AIPOL MEMBERS USE ONLY.
Please do not hand this out to members of the public

AiPol

Australasian Institute of Policing

Journal of the Australasian Institute of Po

Volume 17 Number 2 • 2025

ARTIFICIAL INTELLIGENCE

The Paradigm Shift in Law Enforcement

Part I: Overseas Policing

Find us on Facebook

Hedland POOL CARE

Call us to arrange a quote on 0477 307 774

www.hedlandpoolcare.com.au

Hedland pool care is a local business that strives for personal service and quality work.

Main Supplier of Astral/Zodiac Pool Equipment

Cleaning/Balancing, Servicing and Maintenance.
Pool Supplies, Pumps and Parts as well as complete System Installs

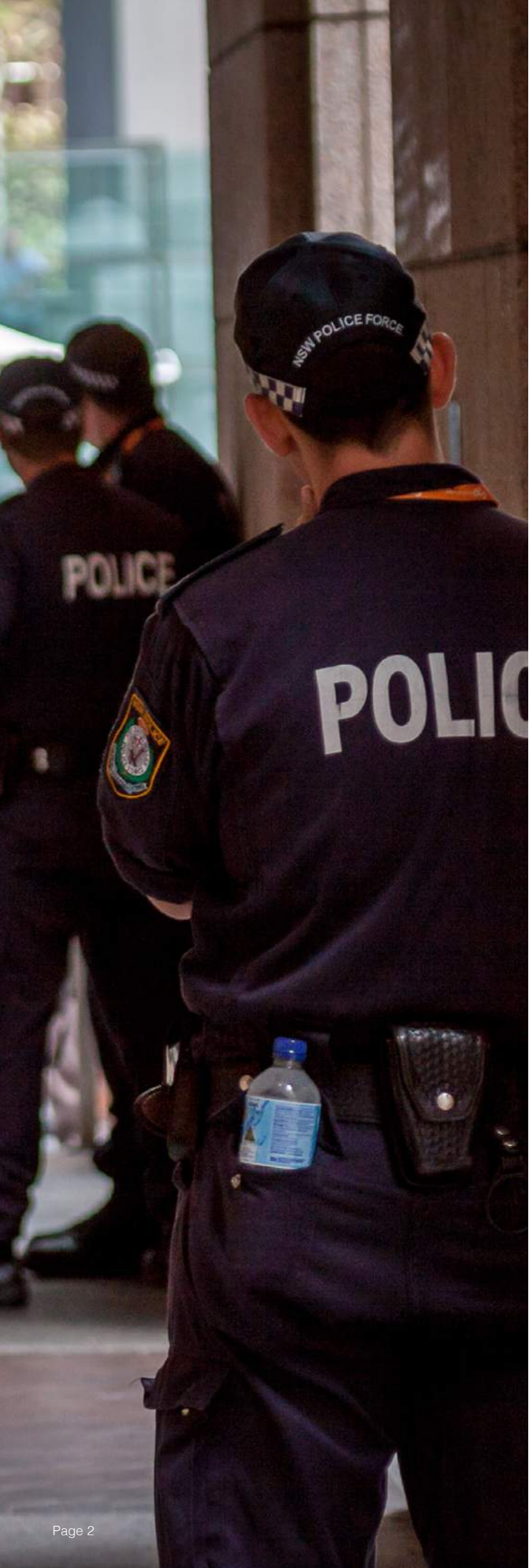
Proudly Supporting Our Local Police Members

AFP

It takes **experienced police** to tackle **complex global crime**

At the AFP you can use your skills to make an impact on crime nationally and internationally. With roles across Australia, career progression opportunities and help relocating, the AFP can take you where you want to be.

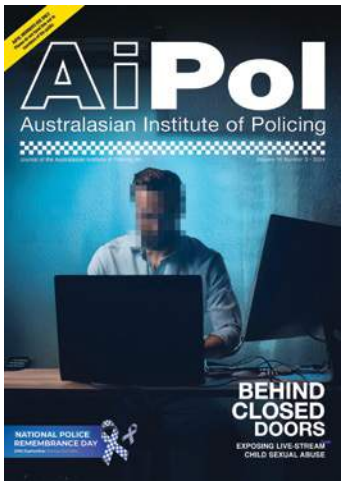
Transfer now through the
AFP Skilled Policing Program
afp.gov.au/skilledpolice

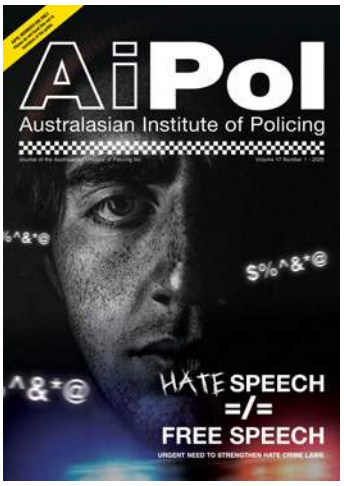


AiPol
Australasian Institute of Policing

Vol. 17, No. 2
June 2025

Published by the Australasian Institute of Policing Inc.
A0050444D ABN: 78 937 405 524
ISSN: 1837-7009





Visit **www.aipol.org** to view previous editions and to subscribe to receive future editions.

Contributions

Articles on issues of professional interest are sought from Australasian police officers and police academics. Articles are to be electronically provided to the Editor, aipoljournal@aipol.org. Articles are to conform to normal academic conventions. Where an article has previously been prepared during the course of employment, whether with a police service or otherwise, the contributor will be responsible for obtaining permission from that employer to submit the article for publication to Australasian Policing.
Contributors are expected to adhere to the Journal's publishing guidelines. These guidelines are available in this Journal. All papers are peer-reviewed.

Disclaimer

While every effort is made to check for accuracy, the Publishers or Editors cannot be held responsible for the content, errors or omissions inadvertently published in articles and advertisements in Australasian Policing. Views expressed by contributors are not necessarily those of AiPol, the Editors or the Publisher. No responsibility for loss occasioned to any person acting, or refraining from acting, as a result of material in this publication can be accepted.

Copyright

All rights reserved. No part of this publication may be reproduced or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or be stored in any retrieval system of any nature, without written permission of the copyright holder and the Publisher, application for which in the first instance should be made to the Publisher for AiPol.

TABLE OF CONTENTS

Editorial	5
President's Foreword	6
Artificial Intelligence as an Innovative Element of Support in Policing	11
AI There, You're Nicked: Tech Is Reshaping How We Fight Crime	18
AI to Free Up Thousands of Police Hours and Cut Court Backlogs	22
Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety	27
New AI Tool to Identify Knives Could 'Transform' Policing of Knife Crime	38
New York City Wants Subway Cameras to Predict 'Trouble' Before It Happens	40
AI Can Help Police Predict if Someone Is at Risk of Domestic Abuse	41
Modesto Police Department Experimenting With AI Gun Detection: How Does It Work?	42
Cyborg 1.0: Thai Robocop Patrols Streets With 360° Eyes, Live Face-Tracking Power	45
Spherical Police Robots	47
Can AI Help Fresno Police Do Their Jobs?	48
Responsible AI in Policing	50
ACLU Opposes AG Yost, Cleveland Police on Use of Facial Recognition in Murder Case	55

ARE THEY TRIPLE OK?

Even the most resilient emergency services workers and volunteers can be affected by stress and trauma related to their work, or as a result of other life challenges. Are They Triple OK? resources provide practical tools and tips on how to start an R U OK? conversation with a workmate, friend or family member in the emergency services, to help them feel connected and supported, long before they're in crisis.

Scan to learn more

ruok.org.au/triple-ok

R U OK?™

A conversation could change a life.

Editorial

DR AMANDA DAVIES

Editor, Senior Researcher at the Charles Sturt University

> ***"Embracing the capabilities of AI is transforming policing and law enforcement globally through technologies that enhance surveillance, crime prevention, resource allocation, and administrative efficiency."***

Welcome to the latest edition of the journal. We are surrounded in our personal and professional lives with the capabilities of Artificial Intelligence (AI) it is here to stay, and it has the capacity to change the way organisations do business, including police and law enforcement. Embracing the capabilities of AI is transforming policing and law enforcement globally through technologies that enhance surveillance, crime prevention, resource allocation, and administrative efficiency. There is however a call to progress cautiously, whilst AI offers substantial benefits, such as improved predictive policing and real-time threat detection, it brings with it the need to consider associated issues such as ethics, transparency, bias, and accountability.

Governments across the world are grappling with the challenges associated with establishing legal parameters for the use of AI and as the capabilities of AI increase exponentially to offer more sophisticated and nuanced tools to aid legitimate organisations there is a flip side. Unfortunately, that flip side is that AI is also assisting the development of sophisticated and ever-increasing illegal activities. As noted in the AiPOL President's Foreword the range of activities that are being witnessed appears limitless and is having catastrophic impact on communities, their safety, financially, physically and emotionally.

In this issue the article *Artificial Intelligence as an Innovative Element of Support in Policing offers* is an insightful discussion that reaches to the core of one of the issues that plagues the efficiencies of police and law enforcement agencies – i.e the demand of the administrative load associated with policing activities. Here the authors present a targeted and thoughtful argument for adopting AI in the form of large language models to assist with administrative tasks enabling organisations to more efficiently and effectively allocate their critical workforce – extending this to the judicial domain there is potential here also to aid and, in some cases, revolutionise the demanding administrative load.

The article *Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety* offers a clear and simple explanation of the manner in which AI has revolutionised the efficient and effective policing of crime through enhancing the accuracy of profiling not only the potential offender/s also the location and crime typology. Similarly, addressing knife crime through engaging AI to rapidly identify the source of weapons has the potential according to researchers at the University of Surrey, to support policing efforts to mitigate the extent of this criminal behaviour in the UK.

Whilst there is a call to be cautious and not place AI on a pedestal as the panacea for all police and law enforcement responsibilities, the world is witnessing the emergence of this technology in all of its forms as a breakthrough in addressing the overwhelming demands of maintaining community safety and security. It will be as we forge into the future with this technology that we will see of how this partnership will impact our lives. The AiPOL journal team looks forward to keeping you informed on this topic.

