USING AI-POWERED SYSTEMS FOR IDENTIFYING AND INVESTIGATING CYBERCRIMES TO ENHANCE CYBERSECURITY IN LAW ENFORCEMENT

by

CHRISTOPHER S. HOPE

BS, University of Phoenix, 2014

MS, University of Phoenix, 2016

A Research Paper Submitted to the School of Computing Faculty of
Middle Georgia State University in
Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2024

USING AI-POWERED SYSTEMS FOR IDENTIFYING AND INVESTIGATING CYBERCRIMES TO ENHANCE CYBERSECURITY IN LAW ENFORCEMENT

Christopher S. Hope, Middle Georgia State University, christopher.hope@mga.edu

Abstract

Artificial Intelligence (AI) can be a valuable ally for law enforcement in combating crime in the digital age. AI's analytical capabilities have several advantages, including detecting patterns, processing vast amounts of data, and analyzing unstructured data. Some challenges require responsible implementation, such as mitigating bias, protecting privacy, and ensuring transparency and accountability. This study aims to explore the potential of AI in improving criminal investigations and prosecution rates, determine methods for safeguarding sensitive data, and encourage responsible AI use to advance justice in the digital age. By utilizing AI's power responsibly, law enforcement can combat crime more effectively, protect communities, and uphold the principles of justice.

Keywords: Artificial Intelligence (AI), Law Enforcement, Criminal Investigations, Crime Prevention, Cybersecurity, Data Analysis, Algorithmic Bias, Ethical Considerations

Introduction

In today's digital age, hackers use various tactics to access sensitive information, including social engineering. Hackers trick employees into revealing the data needed to infiltrate a network by pretending to be a trustworthy third-party entity (Pettit, 2023). This is the first step in a series of actions to gain administrative control of targeted data. However, organizations with robust monitoring and alert systems can identify unusual behavior, privilege escalation, and other signs of a potential attack, which can help thwart hackers' efforts.

While technology has given criminals an edge over law enforcement, it has also provided the police with tools to work more intelligently and efficiently. By continually improving their methods, law enforcement stays ahead of criminal activity (Johnson et al., 2023). Integrating Artificial Intelligence (AI) into criminal investigations presents an opportunity to solve more cases and improve prosecution rates. Once viewed skeptically for local government use, cloud-based storage has emerged as a cost-effective option with enhanced security features and increased computing capacity, which is particularly beneficial for complex tasks like analytics and digital forensics (Chowdhury, 2021).

This study examined the use of AI in criminal investigations and its potential to enhance case resolution and prosecution rates. AI can identify potential criminal activity, from financial crimes to cyber fraud and employee theft. By assisting law enforcement agencies in processing and analyzing vast amounts of data, AI acts as a force multiplier, saving time and money while improving accuracy. In addition, combining human expertise with AI can streamline forensic investigations, enabling investigators to focus on areas where fraud is most likely to occur. The ability of AI to process unstructured data, such as videos, images, e-mails, and text files, also holds the potential to revolutionize criminal investigations by offering a more efficient and practical approach to fighting crime (Europol, 2023).

This research explored how AI can improve criminal investigations, focusing on enhancing case resolution and prosecution rates. Using AI's analytical capabilities, law enforcement agencies can identify and prosecute criminal activities more accurately and efficiently (Rigano, 2018). The collaboration between human expertise and AI can lead to more streamlined forensic investigations and targeted efforts to combat fraudulent activities (Sayegh, 2022). AI's ability to analyze unstructured data can transform criminal

investigations, offering a practical and resource-efficient approach to combating crime (Police 1, 2022). This study provides valuable insights to inform future strategies, encourage innovation, and advance justice in the digital age.

The implementation of AI has the potential to significantly enhance criminal investigations, leading to an increased rate of case resolution and prosecution. AI technology can identify areas of potential criminal activity, ranging from money laundering, fraud, and terrorist financing to more commonplace crimes like cyber fraud, employee theft, and fake invoices. By assisting law enforcement agencies in processing and analyzing vast amounts of data, AI acts as a force multiplier, saving time and money while improving accuracy (Rigano, 2018).

