwrite, March 12, 2020. https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/.

Dixon, Lucas, John Li, Jeffrey Sorensen, Nithum Thain, and Lucy Vasserman. "Measuring and Mitigating Unintended Bias in Text Classification." In *Proceedings of AAAI/ACM Conference on AI, Ethics, and Society*, 67–73. New Orleans, LA, USA: ACM Press, 2018. http://dl.acm.org/citation.cfm?doid=3278721.3278729.

Economist. "The World's Most Valuable Resource Is No Longer Oil, but Data." *Economist*, May 6, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Ehteshami Bejnordi, Babak, Mitko Veta, Paul Johannes van Diest, Bram van Ginneken, Nico Karssemeijer, Geert Litjens, Jeroen A. W. M. van der Laak, and and the CAMELYON16 Consortium. "Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer." *JAMA* 318, no. 22 (December 12, 2017): 2199–2210. https://doi.org/10.1001/jama.2017.14585.

Electronic Frontier Foundation. "Search the Data – Atlas of Surveillance." Accessed January 10, 2021. https://atlasofsurveillance.org/search?sort=state_desc&technologies%5B86%5D=on.

European Commission. *On Artificial Intelligence – A European Approach to Excellence and Trust*. COM(2020) 65 Final. Brussels: European Commission, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN.

Federal Bureau of Investigation. "Next Generation Identification (NGI)." Accessed September 4, 2020. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

Ferranti, David de, Justin Jacinto, Anthony J. Ody, and Graeme Ramshaw. *How to Improve Governance: A New Framework for Analysis and Action*. Brookings Institution Press, 2009.

Future of Privacy Forum. *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning*. Washington, DC: International Association of Privacy Professionals, 2018. https://iapp.org/media/pdf/resource_center/FPF_Artificial_Intelligence_Digital.pdf.

Garvie, Clare, Alvaro M Bedoya, Jonathan Frankle, Moriah Daugherty, Katie Evans, Edward J George, Sabrina McCubbin et al. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Washington, DC: Center on Privacy and Technology at Georgetown Law, 2019. https://www.perpetuallineup.org/.

Goodwin, Gretta L. *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains*. GAO-19-579T. Washington, DC: Government Accountability Office, 2019.

Green, Andy. “Complete Guide to Privacy Laws in the US.” *Inside Out Security* (blog), March 29, 2020. https://www.varonis.com/blog/us-privacy-laws/.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Test Part 3: Demographic Effects*. NISTIR 8280. Gaithersburg, MD: National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.IR.8280.

Guariglia, Matthew. “Technology Can’t Predict Crime, It Can Only Weaponize Proximity to Policing.” Electronic Frontier Foundation, September 3, 2020. https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing.

Harvard Law Review. “State v. Loomis.” Harvard Law Review, March 10, 2017. https://harvardlawreview.org/2017/03/state-v-loomis/.

High-Level Expert Group on Artificial Intelligence. “Ethics Guidelines for Trustworthy AI: High-Level Expert Group on Artificial Intelligence.” European Commission, 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

Hill, Kashmir. “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match.” *New York Times*, December 29, 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

———. “Wrongfully Accused by an Algorithm.” *New York Times*, June 24, 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Hollywood, John, Dulani Woods, Andrew Lauland, Brian Jackson, and Richard Silberglitt. *Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group*. Santa Monica, CA: RAND, 2018. https://doi.org/10.7249/RR1987.

Julia Angwin, Jeff Larson. “Machine Bias.” Text/html. ProPublica, May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Kerr, Orin S. “The Mosaic Theory of the Fourth Amendment.” *Michigan Law Review* 111, no. 3 (December 2012): 311–54.

Kirkpatrick, Keith. “It’s Not the Algorithm, It’s the Data.” *Communications of the ACM* 60, no. 2 (January 23, 2017): 21–23. https://doi.org/10.1145/3022181.

Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner. “How We Analyzed the COMPAS Recidivism Algorithm.” ProPublica, May 23, 2016. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Lau, Tim. “Predictive Policing Explained.” Brennan Center for Justice, April 1, 2020. https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

PredPol. “Law Enforcement | PredPol Law Enforcement Intelligence Led Policing Software | PredPol Law Enforcement Intelligence Led Policing Software.” Accessed November 24, 2020. https://www.predpol.com/law-enforcement/.

Law Enforcement Forecasting Group. *Increasing Analytic Capacity of State and Local Law Enforcement Agencies: Moving Beyond Data Analysis to Create a Vision for Change*. 2010-DB-BX-K003. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice, 2012. https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/LEFGIncreasingAnalyticCapacity.pdf.

Levy, Jack S. “Case Studies: Types, Designs, and Logics of Inference.” *Conflict Management and Peace Science* 25, no. 1 (February 2008): 1–18. https://doi.org/10.1080/07388940701860318.

LII / Legal Information Institute. “Townsend v. Burke.” Accessed November 8, 2020. https://www.law.cornell.edu/supremecourt/text/334/736.

Lum, Kristian, and William Isaac. “To Predict and Serve?” *Significance*, October 2016.