President's Foreword

JONATHAN HUNT-SHARMAN

President, Committee of management, Australasian Institute of Policing

It's a Brave New World

Policing & AI

From a criminal investigation and national security stance, Artificial Intelligence (AI) is causing havoc for the 'good guys' in law enforcement and national security.

AI generates deepfake videos to defraud you by impersonating someone you know, phishing e-mails to steal your login credentials, malware code to break into your computer and ransomware to lock you out of it until you pay—common tools in a multi-billion-dollar scam industry run by organised crime. In addition, State based actors are using AI to generate deepfake videos and fake social media posts utilising disinformation to interfere with democratic elections, destabilise societal values, causing division, polarisation and violence within stable communities. Policing is on the 'back foot' until it embraces the latest AI innovations for the 'good' of society.

In 1932 Aldous Huxley's dystopian novel *Brave New World*, he used the phrase to highlight the ironic, potentially negative aspects of a seemingly perfect world, where individual freedom and genuine human experience were sacrificed for stability and happiness. *The Brave New World* is a society where technological controls and conditioning creates a seemingly perfect but ultimately dehumanising existence.

In 1949 George Orwell wrote the novel *1984*. It also warned of the dangers of a dystopian world. It centred on the technological advances that enables the State the ability to conduct mass surveillance of people and behaviours within society. Orwell, a staunch believer in democratic socialism, in his novel models a once democratic society's transformation into totalitarianism.

As AI has continued to advance, we have seen science fiction writers and movie directors warning of the dangers of having AI without appropriate constraints, safety nets, and rules. In the science fiction world freedoms are curtailed by the advances of AI. Interestingly, many of the futuristic AI devices in movies such as '*I-Robot*', '*RoboCop*', '*Minority Report*', '*James Bond*', '*Mission Impossible*' and even the 1962 animated sitcom '*The Jetsons*' have gone from fiction to reality in only a few short years. Indeed in some cases we are now seeing AI reality overtaking fiction! So where does that leave Policing? How does policing adapt to this technology whilst not having over reach into our freedoms? How can the 'good guy' use AI for the greater good?

We are seeing AI increasingly being used in policing for data analysis, crime prediction, detection and prevention offering potential benefits like improved efficiency and resource allocation. There are now many international examples of AI in policing and it is growing at an exponential rate.

However, as can be rightly expected, there are concerns about bias, privacy, and accountability. Many of these issues appear to be being addressed 'on the run' when looking at the overseas experience, particularly where there have been successful legal challenges.

AI in Australian policing is somewhat in its infancy. Australian governments and federal, state and territory police agencies are all very conscious of ensuring there is no over-reach using AI. They are conscious of the need for careful consideration and oversight, especially with technologies like facial recognition and predictive policing algorithms.

That being said, there are varying degrees of AI being used in all Australian police jurisdictions. Fortunately there is a great opportunity with limited Police agencies compared to say the USA or Europe, to ensure appropriate accountability and transparency measures are in place to reduce judicial and societal concerns and to ensure national standards are adopted across jurisdictions.

There are many AI benefits for policing already identified internationally, some of which have commenced in Australia, and others that can be adopted in Australia after careful consideration. Some of the benefits of AI already identified are:

- **Data Analysis:**
  AI can analyse crime data, such as voluminous email or sms messaging, company records and computer files to identify evidence and identify criminal associates from materials seized under Search Warrants or other lawful means. It supports the police investigations and the completion of briefs of evidence by reducing the manual workload for investigators so that they can focus their limited resources on non manual tasks.
- **Predictive Policing:**
  AI can analyse crime data to identify patterns and predict where and when crimes might occur, allowing for proactive resource allocation and preventative measures.
- **Enhanced Crime Detection:**
  AI can help identify connections and patterns within large datasets, assisting in the detection of various crimes, including child abuse, financial crimes, and terrorism.
- **Resource Optimisation:**
  AI can help optimise police deployments, ensuring efficient resource allocation and coverage, especially in areas with limited resources.

- **Improved Public Safety:** AI-powered surveillance and robotic security devices can help prevent crimes and reduce the risk to police officers.
- **Accountability and Transparency:** AI can assist in analysing body camera footage, helping to identify potential misconduct and improve accountability of police as well as reducing vexatious complaints against police.

We are fortunate that we can learn from overseas police jurisdictions that have already adapted and utilised AI in areas not yet adopted in Australia. In particular, we can avoid the outcomes where it has led to failed prosecutions or public inquiries.

AI Issues identified overseas include:

- **Bias and Discrimination:** AI algorithms can perpetuate biases present in the data they are trained on, potentially leading to discriminatory outcomes in policing.
- **Privacy Concerns:** The use of AI in policing, particularly facial recognition technology, has raised concerns about data privacy and potential misuse.
- **Accountability and Oversight:** Determining accountability for AI-driven decisions and ensuring proper oversight and transparency in the deployment of these technologies is crucial.
- **Lack of Transparency:** AI algorithms can be opaque, making it difficult to understand how they arrive at their decisions, which can erode public trust.
- **Ethical Considerations:** The use of AI in policing raises ethical questions about the balance between efficiency, public safety, and individual rights.

In our *Brave New World*, AI algorithms are already being used by police to predict crime hotspots and identify potential offenders. AI-powered facial recognition systems are being used to identify suspects and monitor public spaces. AI is being used to analyse body camera footage to identify potential misconduct and improve officer accountability and AI is analysing voluminous documentary, real, and forensic evidence during police investigations and for Court preparation. Now of course, the other great advancements are occurring in robotics Robots are being used for surveillance, hazardous material handling, and other tasks that may put officers at risk.

AiPOL believes that Australian police agencies are taking the correct approach. AiPOL commends the work being done by the Australia New Zealand Policing Advisory Agency (ANZPAA). ANZPAA, on behalf of police agencies in Australia and New Zealand, has been focusing of four (4) key areas:

- **Developing Ethical Frameworks:** Establishing clear ethical guidelines and standards for the use of AI in policing.
- **Ensuring Transparency and Accountability:** Insisting that AI algorithms are more transparent and establishing clear accountability mechanisms for their use.
- **Training and Education:** Developing educational modules for police officers on how to use AI tools responsibly and ethically, and how to interpret the data they generate.
- **Collaboration and Dialogue:** Encouraging open dialogue and collaboration between law enforcement agencies, technology developers, academics and the community to address the ethical and social implications of AI in policing.

AiPOL is closely monitoring the advancements in AI and its adoption by various Australian Police agencies. AiPOL is interested in the work being done to ensure that the Australian public embraces and supports the appropriate use of AI in policing.

In our *Brave New World*, we are fortunate that the independent Office of Constable protects the rights of all Australian citizens. This independence is even more important as we move into the *Brave New World of AI*. All Australians should be comforted that the independent Office of Constable is the bedrock of modern day policing in Australia. Every Constable is an independent legal entity, the public's guarantee of impartiality. Officers of the Crown operate independent of undue influence, interference and with personal responsibility which requires a unique type of person and commitment. This provides our protection against the totalitarian State.

AiPOL will continue to influence decision makers in this important evolution of AI in Policing to ensure that Policing with AI is compatible with the public's expectation of the independent Office of Constable.

afac25

powered by INTERSCHUTZ

26 – 29 AUGUST 2025

PERTH CONVENTION AND EXHIBITION CENTRE

AUSTRALASIA'S PREMIER CONFERENCE AND EXHIBITION

From local to global: leveraging systems, capability and connection

AFAC25 powered by INTERSCHUTZ Conference & Exhibition returns to Western Australia, delivering products, services, and solutions for all emergency management and first responder sectors.

Police Fleet requirements and asset management, PPE, safety and rescue equipment, workforce learning and development, community risk reduction strategies and systems, emerging response operations communication technology, drones, aerial response and so much more.

A world class showcase of international and national brands with best practice solutions for all first responder sectors.

AFAC25

Emergency / Rescue

Public Safety / Defence / Corrections

Critical Infrastructure

Visit **afacconference.com.au**
or scan the QR code to find out more:

#afac25

SPONSORED BY

NRMA INSURANCE | A Help Company

AFAC25 Resilience Lane Partner Sponsor & ADRC25 Industry Partner Sponsor

Natural Hazards Research Australia

Industry Research Partner Sponsor

Australian Institute for Disaster Resilience

AFAC25 Knowledge Centre Sponsor

ISUZU AUSTRALIA

Welcome Function Sponsor

GAAM Emergency Products

Lanyard Sponsor

FOR EMERGENCY MANAGEMENT AND FIRST RESPONDERS

Delivering solutions to these industry groups:

- Fire
- First Responders / Police / Ambulance
- HazMat / Industrial
- Fire Prevention / Built Environment
- Resilience / Recovery
- Mining / Gas & Petroleum

INDUSTRY COLLABORATIVE SECTORS

WORKFORCE — **FIRE SAFETY**

CAPABILITY

Equipment | PPE | Fleet

COMMUNITY RISK REDUCTION — **RESPONSE OPERATIONS**

HOST AGENCIES

Government of Western Australia | DFES Department of Fire & Emergency Services

PARKS AND WILDLIFE SERVICE

DESTINATION PARTNER

Perth Convention and Exhibition Centre Western Australia

Western Australia | Business Events Perth

DELIVERED BY

afac

Deutsche Messe

WE'RE RECRUITING

SECURITY | TECHNOLOGY | MANAGEMENT

SECURECORP.COM.AU/EN/NOW-RECRUITING

SECURECORP

International Conference on Industry Sciences and Computer Science Innovation

Artificial Intelligence as an Innovative Element of Support in Policing

HANA DUBRAVOVA [A*],

JAN CAP [B],

KRISTYNA HOLUBOVA [C],

LUKAS HRIBNAK [D]

Abstract

Currently, the public security sector is faced with an increasing administrative burden that limits the ability of police officers to focus on core security tasks. This paper focuses on the possibility of using large-scale language models (LSMs) as an innovative tool to address this challenge. Based on a careful literature review and analysis of current trends in artificial intelligence, the author team develops a concept for integrating GPTs into police practice, with an emphasis on the potential for reducing administrative burden and supporting efficient processing of relevant information.