Moreover, by combining human expertise with AI, forensic investigations can be streamlined, saving valuable time and resources and enabling investigators to focus on areas where fraud is most likely to occur. AI also allows companies to process unstructured data, such as videos, images, e-mails, and text files, to detect criminal activity and prevent potential crimes. This technology can potentially revolutionize criminal investigations, providing a more efficient and practical approach to fighting crime (Rigano, 2018). This research will answer the following question:

RQ1: *How can integrating artificial intelligence techniques enhance the effectiveness of law enforcement agencies in investigating crimes and enforcing the law?*

Review of the Literature

AI Integration in Law Enforcement

A study aimed to gather insights from 111 citizens on using AI by law enforcement agencies (LEAs) in the context of cybercrime and terrorism. The participants provided valuable suggestions for necessary safeguards, highlighting several key themes. Firstly, educating LEA staff on ethical practices and civic education can help children understand data collection processes and the role of AI in decision-making. It is crucial to simplify language, use short sentences, and avoid technical terms to make the information accessible and easy to understand. By prioritizing the most essential information and organizing it logically, we can ensure that the text flows smoothly and is easily comprehended.

Additionally, using active voice and simple vocabulary can further increase the text's clarity and effectiveness. (Ezzeddine et al., 2023). Secondly, participants recommended regular evaluations of AI tools to prevent biases and detect algorithm errors.

Rigano (2018) also stressed the need to anonymize collected data to protect privacy and prevent misuse properly. Thirdly, the development of legal frameworks, national and international regulations, and policies to limit LEAs' use of data. It was also suggested that independent agencies or third parties monitor and supervise AI implementation. Fourthly, participants suggested careful selection and vetting of staff involved in AI data collection and handling. The importance of human validation of AI decisions and interpretations to avoid errors and biases was highlighted. Fifthly, concerns were expressed about invasion of privacy, and it was recommended that data collection be limited, consent from individuals be obtained, and non-relevant information be disposed of (Rigano, 2018).

Ezzeddine et. Al (2023) suggested judicial control over obtained information. A small group of participants opposed using AI altogether and suggested relying on traditional methods. Lastly, some participants acknowledged the existence of adverse effects but questioned the feasibility of preventing them. The study emphasizes the importance of citizen perspectives in legitimizing the deployment of AI tools by LEAs. The findings highlight the need for safeguards to address concerns related to privacy, biases, and potential negative consequences of AI use in law enforcement (Ezzeddine et al., 2023). The insights gained can contribute to developing responsible AI practices and policies in the context of LEAs.

In the article, How Will Artificial Intelligence Affect Policing and Law Enforcement? The article discussed various aspects of AI's role in policing, such as predictive policing, surveillance technologies, and data analysis. Predictive policing involves using AI algorithms to analyze historical data to predict potential criminal activity, which can help law enforcement allocate resources effectively (Editorial Team, 2023). The article also examined using AI-powered surveillance technologies, including facial and license plate recognition, in law enforcement. However, the article highlighted ethical concerns surrounding AI in policing, such as privacy, bias, and potential abuse. It emphasizes the importance of transparency and accountability in AI-powered law enforcement, calling for clear regulations and oversight. The article also stresses the impact of AI on community trust in law enforcement and how striking the right balance between technological innovation and civil liberties is crucial. Overall, the article explores the growing role of AI in policing, its potential benefits, ethical concerns, and the importance of ensuring transparency and accountability to maintain public trust (Hsiung et al., 2023).

Law Enforcement Framework

The Cybersecurity Resilience and Law Enforcement Collaboration (CyRLEC) Framework is an all-encompassing strategy for cybersecurity that prioritizes cooperation with law enforcement to minimize online attacks. This framework aims to establish a comprehensive and integrated approach to cybersecurity by emphasizing collaboration with law enforcement agencies to mitigate cyber threats (Schiliro, 2023). Its five core components include risk management, prevention, detection, response, and collaboration. A comparison of the CyRLEC Framework and the NIST Cybersecurity Framework reveals significant distinctions. The study used a qualitative design with semi-structured interviews in a simulated real-world situation, focusing on healthcare organizations. The study concluded that the CyRLEC Framework is an adaptable and thorough system for managing cybersecurity risks, particularly in the healthcare industry (Schiliro, 2023).