Malik, Abish, Ross Maciejewski, Sherry Towers, Sean McCullough, and David S Ebert. “Proactive Spatiotemporal Resource Allocation and Predictive Visual Analytics for Community Policing and Law Enforcement.” *IEEEE Transactions on Visualization and Computer Graphics* 20, no. 12 (2014): 10. https://doi.org/10.1109/TVCG.2014.2346926.

Manheim, Karl, and Lyric Kaplan. “Artificial Intelligence: Risks to Privacy and Democracy.” *Yale Journal of Law and Technology* 21, no. 106 (December 13, 2019): 107–88.

National Science and Technology Council. *Preparing for the Future of Artificial Intelligence*. Washington, DC: Executive Office of the President, 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

Northpointe. *Practitioner’s Guide to the COMPAS Core*. Northpointe Inc., 2015. http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf.

Osoba, Osonde, and William Welser. *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1744.html.

———. *The Risks of Artificial Intelligence to Security and the Future of Work*. PE-237-RC. RAND Corporation, 2017. https://doi.org/10.7249/PE237.

Perry, Walt L., Brian McInnis, Carter C. Price, Susan C. Smith, and John S. Hollywood. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RR-233-NIJ. Santa Monica, CA: RAND, 2013. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

PredPol. "PredPol Mission." Accessed November 24, 2020. https://www.predpol.com/about/.

Roberts, David J, and Meghann Casanova. *Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide, Summary*. 239605. Alexandria, VA: International Association of Chiefs of Police, 2012. https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf.

Rouse, Margaret. "What Is Black Box AI?" WhatIs. Accessed November 21, 2019. https://whatis.techtarget.com/definition/black-box-AI.

Sacca, Giacomo. "Not Just Another Piece of Equipment: An Analysis for Police Body-Worn Camera Policy Decisions." Master's thesis, Naval Postgraduate School, 2017. https://calhoun.nps.edu/handle/10945/56797.

Sandvig, Christian, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort. "Can an Algorithm Be Unethical?" In *65th Annual Meeting of the International Communication Association*. San Juan, Puerto Rico: ICA, 2015. http://social.cs.uiuc.edu/papers/pdfs/ICA2015-Sandvig.pdf.

Schuppe, Jon. "How Facial Recognition Became a Routine Policing Tool in America." *NBC News*, May 11, 2019. https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

Shankland, Stephen. "Boosted by Ai, Facial Recognition Eases Our Path Through an Increasingly Digital World." CNET, March 28, 2019. https://www.cnet.com/news/huge-leaps-in-ai-have-made-facial-recognition-smarter-than-your-brain/.

Smith, Mark P. "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies." Official memorandum, Los Angeles, CA: Los Angeles Police Department, 2019. http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

Spielberg, Steven. *Minority Report*. 20th Century Fox, 2002.

Strauss, Peter. "Due Process." Cornell Law School Legal Information Institute. Accessed September 13, 2020. https://www.law.cornell.edu/wex/due_process.

Surveillance Technology, *Santa Cruz Municipal Code* § 9.85 (2020). https://www.codepublishing.com/CA/SantaCruz/#!/SantaCruz09/SantaCruz0985.html#9.85.

Sweeney, Latanya. *Simple Demographics Often Identify People Uniquely*. Data Privacy Working Paper 3. Pittsburgh, PA: Carnegie Mellon University, 2000.

Teufel III, Hugo. "Privacy Policy Guidance Memorandum." Official memorandum. Washington, DC: U.S. Department of Homeland Security, December 29, 2008. https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

National Archives. "The Bill of Rights: A Transcription," November 4, 2015. https://www.archives.gov/founding-docs/bill-of-rights-transcript.

V. Kavya, and Arumugam S. "A Review on Predictive Analytics in Data Mining." *International Journal of Chaos, Control, Modelling and Simulation* 5, no. 1/2/3 (September 30, 2016): 1–8. https://doi.org/10.5121/ijccms.2016.5301.

Verma, Sahil, and Julia Rubin. "Fairness Definitions Explained." In *Proceedings of the International Workshop on Software Fairness*, 1–7. Gothenburg, Sweden: ACM, 2018. https://doi.org/10.1145/3194770.3194776.

Villasenor, John, and Virginia Foggo. "Artificial Intelligence, Due Process, and Criminal Sentencing." *Michigan State Law Review*, no. 295 (2020): 60.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* IV, no. 5 (December 15, 1890): 29.

WCPO Statement in Response to New York Times Article Wrongfully Accused by an Algorithm, June 24, 2020. WCPO Press Release. Detroit, MI: County of Wayne, 2020.

Woodward, John D., Jr., Christopher Horn, Julius Gatune, and Aryn Thomas. *Biometrics: A Look at Facial Recognition*. Santa Monica, CA: RAND Corporation, 2003. https://apps.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf.

Završnik, Aleš. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." *ERA Forum, Journal of the Academy of European Law* 20, no. 4 (February 2020): 567–583. https://doi.org/10.1007/s12027-020-00602-0.

Zoufal, Donald R. "'Someone to Watch Over Me?' Privacy and Governance Strategies for CCTV and Emerging Surveillance Technologies." Master's thesis, Naval Postgraduate School, 2008. https://calhoun.nps.edu/handle/10945/4167.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California