As part of this research, we have identified key areas of policing where AI could bring significant value, including data analysis and document production assistance. However, it should be emphasised that this technology is still in its early stages of development and its implementation would require a carefully considered approach involving interdisciplinary collaboration and further research to test the theoretical assumptions presented in this study. Thus, this paper contributes to a deeper understanding of the potential benefits and challenges of integrating GPT into policing practice and outlines a path towards future innovative solutions in the field of public safety.

* Corresponding author.

a Police Academy of the Czech Republic in Prague, Faculty of Security Management, Department of Management and Informatics, 0000-0003-3421-2194, dubravova@polac.cz Czech Republic

b Police Academy of the Czech Republic in Prague, Faculty of Security and Law, Department of Criminalistics, Czech Republic, 0000-0003-1828-362X, cap@polac.

c z Czech Republic

c Police Academy of the Czech Republic in Prague, Faculty of Security Management, Department of Crisis Management, 0000-0001-9430-1880, holubova@polac.cz Czech Republic

d Police of the Czech Republic, Police Presidium, Police Education and Training Unit, 0009-0008-1298-316X, hribnak@polac.cz Czech Republic

Introduction

Artificial intelligence (AI) is a field of computer science that deals with developing computer systems with the ability to perform tasks that would otherwise require human intelligence. This can include tasks such as image recognition, creating new images, natural language recognition and generation, and other tasks. A subset of AI is machine learning, which allows computers to learn and improve their capabilities by processing large amounts of input data. This allows such systems to "self-learn" to perform tasks that would otherwise be difficult or impossible for humans or traditional programming.

Large-scale language models are growing in popularity in natural language processing, especially with the Transformer model based on the "attention" mechanism introduced by Google in 2017. This model can efficiently predict the probabilities of the following words in a text sequence and differs from traditional language models such as RNN or CNN by simultaneously processing the entire input sequence, thanks to the attention mechanism. In recent years, there have been other innovations, such as the combination of bidirectional transformer with masked language model architecture in Google AI Language and generative pre-training in Open AI, which involves a combination of generative and discriminative neural networks and is considered one of the most efficient approaches in modern language models such as GPT-3 and BERT

Current studies and scientific research projects show that artificial intelligence (AI) could significantly impact the labour market in the Czech Republic, increasing unemployment by 30%. The development of AI is also creating new job opportunities that are focused on the development, programming, and implementation of these technologies. It can be concluded that, shortly, companies will be forced to adapt to new technologies and the creation of a supply of new jobs.

In the environment of security forces such as the Czech Police, LLM can help in areas such as processing large amounts of data (processing large-scale analyses and producing summary reports, looking for hidden patterns to understand crime trends better), detecting fraud and fraudulent activities, for example in monitoring financial transactions or identity verification, predicting risk situations such as possible terrorist attacks or predicting dangerous situations in transport, and automating processes (sorting and categorising documents). Opinions on the overall impact of AI on public security vary and go in different directions. On the one hand, using AI in security systems can bring benefits in the form of early risk detection and threat prevention. AI can help detect suspicious behaviour, identify threats, and prevent crimes. On the other hand, AI can negatively impact individuals' privacy and lead to human rights violations. Moreover, if AI is in the hands of criminals or terrorists, it can become a dangerous tool for attacking and threatening public safety.

Elisabeth Joh has addressed the area of the use of AI in policing in her article, where she outlines the use of AI in policing and its benefits. In her article, she mentions the possibility of predicting to identify suspects on the spot or increasing the safety of people against violence.

The AI-based algorithm is simultaneously effective as a means of risk detection, prevention of criminal activities and prediction of illegal activities, and AI is also used in digital forensics.

Thus, the public often has very distorted ideas about the work of police officers, mainly based on the lens of crime and action films. However, the reality of day-to-day policing is quite different. The administrative side of the job is not only far removed from the adventure stories of the silver screen, but its complexity and time-consuming nature can also limit the ability of police officers to focus on their core duties and basic security tasks. The administrative burden and the options to alleviate it are often mentioned in public discussions and occupying a prominent position in the priorities of police management. Let us leave aside the approaches and possible solutions of the past and focus our attention on modern technology, which has recently gained a great deal of attention from experts and the public. This is (to put it simply) artificial intelligence and large language models.

This study combines a detailed analysis of the literature on large-scale language models and practical experience in policing. The author team, whose members are or have been police officers with an average of over 15 years of service, analysed recent studies and articles in the field of AI to gain a deeper insight into the principles of LLM and how they can be used in police practice. Practical experience in policing in different areas brings a unique perspective, allowing suggestions for the integration of LLM into specific work practices, which can ultimately lead to the definition of new trends in police practice.

Using AI as an Innovative Element in Policing

The areas of policing where generative AI could provide effective support are extensive. In those areas where administrative activity dominates over practical tasks, AI could make a significant contribution. Generative pre-trained transformers, especially with new plugin modules, offer extended potential, including code analysis and data imaging. This technology could form the basis for systems to process police-relevant information, analyse data, and assist in creating documents for various policing activities. However, it should be stressed that these possibilities remain at the level of hypothetical scenarios for the time being, and the following section of this paper should therefore be viewed in this light. So far, no contradicted and verified scientific evidence provides data to verify these theoretical assumptions. To use this technology effectively, further steps in developing these systems would need to be taken. These steps should include further research and experimentation that could provide compelling evidence of the utility and effectiveness of GPT to reduce the administrative burden on the police. Interdisciplinary cooperation between experts in law, policing and artificial intelligence would be a prerequisite. The possibilities of using AI in police practice are shown in Table 1.

Writing Support

Within the framework of basic police activities, it is necessary to create primary documents, the content of which is the textual capture of objective facts as inputs for further elaboration of the case under investigation and which are internally structured according to criteria resulting from both legal norms and internal acts of management.

Possibilities of Using AI in Police Practice
Support in the creation of primary documents
GPT-based personal assistant
Use of GPT to support investigations
Use of GPT in analytical processes
Use of GPT in international police cooperation
Use of GPT in criminalistic-technical activities
Using GPT to create communication tools for communicating with the public and receiving criminal reports

Table 1. Use of artificial intelligence in policing.

Figure 1 Possibilities of Using AI in Police Practice.

A typical case includes official records, interrogation reports, inspection reports, and other documents in the case file. The contribution of GPT to creating such texts can be considerable, especially in conjunction with the speech-to-text function. Thus, a recording of an event made by a police patrol on a mobile phone can be used as a primary source of information, which then converts the audio recording into text using speech-to-text recognition technology. The advantage of the outlined procedure may be, among other things, that the audio recording can be made with a minimum time interval from the event in question so that there is no reduction in the quantity and quality of the description due to forgetting.

The next step is to process the converted text using the GPT model, characterised by its ability to understand and develop textual context based on extensive prior training involving many documents of the same type. As a human-supervised learning technique, Finetuning uses pre-labelled data to finetune the model's parameters to fit a specific task better.

The potential benefits of such an approach are significant. Among other things, it means reducing the administrative burden of producing detailed event reports. Using audio recordings as the primary source of data, which could have been taken immediately after the documented event, can also bring a higher level of objectivity and accuracy to the documentation process. This has the potential to improve the efficiency and quality of policing significantly.

GPT-Based Personal Assistant

The GPT-based assistant represents an innovative application of artificial intelligence in policing, using speech recognition and generation technologies. This digital tool offers efficient and flexible information support for police officers. The officer can interact with the assistant through written questions and the spoken word.

The main advantage of a GPT assistant would be the ability to process and retrieve information from a large data set - legal documents and internal sources. This digital tool would have information from various sources, including laws and sub-legislative legal standards, internal management acts, methodological guidelines, manuals and training materials, e.g., criminalistic tactics and techniques, psychology, and other applied scientific disciplines. Thanks to this complexity of data, the GPT Assistant could provide up-to-date and accurate information that could substantially contribute to the efficiency and quality of police activities.

With cloud technologies, this system would be accessible from various devices, whether desktops in the office or mobile devices in the field. This feature would allow officers to access relevant information quickly and efficiently, even at the crime scene or on patrol.

The advantage of such an assistant is the ability to provide specific legal advice and information in real-time, which is particularly useful in fast-paced situations during police duty. A GPT assistant can also adapt to individual needs based on the duty assignment and communication style of a particular police officer. It can gradually improve its ability to understand and respond effectively to the officer's queries thanks to training data and machine learning algorithms.

A personal assistant capable of analysing data from closed cases can identify key patterns, effective strategies and tactics that led to their successful resolution. These insights can generate personalised outcomes tailored to the officer's assignment and specific needs. Personalised outputs may include various learning materials such as case studies of similar successful cases, suggestions for effective strategies and tactics for specific situations, or information on new practices and technologies that can help increase the officer's proficiency and performance. The assistant can thus serve as an essential tool for continuous personalised further training of police officers and potentially contribute to the adaptability of police officers to new challenges, taking into account their service and personality profile.

Use of GPT to Support Investigations

Within the potential use of GPT technology in supporting police investigations is the ability of this model to learn from structured data, specifically investigative files and the documents contained therein, how the documents are structured internally, what logical operations are used in their creation and organisation, what the legal justifications are for investigative actions, and under what specific circumstances these actions are performed. This ability to extract and apply relevant patterns and structures from large datasets is one of the key advantages of GPT technology.

GPT is then able to use its ability to analyse large amounts of data from a particular investigation file and generate text based on the input requirements. In this way, the GPT can compile the datasets from the investigation file into output text in the required form, including the relevant legal justification. It is important to emphasise that the police officer makes all decisions in this process, which is his/her responsibility. The GPT, in this context, only serves as a tool to facilitate and streamline the investigation process but does not take over the decision-making power of the police officer.