The research findings demonstrate the value of the CyRLEC Framework in improving cybersecurity resilience and promoting effective collaboration with law enforcement agencies. The paper contributes to the knowledge of cybersecurity frameworks and offers practical insights for organizations seeking to enhance their cybersecurity posture (Ratiu, 2023).

Machine Learning and Law Enforcement

Berk (2020) explored the applications of machine learning and big data analytics in criminology and criminal justice. The recent developments in these technologies and their potential impact on understanding and addressing crime-related issues were also explored (Berk, 2020).

Redden et al. (2020) highlight that machine learning, a subset of artificial Intelligence, has become increasingly prominent in analyzing large volumes of data and extracting patterns and insights (Redden et al., 2020). Machine learning algorithms can be applied to criminology and criminal justice fields. These algorithms can help with crime prediction, offender profiling, and risk assessment.

Furthermore, the potential benefits of employing big data analytics in criminology research are emphasized in the article. Researchers can identify trends, correlations, and predictive patterns in criminal behavior by analyzing significant amounts of data, such as criminal records, social media activity, and geographical information (Chiancone, 2023). This information can be valuable in designing effective crime prevention strategies, resource allocation, and policymaking.

Law enforcement can use data analysis to identify trends, correlations, and predictive patterns in criminal behavior. Various data sources, including criminal records, social media activity, and geographical information, can be collected and integrated to locate crime hotspots, detect potential threats, and allocate resources more efficiently. Advanced analytical techniques like machine learning algorithms and predictive analytics models can help forecast the likelihood of crimes occurring in specific areas or timeframes. With

data-driven insights, law enforcement can design effective crime prevention strategies, allocate resources efficiently, and continuously evaluate and refine their approaches (George, 2019).

The challenges of using machine learning and big data analytics in this field include data quality, privacy concerns, algorithmic bias, and interpretability (Berk, 2020). The importance of addressing these challenges and ensuring these technologies' ethical and transparent use is emphasized. The article continues to identify potential future directions for research and practice in the field of criminology and criminal justice, including the integration of multiple data sources, real-time data utilization for crime prevention, and interdisciplinary collaborations to leverage the full potential of machine learning and big data analytics (McKay et al., 2022).

Raaijmaker (2019) discussed the challenges and opportunities of integrating artificial Intelligence (AI) in law enforcement workflows, particularly security. The research emphasized the need for AI models to be explainable and auditable, allowing for transparency and accountability. The article also addressed the issue of bias in AI systems and the importance of handling it properly. It highlighted the role of human factors in effectively utilizing AI in law enforcement, including the need for training and supporting personnel in understanding and interpreting AI model outcomes (Raaijmakers, 2019). Finally, the research underscored the potential benefits of AI in law enforcement while acknowledging the obstacles that need to be overcome for successful integration.

According to an article by Police 1 (2022), the most prominent technology challenges facing police leaders discuss the significant technology challenges faced by police leaders. It highlighted several key issues, including the need for better data integration and sharing, the challenge of managing and protecting sensitive information, the impact of emerging technologies such as artificial Intelligence and predictive analytics, and the increasing demand for digital evidence collection and storage (Police 1, 2022). The article emphasizes the importance of investing in technological solutions that can enhance law enforcement capabilities while addressing privacy and accountability concerns and addressing the critical role of technology in modern policing and the need for police leaders to navigate these challenges effectively (Police 1, 2022).

Social Engineering

Sayegh (2022) described social engineering as a low-tech but highly effective method for cybercriminals to exploit human vulnerabilities and gain unauthorized access to sensitive information (Sayegh, 2022). It explains how social engineering techniques, such as phishing, pretexting, and baiting, manipulate human behavior to deceive individuals into divulging confidential data or performing actions that compromise security. The article highlighted the risks associated with social engineering attacks and emphasized the need for individuals and organizations to be aware of these tactics and implement robust security measures. It also provides practical tips and recommendations to mitigate social engineering risks, including employee training, strong password practices, and multi-factor authentication. The overall message is to raise awareness about the dangers of social engineering and encourage proactive measures to protect against such threats (Sibley, 2023).

In a study conducted by Rigano (2018), the article discussed the use of artificial Intelligence (AI) in addressing the needs of the criminal justice system. It highlighted how AI technologies can enhance various aspects of criminal justice, including crime prevention, law enforcement, and offender rehabilitation (Rigano, 2018). The article provided examples of AI applications, such as predictive policing algorithms, facial recognition systems, and risk assessment tools, that can assist in making more informed decisions and allocating resources more effectively. It also acknowledges the potential challenges and ethical considerations of using AI in criminal justice, such as bias and privacy concerns (Zvelo, 2023). The article emphasizes the importance of responsible and accountable use of AI, promoting transparency, fairness, and ongoing evaluation of these technologies (Novak, 2023). It concluded by discussing the possibilities and the potential for AI to impact the criminal justice field significantly.

AI Implementation in Airports

The use of artificial Intelligence (AI) in airport security has been a topic of interest and discussion in recent years (Puckett, 2023). AI can enhance security by reducing human error and improving threat detection (Jacobson, 2022). The application of AI in airport security raises several ethical concerns of privacy implications when using AI to assess traveler intent. This article provides an overview of the use of AI in airport security, focusing on the Transportation Security Administration's (TSA) trials using AI to predict passenger intent.

Jacobson (2022) highlighted the challenges associated with this technology, including the possibility of errors in AI assessments and the potential for bias against certain groups of travelers (Jacobson, 2022). Despite these challenges, the potential benefits of AI are also acknowledged, such as reducing physical screenings and streamlining the travel process.

TSA faces ethical limits on AI, but advancement work must persist. It concluded that AI development in airport security must be pursued responsibly and ethically to maintain a competitive edge. The author advocates for balancing security concerns with individual rights and freedoms. This requires careful consideration of the implications of AI technology on privacy and civil liberties and a commitment to ensuring that the use of AI in airport security is by ethical standards (Jacobson, 2022). AI in airport security can potentially revolutionize the field, but it must be done responsibly and ethically.

The utilization of facial recognition technology by the Transportation Security Administration (TSA) at airports has been a topic of much discussion. While the TSA claims its pilot program was 97% effective, there are concerns regarding the accuracy of the technology and the privacy implications that come with it (Davis, 2023). The TSA intends to make facial recognition mandatory in the future, but critics have raised concerns regarding its reliability and privacy implications. The agency plans to expand facial recognition technology to more than 400 airports across the United States. However, critics are apprehensive about its accuracy, particularly in misidentifying individuals of color and the privacy implications of collecting and storing facial scans of millions of travelers (Davis, 2023). Proponents have argued that facial recognition technology can enhance security and expedite the screening process, but critics argue that its drawbacks far outweigh its benefits. Some argue that the technology is unreliable and can be used to monitor and track individuals without their consent. The possibility of targeting specific groups, such as Muslims or immigrants, also causes concern among critics. It is imperative to weigh the potential benefits of the technology against the risks before deciding whether to use it (Davis, 2023).

Methodology

A qualitative Delphi study was utilized to determine the best methods to discern optimal strategies for safeguarding sensitive data held within law enforcement agencies. As in most studies, it is the objective to obtain an unbiased sample. In the Delphi method, a panel of experts is formed from individuals in the field. Therefore, the method of selecting expert panel members should be strategic and unbiased as well. Two studies were identified that provide explicit guidance for qualifying individuals as experts. Since most studies incorporate between eight and 16 panelists, a minimum of eight is suggested. The number of panelists should be determined by factors such as the availability of experts, desired geographic representation, and facilitator capability. Using this method of study has the expertise of individuals in the field (Nasa, Jain, & Juneja, 2021). This study investigated how AI can improve criminal investigations and law enforcement efforts. It highlighted AI's ability to identify criminal activities and process large amounts of data, leading to higher case resolution rates (Berk, 2020). The study recognized the challenges in dealing with cybercrime and emphasized the need for continuous improvement in law enforcement tactics. The

study aimed to contribute to understanding the potential benefits and challenges associated with AI implementation in criminal justice (Ezzeddine et al., 2023).