During an investigation, GPT does not have to be used in the actual creation of documents. Utilising its capabilities can also be valuable to the investigator when navigating through a large file. Thus, an investigator can formulate questions about portions of an investigative file, and the GPT can provide an analytical and synthetic output based on those instructions. For example, the GPT can use the information contained in testimony, official records, forensic analyses, and other documents to create a chronological overview of events relevant to the case that could help the investigator better understand the course and context of the events that form the core of the case under investigation.

Furthermore, GPT could be a tool for detecting patterns and connections between different information in a file. Given its ability to analyse large amounts of data and identify potentially relevant relationships between them, GPT could, for example, identify consistent elements in the testimony of different witnesses or matches between forensic findings and information in other documents.

Finally, GPT could create structured summaries of key information in the case file and investigation plans. These summaries could include, for example, a list of key people, important events and locations, relevant legal issues and other relevant aspects to the case. These summaries could help the investigator to keep track of the main aspects of the case and also help him to identify the paths that the investigation should take.

A key factor in the success of this approach is the quality and relevance of the data on which the model is trained. The training data must be free of biases and relevant to the specific context in which the model will be used. Equally important is the human involvement in the finetuning process to ensure that the results generated by the GPT match the needs and requirements of the police. The Cloud Security Alliance (CSA) and Securing Smart Cities have published a report that a program will be developed to introduce secure drones in Smart Cities while emphasising in the program statement that drones will play an essential role in Smart Cities.

Use of GPT in Analytical Processes

With its natural language understanding and big data analysis capabilities, GPT is a potentially revolutionary tool for analytics in a police environment. Its advantages include its ability to process and analyse a wide range of data -from bank statements to financial statements to electronic communication records. As part of this process, it can identify key information, patterns and connections that may be crucial to elucidate cases under investigation.

In addition, plugins such as Code Interpreter can further extend the capabilities of GPT, enabling advanced data analysis and visualisation. This tool allows the application of statistical methods, using libraries and functions available in different programming languages to calculate statistical indicators, regression analysis, data clustering, or predictive modelling. In this way, patterns, trends or anomalies can be detected and categorise the

data in the desired way during the analytical processes.

A new approach to designing a Conversational Agent (CA) artificial intelligence system for intelligence analysis has been introduced in a prototype Conversational Agent CA based on the principles of situation recognition and the use of interactive visual analysis in the work of analysts.

Using GPT in analytical activities can thus increase the efficiency and speed of investigations. Since GPT can understand instructions in natural language, it can greatly reduce the time and expertise required for data entry and manipulation. It can also reduce errors that can occur when manually processing data. In addition, GPT can produce complex outputs, including summary analytical reports, graphs, charts, and tables, which can facilitate the interpretation and sharing of results.

Use of GPT in International Police Cooperation

International police cooperation is a key part of the modern security environment, which is increasingly globalised and interconnected. GPT technology has particular potential in this context due to its linguistic and contextual understanding capabilities.

The most common form of international police cooperation is the exchange of information between the police authorities of different countries based on a request, which must include a description of the case and requirements for specific outputs, whether it is information from national police databases or information obtained through further investigations by the executive departments. GPT can help automate and streamline the processes involved in this information exchange. For example, GPT can be used to analyse documents in different languages, extract key case information and requests and then generate the text of responses using information from national databases, or even generate the skeleton of a national request for further investigation by locally and substantively competent executive police departments. Such use of GPT can significantly speed up the process of responding to international requests and increase their accuracy and completeness.

The GPT's ability to understand and use many languages is essential for its application in international police cooperation. GPT can be trained in a specific language and then used without restriction in combination with other trained languages. This means that GPT can be used to analyse documents in one language and generate outputs in another language, which can be extremely useful in the context of international cooperation and the ability to overcome language barriers in this way. In addition, GPT can also be used to translate the text, typically, for example, of sent interrogation reports or other investigations and actions carried out.

GPT can also be used to analyse collections of information to identify those that may be relevant to foreign police authorities and that can be provided to foreign authorities without their request. Again GPT technology would be used to generate such outputs.

Use of GPT in Criminalistic-Technical Activities

Applying various scientific and technical methods and procedures is an important element of criminalistic-technical investigation. This includes observation, description, measurement, comparison, experimentation, and application of mathematical and physical methods, as well as more sophisticated physical, chemical and biological techniques. Such methods enable forensic technicians and experts to obtain detailed information on the behaviour of the various elements of material systems and thus to obtain sources of evidence, provided that the provisions of the Criminal Procedure Code have been complied with in the process.

GPT offers some potential advantages to improve and speed up these forensic procedures. With additional tools such as Zapier and Wolfram Alpha, which have a large database of knowledge from many scientific disciplines such as physics, chemistry, mathematics and others, GPT can effectively process and analyse the data obtained from these scientific procedures.

Based on four years of intensive collaboration with criminologists, we present the conceptual design of a visual tool supporting the investigation workflow and Visilant, a web-based tool for exploring and analysing criminal data. In particular, Visilant aims to support the exploratory part of the investigation process, from case overview, through research and hypothesis generation, to case presentation. Visilant tracks the reasoning process and how the data changes, informing the investigator which hypotheses are affected by the changing data and should be revised.

This could include GPT to perform automated calculations and analyses in forensic ballistics, chemistry, electrical engineering, metallography and digital forensics disciplines. GPT could also assist in producing detailed reports on the results of these investigations, saving time and reducing the administrative burden associated with these processes.

Using GPT to Create Communication Tools for Communicating with the Public and Receiving Criminal Reports

Communicating with the public is a key aspect of policing in a modern democratic society, but it can be time-consuming. However, implementing GPT technology can significantly reduce this burden while improving the quality of service provided. It is also essential to consider that such a system could promote transparency and trust in public institutions - by creating a platform capable of providing informed answers to citizens' questions, the police could demonstrate their commitment to openness and accountability. This could help build trust between citizens and the police.

GPT can be used to create a communication interface for interaction with the public. This interface would be trained on legal and sub-legal norms, internal management acts and methodological materials for police activities. As a result, it could provide informed answers to a wide range of questions a citizen might ask. This would not only save time and reduce the administrative burden on police personnel but also increase the availability of information to the public and improve communication between citizens and the police.

A GPT-based chatbot could also be an effective tool for receiving notifications from citizens. Through training, it could gain the necessary knowledge of the methodology of receiving notifications. It could consider other criminal procedures, allowing it to collect information from the notifier in an interactive form, where the resulting notification would contain with high

"Police commanders are addressing the challenges associated with the integration of AI. In this context, for example, the Police Education and Training Unit of the Police of the Czech Republic has already launched initial steps to create an infrastructure to enable future research and development in this area."

confidence all the information and supporting documents necessary for further investigation.

The interaction between the chatbot and the notifier can be tuned to a friendly and matter-of-fact tone, making the operation intuitive and efficient. In addition, the chatbot could allow notifiers to add electronic files to the notification. An essential functionality of the system would then be the need for an electronic signature of the notification so that appropriate action can be initiated to verify it. This feature could greatly facilitate the process of filing a notification and thus simplify the citizen's access to justice.

Conclusion

GPT Technology, with its text analysis and generation capabilities, has the potential to become a valuable tool for policing in all its aspects, from administrative support in document production to investigating complex cases. When properly used and combined with human judgement and experience, this technology can significantly enhance the efficiency, accuracy and quality of police work.

When using AI in a policing environment, it is essential always to consider ethical, legal and security considerations. Accountability principles such as transparency, responsibility, trustworthiness and privacy should be respected at all points and in all circumstances. The European Parliament and the Council of the EU are keen to highlight potential problems and stress the importance of protecting fundamental rights, transparency and impact assessment in using artificial intelligence in criminal law. The primary legislation will be an EU regulation, the so-called "AI Act ". As a possible solution for security issues, it is proposed that the security corps should create its hardware infrastructure, separate from the Internet environment, on which large language models can be developed, trained and operated while meeting security requirements.

However, it is important to stress that although the GPT can be a handy tool for police investigators, it should always be used with the possibility of erroneous outputs in mind. Therefore, police officers must not rely solely on the outputs of the GPT but should consider it as a supplementary resource to help inform and support their professional judgements and decisions. Ultimately, decision-making and analysis of the case under investigation should remain in the hands of qualified investigators with the experience, intuition, and deep knowledge base necessary to handle complex criminal cases.

If we allow ourselves to let our imaginations run wild, we could compare the importance and benefits of GPT in police administration with the exoskeleton for soldiers or testosterone for bodybuilders. The exoskeleton is a technological device that allows soldiers to achieve physical feats that would not be possible without its assistance. It increases their strength, endurance and provides protection. Analogous to this, the GPT can provide police officers with a tool that expands their capabilities. It allows them to analyse large amounts of information that would be difficult for an individual to process and generate synthetic outputs that can support decision-making and document production.

At the current stage of the research, it has not been possible to carry out a comparative analysis due to the circumstances described in the 'Limitations' section, including the lack of empirical data and practical research at this stage. A comparative analysis, including an assessment of the strengths and weaknesses of the current approach compared to alternative methods, would increase the chances of achieving optimal results. In the future, it could provide valuable insights to help effectively design the implementation of large-scale language models (LLMs) in policing. The authors' collective assumption here is that LLMs can lead to a significant increase in work productivity and thus facilitate and streamline the activities of the security forces as well.

The use of LLM in a wide range of policing activities could be beneficial in increasing efficiency, reducing staffing and financial costs, and raising the standard of all policing activities. Police commanders are addressing the challenges associated with the integration of AI. In this context, for example, the Police Education and Training Unit of the Police of the Czech Republic has already launched initial steps to create an infrastructure to enable future research and development in this area.

These processes offer great opportunities for international cooperation. This initiative will increase the speed of integrating technologies to create unified standards and methodologies reflecting international trends and innovations.

The authors identified several key limitations in the study. The first and most important limitation is the absence of empirical data, as this paper primarily formulates possible directions for the use of large language models (LLMs) in police practice, and practical research and development in this area has not yet taken place. Further, subjective interpretations of experiences gained in policing may enter the analysis, which is a potential limitation in the context of scientific rigor.

Given the sensitivity and importance of protecting police data, which may be explicitly subject to confidentiality, it is likely that future research projects will need to move towards the development and implementation of locally operated LLMs outside the Internet environment. This approach would not only ensure maximum cyber security but would also provide a strong guarantee of the protection of the data itself, which is essential for maintaining trust towards the security forces, as well as the protection of the specific methodologies used by these forces in their activities.

1877-0509 © 2024 The Authors. Published by ELSEVIER B.V

This is an open access article under the CC BYAuthors. Published by ELSEVIER B.V.-NC-ND license (**https://creativecommons.org/licenses/by-nc-nd/4.0**)

Peer-review under responsibility of the scientific committee of the iSCSi – International Conference on Industry Sciences and Computer Science Innovation

*** Corresponding author.**
E-mail address: dubravova@polac.cz

AI There, You're Nicked!

Tech Is Reshaping How We Fight Crime

January 24, 2025

RACHEL SYLVESTER

Chairwoman of The Times Crime and Justice Commission

When Trevor Rodenhurst, the chief constable of Bedfordshire, visited his counterparts in Germany he saw first hand the power of artificial intelligence (AI) to solve some of the most heinous crimes.

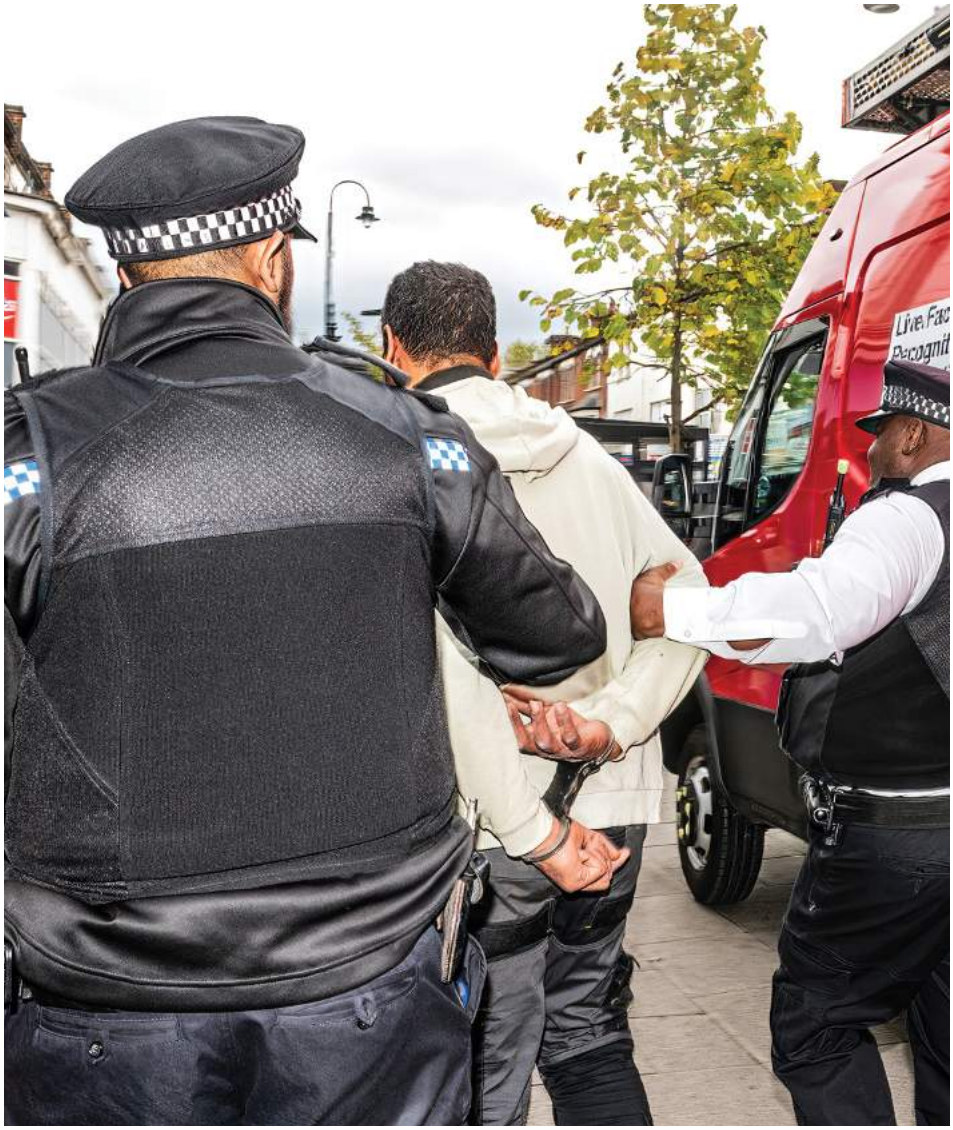
The police there had just rescued a missing child after the young person's mobile phone was flagged by the technology as being next to a known sex offender's device. Now Rodenhurst has introduced the same software into his own force, making Bedfordshire the first county in Britain to be policed by AI. Crimes are already being averted and solved. In the first eight days of the tool being deployed for child protection, the force identified an additional 123 young people who were potentially at risk of abuse or exploitation. There was a 67 per cent cut in the time taken to complete each safeguarding referral and the processing of telephone call data fell from 48 hours to three. The system, developed by the American data analytics firm Palantir, simultaneously extracts information from dozens of sources and creates an operational dashboard with Top Trumps-style profiles of suspects.

Previously, investigators would have to search over 80 different databases looking for clues. Now, at the click of a mouse, they can see a summary of data from thousands of WhatsApp messages, documents and 999 calls. The AI compares phone records, locations, number plates and identities to draw links and build a chart of criminal associates — the modern-day equivalent of the white board with mug shots and pieces of string. In a fast-moving investigation, specialist officers can be automatically allocated tasks, ensuring that relevant people are in the right place at the right time. Detectives receive phone alerts when there is a development in the case.

The software, similar to the platform being used to join up data in the NHS, is saving about 35 per cent of officer and staff time in each advanced operation. Some jobs that would take hours can be finished in seconds. Time spent completing subject profiles has been cut by 80 per cent, and by 75 per cent for building out association charts.

"Needle in a haystack" connections that could never have been spotted by human detectives are being made by the AI. "The results are incredible," says Rodenhurst, who is also the national police lead on serious and organised crime. "If this was in every region, overnight you would join up policing for serious and organised crime, and I think that would be very powerful." When people ask him how he can afford to spend money on technology when resources are tight, he replies: "I can't afford not to."

AI has already transformed the way the private sector operates and it has the potential to revolutionise public services too. This week Peter Kyle, the technology secretary, announced plans for digital passports and driving licences, part of a Whitehall shake-up that aims to use AI tools to save £45 billion by slashing bureaucracy. Keir Starmer describes AI



Nearly 600 suspects were arrested in London last year thanks to the use of live facial recognition software.

as the "defining opportunity" of the age and is promising to turn the UK into an "AI superpower". Donald Trump this week announced a $500 billion "Stargate" project to build AI infrastructure in the US.

Already the NHS is using AI scanners that can cut the time it takes to detect cancer from seven days to seven seconds. Schools have software that tailors lesson plans for teachers and personalises tutorials for pupils. The prime minister suggested AI could soon speed up planning applications and even help spot potholes. It is on policing and national security, however, that the stakes are highest. Criminals are the fastest adopters of technology and the authorities must evolve to keep up. The potential for improving public safety is huge but there are also privacy concerns and warnings of a "surveillance state".

Last year I spent a day with the Metropolitan Police's live facial recognition (LFR) team. A van, parked in a busy shopping street, was fitted with six cameras which scanned the faces of everyone walking past and compared them to images on a watch list of 16,000 faces, a mixture of suspects wanted by the police, registered sex offenders and missing people. I saw an alleged stalker being handcuffed and taken into custody.

Last year nearly 600 suspects were arrested during LFR deployments in London, including 55 for rapes and other violent offences against women and another 58 registered sex offenders who had breached their court conditions. Sir Mark Rowley, the Met commissioner, describes the technology as one of the biggest breakthroughs in fighting crime since fingerprinting. "It is extraordinary, its ability," he told The Times Crime and Justice Commission. "It is accurate, fair and it's not intrusive."

Liberty, the human rights organisation, warns of a "regulatory Wild West" in which tools are being deployed without sufficient debate or proper oversight. Akiko Hart, director of Liberty, says: "We have analogue laws for a digital age with a huge amount of risks and challenges that brings." The public, though, is broadly onside.

A YouGov poll found that 57 per cent of adults backed the police using live facial recognition technology in public spaces compared with 28 per cent who opposed it. As people get increasingly used to sharing their data with both public and private sector, there is also growing support for a universal digital ID. According to a More In Common survey, 53 per cent of the public were in favour and 19 per cent against the idea.

The ethical dilemmas cannot be ignored but nor can the perils of failing to adapt. Dame Lynne Owens, deputy commissioner of the Met, says most people would be "horrified" if they understood how fragmented and incomplete police computer systems are. "If you have a prolific offender who targets women and young girls, who lives in Durham and is worried Durham police are on to him, and decides to move to Devon and Cornwall, it is a bit too much luck of the draw whether Devon and Cornwall will know he has moved to them," she says.

There are 43 police forces in England and Wales, each with multiple disconnected databases. The police national computer is 50 years old and woefully inadequate. The so-called "common platform" for the criminal courts has been beset by technical difficulties, with cases suddenly dropping off the system and hearings starting late because judges or barristers cannot log on. The impact on productivity is staggering, but dysfunctional IT is also disastrous for public safety.