Research Objectives

The study explored the potential of AI for improving criminal investigations and prosecution rates. It identified methods for safeguarding sensitive data within law enforcement agencies, deepened our understanding of the benefits and challenges of AI in criminal justice, and encouraged the responsible use of AI to advance justice in the digital age. The study used a qualitative Delphi methodology to gather data from a panel of criminal justice and AI experts. Findings were used to develop guidelines for responsible and effective AI deployment in criminal investigations. This research had significant implications for improving law enforcement's effectiveness in investigating and prosecuting cybercrimes while ensuring ethical and responsible AI use.

Sample

A distinguished panel of twelve individuals were asked to participate from across the United States was asked to assess the use of Artificial Intelligence (AI) in criminal investigations and its potential to enhance case resolution and prosecution rates (Nasa et al., 2021). Each panel member has been carefully selected based on their field expertise and background in AI, hacking, programming, and law enforcement. The criteria for selection were based on their experience and training. Possessing profound insights into these incidents' professional and personal aspects and their inclusion promises to offer invaluable knowledge in preventing future breaches.

Individuals were selected randomly based on their qualifications, certifications, and current positions without any specific organization or individual in mind to ensure impartiality. Each panel candidate is certified in their respective area of expertise and has a technological background in a supervisory role within a company. Participants in the study included local sheriff and police departments, state agencies, as well as experts in AI from private technology companies. The participants were scattered throughout the State of Georgia and Florida, which provides a broad scope of participants with different expectations based on the data specific to their region.

Procedures

Questionnaires were distributed in the form of electronic mail (e-mail) to distribute the web link and a quick response (QR) code that will direct the participants to the online survey device SurveyMonkey, and the opinions of these experts will remain anonymous. Participants were given two weeks to respond, followed by round two of the survey and given two additional weeks. To promote unbiased answers, each member will have no intermediary, nor will participants be subjected to the resolutions of the other panel members, which will preclude the influence in any path. With this method, the research structure is founded on the expertness of the control board members and cannot be touched by the influence of any arrangement that the outcomes of the inquiry may feign. Each cycle is designed to get a consensus from the panel, and the NVIVO software will be applied to identify any trends in the inquiry.

The Delphi process will involve three iterative rounds of questionnaires:

Round 1: Open-ended questions will explore AI use in criminal investigations, data collection methods, and public/law enforcement trust in AI. These responses will establish a baseline.

Round 2: The questions will build upon Round 1's findings, refining the discussion with themes identified from expert feedback.

Round 3 (Optional): A summary of key findings will initiate focused discussions on optimal implementation strategies and potential solutions.

Each round will allow approximately two weeks for responses, with flexibility to accommodate unforeseen issues. Data will be analyzed using NVivo software to categorize responses and identify emergent themes.

Results

How can integrating artificial intelligence techniques enhance the effectiveness of law enforcement agencies in investigating crimes and enforcing the law?

Twelve individuals were asked to participate; six responded to the survey, setting the response rate among the participants at 50 percent. Of those who responded, most participants favored implementing AI in a law enforcement setting, as shown in Table 1. According to survey respondents, AI could streamline tasks such as transcribing interviews, analyzing vast datasets, cross-referencing information, and identifying patterns that human analysts might miss. It could also be helpful for evidence analysis, including facial recognition and object tracking in video footage, DNA analysis, and identifying suspects through social media language. Additionally, AI could provide initial contact via chatbots, self-reporting tools for crimes, and more effectively identify victim needs and resources for victim support.