New AI tools can build the links and help investigators trawl through otherwise inaccessible mountains of data. In West Mercia the police are trialling a system called Dragon Slayer, which uses AI to sift through huge downloads of material and highlight conversations that indicate paedophile grooming behaviour. Avon and Somerset police are testing an AI tool known as Söze, named after the criminal mastermind Keyser Söze in the Kevin Spacey film The Usual Suspects, which officers say can do 81 years of detective work in 30 hours, analysing megabytes of data including video footage, financial transactions, social media posts and emails simultaneously.

According to Paul Taylor, the national police chief scientific adviser, the next step could be on-the-spot DNA analysis, allowing officers to use a Covid-style swab and equipment similar to an espresso machine to identify potential suspects without having to send samples to a forensics lab. “Technology is democratising our ability to do specialist tasks,” he says.

There are potential applications for prisons too. Shabana Mahmood, the justice secretary, is looking at how AI could be used to tackle violence in overcrowded jails by monitoring and predicting prisoners’ behaviour. She is also considering whether new technology could be deployed to create virtual prisons, with more criminals punished in the community under house arrest.

Solving millions of policing hours

The potential efficiency gains from automation are huge. Several forces have introduced an AI tool to redact personal data in documents before they are sent to the Crown Prosecution Service. The College of Policing estimates this software would save about 7.5 million policing hours a year, equivalent to more than 4,000 full-time officers, if it were adopted nationwide.

Technology can also allow the police to communicate better with victims. In Kent, the constabulary created a rapid video response for domestic violence. Instead of taking almost 33 hours on average to respond in person to a non-urgent call, an officer could speak to the victim within minutes using a secure link. The pilot saw a 50 per cent increase in arrests and an 11 per cent increase in victim satisfaction.

The Norfolk force has introduced a similar system and is also now piloting an AI tool that transcribes the victim statement, suggests questions to the officer, then fills in the forms needed to create a case file. It has doubled the number of cases the 12-strong domestic abuse team is able to deal with every day.

It is a long way from *Dixon of Dock Green* but Alex Murray, director of threat leadership at the National Crime Agency (NCA) and the National Police Chiefs’ Council lead for AI, says embracing technology is “not only desirable, it’s necessary”. As he puts it: “If we decide to slow down here we will lose the battle against crime and serious organised crime. The opportunities are huge but to a certain extent we’re just catching up.”

Policing in the 21st century is a long way from that seen in the BBC drama Dixon of Dock Green.

For decades politicians have been obsessed with “bobbies on the beat” but the threat is increasingly online. According to the NCA, fraud and cybercrime make up over half of all crime experienced by individuals in England and Wales. Last year there were over 2.75 million adult victims. Companies and public services are also increasingly at risk. Global ransomware payments reached $1.1 billion in 2023, with the true cost to society estimated at over $100 billion. The NHS, the British Library and Transport for London have all been targeted by hackers.

Although parents worry about their children playing outside, the likeliest danger to them is on the computer in their bedroom. There were 10,000 arrests for crimes involving online child sexual exploitation in the UK last year, double the number five years previously. James Babbage, director-general for threats at the NCA, says: “The single greatest area that is causing serious organised crime to grow is not actually about anything that criminals are doing, it’s about us, it’s about the fact that regularly and routinely in our day-to-day lives we’re increasingly dependent on online services.”

It is AI, with deepfake technology, that is revolutionising crime, allowing fraudsters and terrorists to operate at scale, across continents, while personalising content for each victim. One romance scammer tricked women into handing over thousands of pounds by creating a Tinder identity called Mike Murdy, a handsome US army colonel looking for love, whose videos, image and voice were created entirely by AI.

There are algorithms that can “nudify” family photos for the benefit of paedophiles. Reports of child sexual extortion, in which young people are encouraged to exchange intimate images then blackmailed, have rocketed eightfold in a year, according to the Internet Watch Foundation. A sinister marketplace has evolved on the dark web where computer specialists hire out their services to create a fake website or a piece of ransomware.

Shane Johnson, professor of future crimes at University College London, says “crime just follows opportunity”. He identifies “data poisoning attacks”, which seek to distort AI systems by tainting the data on which they are trained, as a possible future threat. Our growing reliance on smartphones at home and computers in cars creates other

Technology must be considered an invaluable tool in the fight against crime.

vulnerabilities. "The technology is moving much faster than our understanding of it and how to legislate," Johnson says.

Jonathan Hall KC, the government's independent reviewer of terrorism legislation, has highlighted the risk of "chatbot radicalisation". It was far too easy for Axel Rudakubana, the Southport killer, to find extremist material.

Estonia's integrated digital model

In Estonia, technology is so integral to the criminal justice system that the government department which oversees it is called the Ministry of Justice and Digital Affairs. All citizens have a digital ID to access public services and verify who they are to banks or shops. The unique electronic identifier, available as an app or a physical card, is seen as an eligibility tool rather than a civil liberties intrusion, allowing people to book doctors' appointments and claim benefits. Since its introduction over 20 years ago, it has improved the efficiency of the state and driven down fraud.

At Tallinn Prison, inmates have tablets which they can use to follow their case, speak to family members, take educational courses or order groceries, logging on to a secure "e-Justice" portal with facial recognition technology. As offenders near the end of their sentence they go out to work, tracked by a mobile phone that monitors their movements and ensures they stick to approved routes.

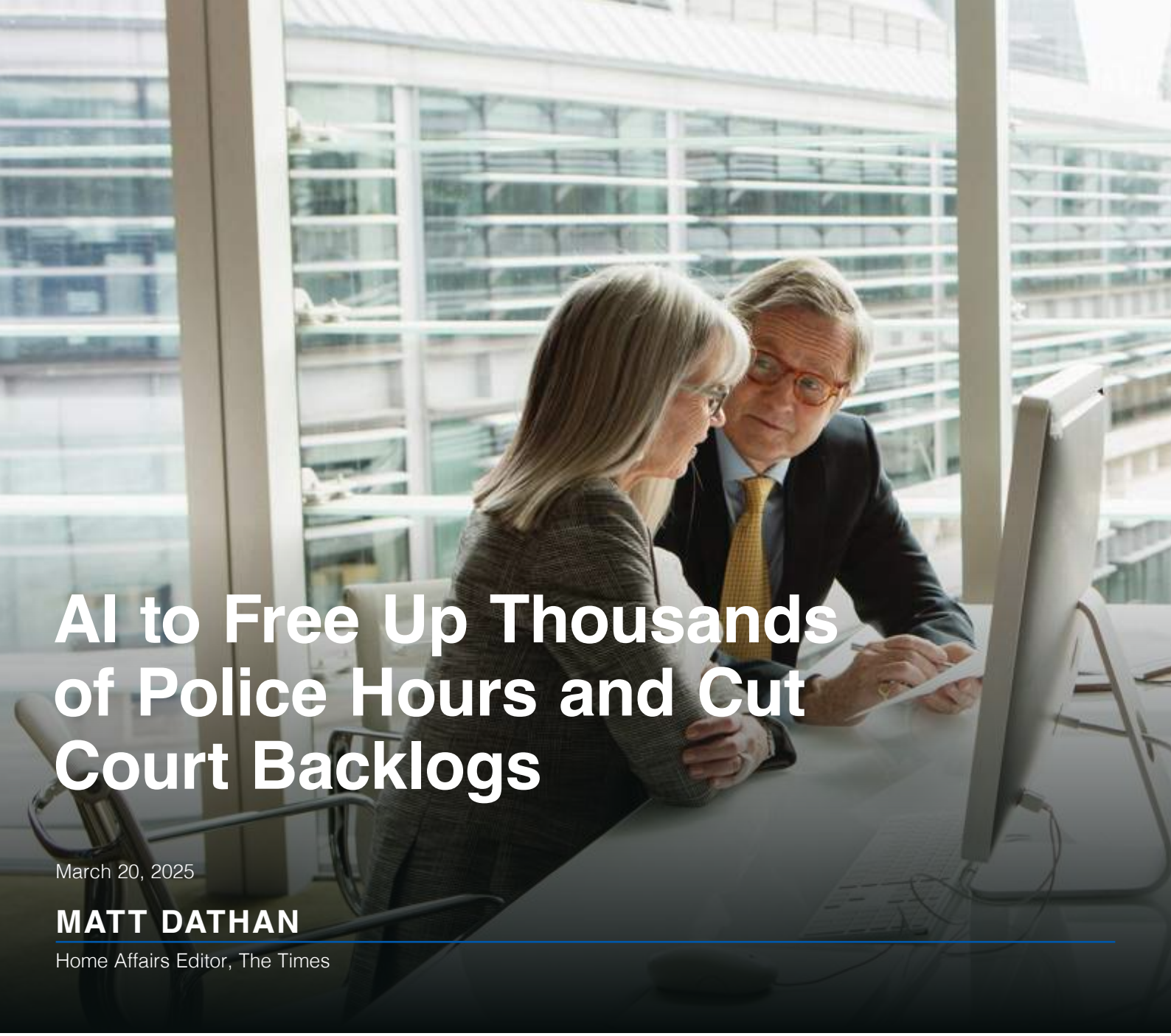
When a crime is reported, a single digital case file is created to ensure that police, prosecutors, courts, forensics teams and defence lawyers all have the same information. Estonia is piloting virtual autopsies, using CT and MRI scans to work out the cause of death without having to cut open a body, which is cheaper, quicker and less distressing for families. By the end of next year the court system will be entirely digitised. Liisa-Ly Pakosta, the minister of justice and digital affairs, says online services are "more secure" than paper-based bureaucracies because "every movement is checkable, everyone can see who has looked at your data".

Technology is, she told the Times commission, an invaluable tool in the fight against crime. "You have another Sherlock Holmes at the table but a digital one. We see innovation as an opportunity for the economy but also for the public sector to do better."

The public must, of course, be reassured that the systems are not biased and that their data will be strictly guarded, but those we expect to protect us cannot allow themselves to be outflanked by those who seek to do us harm. Baroness Manningham-Buller, the former director-general of MI5, says that a kind of "arms race" is under way. "Criminals are there and the state has got to keep up with them, but operating to a different standard to the criminals."