Table 1 Overall results

Positive Responses (%)	Negative Responses (%)
67.96%	32.04%

AI bias, accuracy, and privacy concerns must be addressed before effective implementation. Respondents favored using focused AI applications for clearly defined tasks rather than a complete overhaul of policing. Calls for transparency, oversight, and strong policies highlight the need for proactive accountability frameworks alongside AI development. Many also doubted AI's suitability for complex tasks like de-escalation or replacing human judgment.

The findings of the survey suggest that there is an overall positive outlook on the incorporation of AI in law enforcement. The participants were divided into two distinct categories: those who work in law enforcement and those who do not. Those affiliated with law enforcement displayed a slightly stronger inclination toward implementing AI in their profession. In contrast, those without any affiliation showed a slightly lower level of enthusiasm but remained neutral in their views. Additionally, the study's findings showed that males were more likely to have negative responses toward AI than females, as shown in Table 2. While the sample size may not fully represent the wider population, these results indicate that the acceptance of AI in law enforcement is mainly viewed favorably.

Table 2 Results by Gender

Gender	Positive Responses (%)	Negative Responses (%)
Male	55.56%	44.44%
Female	100%	0%

Additionally, a breakdown by agency revealed that law enforcement agencies were more open to utilizing AI than subject matter experts. It is worth mentioning that the subgroup of Florida Sheriffs showed the

highest rate of positive response among the subcategories, as indicated in Table 3. Conversely, the AI SME group displayed the lowest positive response rate among the categories listed.

Table 2 Results by agency

Law Enforcement Status	Positive (%)	Negative (%)
GA Sheriffs	22.65%	10.74%
FL Sheriffs	33.98%	9%
AI SME	11.33%	12.3%

In conclusion, the data shows that AI has the potential to make law enforcement more effective, mainly in investigative support and efficiency gains. However, successful integration builds trust by proactively addressing bias concerns, ensuring transparency, and safeguarding privacy. It also requires emphasizing AI as a powerful tool to assist officers, not replace them, and involving the community in discussions about AI's role in shaping implementation and addressing concerns. Figure 1 is a word cloud that exhibits the most frequently used terms in a dataset about law enforcement and body-worn cameras. The size and boldness of a word denote its prevalence in the text. Prominent concepts include "law," "enforcement," "police," and "body-worn," as well as "evidence," "accountability," "transparency," and "justice." Additional words like "data," "public," "safety," and "crime" are also present in smaller print. Furthermore, the cloud draws attention to negative aspects of law enforcement with terms such as "criminal," "suspicious," and "oversight.".

Figure 1 Word Cloud of Frequent Words

Figure 2

Limitations

The drawbacks of relying on small sample sizes in survey research are widely acknowledged and require careful consideration. Findings from such studies may only apply to a limited population, making it essential to use more comprehensive and representative samples for more reliable insights. Although open-ended questions can provide rich qualitative data, analyzing them from a quantitative perspective can be challenging. Additionally, survey participation is voluntary, which can attract respondents with preconceived opinions and introduce bias. The absence of demographic data can also obscure the influence of factors like age, education, or technological proficiency on attitudes toward AI.

To ensure the accuracy and reliability of future research, a more extensive and diverse sample must be required to represent the population of interest accurately. Random sampling methods can help mitigate selection bias. A mixed-methods approach incorporating open-ended and closed-ended questions like Likert scales can yield qualitative and quantitative data. By collecting demographic information, we can analyze how age, education, and familiarity with technology influence viewpoints. Moreover, honing in on specific AI implementations, such as facial recognition and data analysis, can unveil more nuanced support or concerns, enhancing clarity.

Conclusion

This research focused on the application of Artificial Intelligence (AI) in criminal investigations and prosecutions. AI presents significant potential in various areas, including pattern recognition, data processing, and analysis of unstructured data. However, some challenges must be addressed, such as bias, privacy, and transparency. Experts recommend using AI in law enforcement, but it should be used to complement human judgment, not replace it. Proactive measures like regular bias audits, independent oversight, and robust policies are necessary to ensure AI's ethical and accountable use. Community engagement, transparency, and educational initiatives are also critical. Future studies should expand their scope to include more extensive and diverse samples and explore specific AI applications. Ethical safeguards are essential for AI to revolutionize criminal investigations and law enforcement, and further research and regulatory frameworks will establish responsible use.

References

Amos, Z. (2022, 03 30). *The State of AI in Policing*. Retrieved from Unite.AI: https://www.unite.ai/the-state-of-ai-in-policing/

Berk, R. (2020, 11 13). *Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement.* Retrieved from Annual Reviews.org: https://www.annualreviews.org/doi/10.1146/annurev-criminol-051520-012342

Chiancone, C. (2023, October 03). *The Role of Artificial Intelligence in Law Enforcement.* Retrieved from LinkedIn.com: https://www.linkedin.com/pulse/role-artificial-intelligence-law-enforcement-chris-chiancone/

Chowdhury, M. (2021, August 13). *AI in Forensic Investigation and Crime Detection.* Retrieved from Analytics Insight: https://www.analyticsinsight.net/ai-in-forensic-investigation-and-crime-detection/

Cooper, D., & Schindler, P. (2014). *Business Research* (12th ed.). New York, NY, USA: McGraw-Hill/Irwin.

Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Vol. 5th). Los Angeles, CA: SAGE Publications, Inc. doi:2017044644

Davis, W. (2023, July 01). *The TSA will use facial recognition in over 400 airports.* Retrieved from The Verge: https://www.theverge.com/2023/7/1/23781040/the-tsa-will-use-facial-recognition-in-over-400-airports

Editorial Team. (2023, 07 15). *How Will Artificial Intelligence Affect Policing and Law Enforcement?* Retrieved from Artificial Intelligence +: https://www.aiplusinfo.com/blog/artificial-intelligence-ai-and-policing/

Europol. (2023, March 27). *ChatGPT: The impact of Large Language Models on Law Enforcement.* Retrieved from europol.eruopa.eu: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Citizen Perspectives on Necessary Safeguards to the Use of AI by Law Enforcement Agencies. *Springer Nature - Book Series 2023: Transactions on Computational Science & Computational Intelligence Springer Nature - Book Series: Transactions on Computational Science & Computational Intelligence*.

George, J. (2019, March 27). *Fighting Crime with Data: Can 'Predictive Analytics' Prevent Crime Before It Happens?* Retrieved from LinkedIn.com: https://www.linkedin.com/pulse/fighting-crime-data-can-predictive-analytics-prevent-before-george/

Hsiung, C., Chen, F., & Horowitz, A. (2023, September 20). *Exploring AI for Law Enforcement.* Retrieved from Police Chief: https://www.policechiefmagazine.org/exploring-ai-law-enforcement-interview/

Interpol. (2023). *Artificial Intelligence Toolkit*. Retrieved from Interpol: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit

Jacobson, S. (2022, November 07). *TSA faces ethical limits on AI, but advancement work must persist.* Retrieved from Stars and Stripes: https://www.stripes.com/opinion/2022-11-27/tsa-artificial-intelligence-8207585.html

Johnson, A., Egan, E., & Londono, J. (2023, January 09). *Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms.* Retrieved from Information Technology & Innovation Fountation: https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/

McKay, S., Hartnett, G. S., & Held, B. (2022, March 22). *Airline Security Through Artificial Intelligence.* doi:https://doi.org/10.7249/PEA731-1

Nasa, P., Jain, R., & Juneja, D. (2021, July 20). Delphi methodology in healthcare research: How to decide its appropriateness. *Would Journal Of Methodology, 11*(4), 116-129. doi:10.5662/wjm.v11.i4.116

Novak, C. (2023, July 05). *The Role Of AI In Social Engineering.* Retrieved from Forbs.com: https://www.forbes.com/sites/forbestechcouncil/2023/07/05/the-role-of-ai-in-social-engineering/?sh=1baf238a42a9

Pettit, J. (2023, March 01). *Social Engineering: Definition & 6 Attack Types.* Retrieved from Fortra Tripwire Intergity Mangement: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for

Police 1. (2022, March 22). *The biggest technology challenges facing police leaders.* Retrieved from Police1: https://www.police1.com/chiefs-sheriffs/articles/the-biggest-technology-challenges-facing-police-leaders-7QFimpOSEgJZRQyX/