The only way to square the circle of rising demand and stretched public finances is through technology. Data analytics and artificial intelligence make it possible both to drive efficiency and personalise provision in a way unthinkable a decade ago. And in terms of law enforcement, there are profound risks to not modernising.

As Lord Burnett of Maldon, the former lord chief justice, puts it: "If we don't begin to grasp this type of technology and the advantages it can offer, the danger is that we will just be left behind. To put it bluntly, you'll have the whole criminal justice system riding around on penny farthings while all the criminal and international terrorist classes are driving around in fast Jaguars."



AI to Free Up Thousands of Police Hours and Cut Court Backlogs

March 20, 2025

MATT DATHAN
Home Affairs Editor, The Times

The Fisher report said that police and prosecutors should be allowed to use AI to help resolve the disclosure logjam.

The volume of digital material that must be disclosed to the defence wastes time and clogs the justice system, but technology could solve the problem it helped create.

Artificial intelligence and cuts to red tape will free up hundreds of thousands of hours wasted by police and prosecutors on their legal duty to disclose evidence to the defence.

Ministers are expected to accept the sweeping recommendations of a review that has warned that some fraud cases require so much paperwork that, were it printed, the sheets would stack higher than the Shard in London, the tallest building in Western Europe.

The overhaul will prevent police and the Crown Prosecution Service having to present all digital evidence to the defence in an attempt to cut court backlogs and prevent the collapse of thousands of criminal cases. Ministers will also overhaul data protection laws to save police officers redacting personal material from case files before passing them to prosecutors.

A review by Jonathan Fisher KC found that the law, introduced in 1996, requiring the disclosure of all material that might reasonably be considered capable of undermining the case, is unfit for the modern day because it is swamping police and prosecutors to such an extent that it is jeopardising the proper functioning of the justice system.

Fisher’s report highlighted particular problems created by disclosure requirements in prosecutions for rape, serious organised crime and fraud. It found that a quarter of the Serious Fraud Office’s (SFO) operational budget in 2023 was spent on its disclosure obligations. The largest SFO casefile contained 48 million documents.

Fisher said in his report, extracts of which have been seen by The Times: “If printed, the volume of material in an average SFO case would stack considerably higher than the Shard.”

He said that police and prosecutors should be allowed to use AI to help resolve the disclosure logjam. He said: “We should not be afraid to fight fire with fire.

“The same technology that supercharged the proliferation of digital material may well provide, at least in part, a panacea for the difficulties we presently find ourselves in.

“If the current disclosure regime is not adapted to meet the rising tide of digital material, the ability of the Crown to investigate and prosecute criminal cases will be severely hindered.”

To save more time, Fisher has called for changes in the way evidence files are compiled before a charging decision is made, or in cases where a guilty plea is expected, as well as moving away from “the archaic expectation that an officer must write a detailed description for each and every item of relevant material in a case”.

Government sources said that Fisher’s recommendations will be accepted in full by Yvette Cooper, the home secretary, Shabana Mahmood, the justice secretary, and Lord Hermer, the attorney-general.

Fisher also found that the requirement to disclose evidence to the defence also played a major role in why cases fail. In the final quarter of 2023 disclosure issues were responsible for the collapse of 4,000 cases, which account for a quarter of all cases.

The disclosure burden was also wasting hours of police time for cases that do not manage to reach the CPS. The report calculated that this was equivalent to 306 full-time officers spending “all of their working hours during 2023 building case files, scheduling and redacting material, for cases that ultimately terminated with the CPS”.

It also said that 210,000 hours were spent on redacting material for cases that did not progress beyond the CPS. The review suggested that this time could have instead been used to attend 130,000 burglaries or 100,000 domestic abuse incidents.

R U OK?™

A conversation could change a life.

The R U OK? Are They Triple OK? Podcast

Building connection and comradery

R U OK? has launched a new podcast series to encourage life changing conversations, early intervention and supportive behaviour amongst the peers, family and friends of those who work and volunteer in the police and emergency services.

The '**Are They Triple OK**? podcast' features personal stories and practical tools to increase social support for emergency services personnel and build a mentally healthy workplace. It also includes tips on how to ask, 'are you OK?' and navigate a conversation if someone is not OK.

Episode one features James Maskey, a retired front-line Queensland Police Officer. In 2013, James was diagnosed with Post Traumatic Stress Disorder.

"As first responders historically, we talk about everything except for mental health and, importantly, suicidal thoughts," said Mr Maskey. *"Either because we didn't have the confidence to have that conversation, or we were worried about the impacts of having that chat. And when I say we, I'm talking about me. Certainly, that was my experience."*

Mr Maskey says frontline first responders, in the fire truck, in the ambulance, in the patrol car, have a unique opportunity to get to know their colleagues.

"You know what they like to eat, their coffee order and what their family and their children are up to," he said. "You know the intimate details of their lives because you've got a long time in the car sitting side by side to share so many experiences."

Mr Maskey is now the National Sector Specialist at Fortem Australia, and is passionate about enhancing the mental, physical and social well-being of the first responder community.

"My advice to the emergency services community is to learn how to have an R U OK? Conversation and start having them," he said. "If someone is struggling, reaching out for help can feel like a heavy thing to do, it can be a hard task and it can feel overwhelming. "But when you take the time to ask someone how they're travelling, you can take some of the weight off and some of the burden away. People are often relieved to have a conversation and feel that level of camaraderie."

The '**Are They Triple OK**? podcast' is hosted by Matt Newlands, R U OK? Community Ambassador and former police office and is one of a suite of free resources available from

R U OK? for those who work in the police and emergency services, their families and friends. The podcast and resources including a conversation guide and personal stories that demonstrate the life changing impact of an R U OK? conversation can be found at **ruok.org.au**. The '**Are They Triple OK**? podcast' will also be available for download on a range of streaming services, including Apple Podcasts, Spotify, Google Play and Audible.

'**Are They Triple OK**?' was developed in response to the Beyond Blue nationwide 'Answering the call' survey which found more than half of all police and emergency services employees indicated they had experienced

Scan to learn more

ruok.org.au/triple-ok

a traumatic event that had deeply affected them during the course of their work. Positively, personnel with higher levels of social support and resilience reported lower levels of suicidal thoughts and behaviours.

"The results from 'Answering the Call' showed us that the support of peers, family and friends does make a difference for those who work in frontline services. It's OK to not be OK. It's OK to lean on each other, and it's OK to retire that unhelpful stereotype of being that six-foot bulletproof superhero," said Maskey.

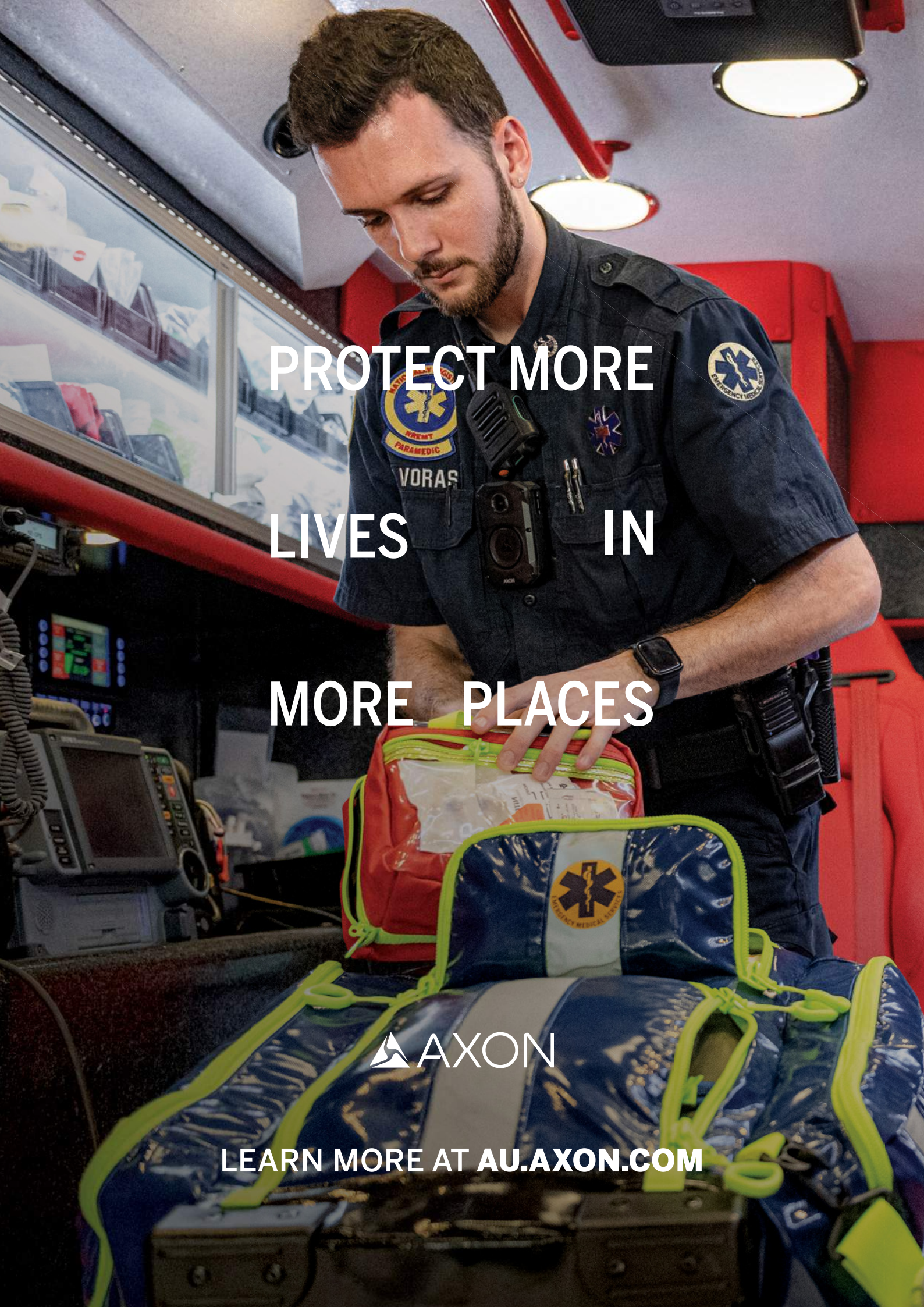
"I would urge leaders to explore vulnerability to share their own story if they have one, or to support others to share their own story as well. We know that this helps in demystifying mental health."