Puckett, J. (2023, March 10). *TSA Is Using Artificial Intelligence to Reduce Unnecessary Pat-Downs.* Retrieved from Conde Nast Traveler: https://www.cntraveler.com/story/new-tsa-scanner-technology-uses-ai-gender-neutral

QSR International. (2018, March 01). *NVivo Feature Comparison*. Retrieved from http://www.qsrinternational.com: http://www.qsrinternational.com/nvivo/nvivo-products/nvivo-product-suite-overview

Raaijmakers, S. (2019, 09 03). Artificial Intelligence for Law Enforcement: Challenges and Opportunities. *Security & Privacy, 17*(5), 74-77. Retrieved from IEEE Explore: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8821442

Ratiu, R. (2023, July 17). *Strengthening Collaboration for Cyber Resilience: The Key to a Secure and Resilient Organization.* Retrieved from ISACA.org: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/strengthening-collaboration-for-cyber-resilience-the-key-to-a-secure-and-resilient-organization

Redden, J., Aagaard, B., & Taniguchi, T. (2020, August). *Artificial Intelligence Applications in Law Enforcement: An Overview of Artificial Intelligence Applications and Considerations for State and Local Law Enforcement.* Retrieved from US Department of Justice Office of Justice Programs: https://www.ojp.gov/ncjrs/virtual-library/abstracts/artificial-intelligence-applications-law-enforcement-overview

Rigano, C. (2018, October 08). *Using Artificial Intelligence to Address Criminal Justice Needs.* Retrieved from National Institute of Justice: https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

Sayegh, E. (2022, May 26). *Social Engineering: Low Tech, High Threat.* Retrieved from Forbes: https://www.forbes.com/sites/emilsayegh/2022/05/26/social-engineering-low-tech-high-threat/?sh=1b1300fe666e

Schiliro, F. (2023, 03 2023). *Building a Resilient Cybersecurity Posture: A Framework for Leveraging Prevent, Detect and Respond Functions and Law Enforcement Collaboration.* Retrieved from Cornell University: https://arxiv.org/abs/2303.10874

Sibley, J. (2023, September 28). *The Intersection of Artificial Intelligence and Social Engineering: Next-Generation Threats.* Retrieved from versprite.com: https://versprite.com/blog/the-intersection-of-artificial-intelligence-and-social-engineering-next-generation-threats/

Stahl, B. C. (2021). *Addressing Ethical Issues in AI.* Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-69978-9_5

Zvelo. (2023, November 08). *The Role of AI in Social Engineering.* Retrieved from zvelo.com: https://zvelo.com/the-role-of-ai-in-social-engineering/

Appendix

The survey for the panel will focus on the following questions related to the use of AI in law enforcement:

1. How can AI be used to increase the safety of body-worn cameras?
2. How can AI be used to de-escalate conflicts and reduce the use of force by police officers?
3. How can AI improve the efficiency of police investigations?
4. How can AI improve the quality of criminal justice data?
5. How can AI be used to support victim-centered policing?
6. How can AI foster trust between law enforcement and the community?
7. How can AI analyze social media data to identify potential suspects or witnesses?
8. How can AI be used to analyze video footage from security cameras to identify suspects or track their movements?
9. How can AI be used to analyze DNA evidence to identify suspects or link multiple crime scenes together?
10. How can AI be used to analyze financial records to identify money laundering or other illicit activity?
11. How can AI be used to analyze phone records to identify suspects or track their contacts?
12. What types of data can the AI system access and process?
13. How accurate is the AI system in making predictions or identifying patterns?
14. How can the AI system be used to generate leads or evidence in a way that is admissible in court?
15. How can law enforcement agencies be held accountable for the use of AI?
16. What mechanisms are in place to ensure that AI is used in a way that is consistent with the law and with ethical principles?
17. What are the consequences for law enforcement agencies that misuse AI?
18. How can law enforcement agencies be more transparent about their use of AI?
19. What information should be made public about how AI is being used in law enforcement?