If you're worried about someone and feel they need professional support, encourage them to contact their Employee Assistance Program (EAP), appropriate agency support service or connect with a trusted health professional, like their local doctor.

Pinnacle Charitable Foundation is a Funding Partner of R U OK? and is proud to fund the 'Are they Triple OK?' campaign.

Specialised wellbeing and mental fitness support for first responders and their families can be accessed through Fortem Australia at **fortemaustralia.org.au.**

For 24/7 for crisis support call Lifeline on **13 11 14**. Text support is also available: **0477 13 11 14**.


PROTECT MORE
LIVES IN
MORE PLACES
AXON
LEARN MORE AT AU.AXON.COM

Using Artificial Intelligence in Law Enforcement and Policing to Improve Public Health and Safety

February 13, 2025

PATRICIA HALEY[1] & DARRELL NORMAN BURRELL[2]

Abstract

The integration of artificial intelligence (AI) policing tools and geo-profiling into contemporary law enforcement strategies has revolutionised analysis of concerning behaviour, offering unprecedented precision in the identification of psychological risk factors and predictive crime analysis. AI's sophisticated pattern recognition capabilities, powered by machine learning algorithms, enable the dissection of vast datasets to uncover complex behavioral trends, latent correlations, and risk indicators often imperceptible to human cognition. This analytical depth enhances law enforcement's ability to identify links between disparate criminal activities, forecast potential threats, and shift from reactive to proactive crime prevention. Complementing AI's prowess, geo-profiling employs spatial analysis rooted in criminology, psychology, and geographic information systems (GIS) to elucidate crime patterns, identify hotspots, and predict offender anchor points. The synergy between these technologies augments investigative efficiency and mitigates cognitive biases inherent in traditional profiling through data-driven objectivity. Moreover, the implications of AI and geo-profiling extend beyond criminal justice, significantly impacting public health and safety. By enhancing crime detection and enabling early intervention, these technologies contribute to reducing violence-related injuries, mitigating psychological trauma, and fostering resilient communities. Police organisations can leverage AI-driven insights to deploy targeted interventions addressing the root causes of violence, such as socio-economic disparities and mental health challenges. This conceptual study explores the transformative potential of AI and geo-profiling in crime prevention, emphasising their role in advancing public safety, promoting health equity, and informing data-driven policies. Ultimately, these innovations represent a paradigm shift in law enforcement and public health, fostering integrated approaches to address the multifaceted challenges of modern crime and its societal impacts.

1 Capitol Technology University, Laurel, MD, United States
2 Capital Technology University and Associate Ethics Fellow, Marymount University, United States Correspondence:
Patricia Haley, Capitol Technology University, United States. E-mail: patriciaaemail@gmail.com/dnburrell@marymount.edu

Introduction

Geo-profiling, also known as spatial profiling, is an advanced investigative technique utilised in criminal profiling and law enforcement to analyse the geographical distribution of criminal activities. This methodology is predicated on the premise that offenders, particularly serial perpetrators, tend to commit crimes near their residences or familiar territories (Glass & Herbig, 2021). By identifying patterns in the spatial distribution of crime scenes, law enforcement agencies can infer probable offender anchor points, such as their homes, workplaces, or frequented locales. One of the foremost advantages of geo-profiling is its capacity to expedite suspect identification. Law enforcement can efficiently narrow down potential suspects involved in similar offenses by meticulously analysing crime patterns, thereby enhancing the focus and efficacy of investigative efforts (Butkovic et al., 2019; Ashby & Craglia, 2007; Casey & Burrell, 2010).

Integrating geo-mapping and geo-plotting technologies further augments the precision of crime analysis. These tools provide dynamic visual representations of crime data, enabling investigators to identify spatial correlations, temporal trends, and potential crime hotspots more clearly (Haley & Burrell, 2024). For instance, by overlaying crime incidents on geographic information systems (GIS), law enforcement can detect clusters of activity that may signify serial offending patterns, thus facilitating the allocation of resources to high-risk areas. This geospatial intelligence improves the timeliness and accuracy of incident reporting and enriches the granularity of information available to investigators, including specific crime locations, timeframes, and environmental contexts (Haley & Burxrell, 2024).

Beyond its applications in law enforcement, geo-profiling holds significant implications for public health and safety. By elucidating crime patterns and identifying high-risk zones, geo-profiling informs the deployment of community-based interventions aimed at violence prevention and public health promotion. For example, public health officials can leverage geo-profiling data to allocate mental health services, social support programs, and crisis intervention resources to communities disproportionately affected by crime. This proactive approach mitigates the immediate risks associated with criminal activities and addresses the broader social determinants of health contributing to community vulnerability.

The Transformative Role of Artificial Intelligence in Criminal Behavior

Artificial intelligence (AI) has revolutionised the domain of criminal behavior, particularly in identifying psychological risk factors, offering unprecedented depth and precision in behavioral analysis. At the heart of AI's transformative capabilities is its sophisticated pattern recognition function, where machine learning algorithms dissect expansive datasets to uncover intricate behavioral trends, risk indicators, and latent correlations often imperceptible to human cognition (Cekic, 2024). For example, AI can identify nuanced links between disparate criminal activities, such as correlating specific modus operandi with geographic crime hotspots or temporal crime trends, thereby providing law enforcement with insights that were previously inconceivable (Cekic, 2024).

The analytical prowess of AI is further amplified by its formidable data processing capacity. Unlike traditional methods constrained by human limitations, AI can rapidly and meticulously analyse voluminous data encompassing criminal histories, psychological behaviors, and socio-environmental factors. Consider a scenario where AI processes thousands of case files to identify recurring themes in offenders' childhood environments, such as exposure to violence or neglect, that may contribute to recidivism. This endeavor would be prohibitively time-intensive for human analysts alone (Cekic, 2024).

Moreover, AI mitigates the pervasive subjective bias inherent in conventional profiling techniques. By relying on empirical data and objective algorithms, AI reduces the influence of cognitive biases and personal intuitions that may skew human judgment. This data-driven objectivity enhances the reliability and accuracy of psychological risk assessments (Cekic, 2024). For instance, AI can analyse linguistic patterns in written communications or social media activity to detect subtle indicators of aggression, deceit, or psychological distress that might remain obscured in traditional evaluations. Additionally, AI's ability to integrate diverse psychological theories, ranging from behavioral reinforcement models to social cognitive frameworks, enriches its analytical depth, providing a comprehensive lens to explore the motivations underlying criminal behavior (Cekic, 2024).

AI's predictive capabilities further distinguish its role in modern criminal analysis. AI can forecast potential criminal activities and emergent threats with remarkable foresight by synthesising data from disparate sources, including digital footprints, surveillance feeds, and socio-demographic databases. Imagine an AI system continuously monitoring online forums for radicalisation patterns, flagging individuals whose behavioral trajectories suggest an escalating risk of violent extremism. This real-time analysis enhances situational awareness and empowers law enforcement to implement preemptive interventions, shifting the paradigm from reactive to proactive crime prevention (Cekic, 2024).

Implications for Public Health and Safety

The integration of AI and geo-profiling into criminal justice systems transcends traditional law enforcement, bearing profound implications for public health and safety. Crime, particularly violent crime, exerts a significant toll on community well-being, contributing to psychological trauma, chronic stress, and adverse health outcomes. By enhancing the precision of crime detection and the efficiency of preventative interventions, AI and geo-profiling technologies play a pivotal role in reducing violence-related injuries, alleviating community fear, and fostering safer, healthier environments.

Public health practitioners can harness insights from AI-driven geo-profiling to inform the strategic deployment of resources, such as mental health services, trauma support programs, and community resilience initiatives. For instance, identifying neighborhoods with high rates of violent crime enables targeted public health interventions aimed at addressing the root causes of violence, such as poverty, social disintegration, and lack of access to healthcare. Furthermore, AI's predictive analytics can support early warning systems for public health crises, such as spikes in substance abuse,

domestic violence, or gang-related activities, facilitating timely responses that mitigate harm and promote community well-being.

The convergence of AI and geo-profiling technologies represents a paradigm shift in criminal justice and public health. These innovations enhance the efficacy of crime prevention and investigation and contribute to a broader vision of public safety that prioritises health, equity, and community resilience. By fostering data-driven, ethically grounded approaches to crime analysis, we can build safer, healthier societies better equipped to address the multifaceted challenges of modern crime and its impacts on public health.

Integrating AI-based systems into law enforcement investigations has revolutionised the analytical landscape, offering specialised tools to enhance operational efficiency, police analysis, law enforcement investigations, and strategic decision-making (Fernandez-Basso et al., 2024). These sophisticated technologies streamline data collection, facilitate comprehensive analysis, and generate actionable insights, thus augmenting the investigative capabilities of law enforcement agencies (LEAs).

Automatic Crawling Tools

Automatic crawling tools are at the forefront of data acquisition, engineered to autonomously harvest vast datasets from diverse digital ecosystems, including social media platforms and the dark web. This automation obviates the need for labor-intensive manual data collection, enabling LEAs to swiftly and efficiently capture relevant intelligence. For instance, during investigations of online radicalisation, these tools can systematically extract posts, comments, and user interactions that may signify extremist activities, providing a critical foundation for subsequent analyses (Fernandez-Basso et al., 2024).

Natural Language Processing (NLP) Tools

Complementing data collection, NLP technologies are employed to preprocess and structure unstructured textual data, rendering it amenable to sophisticated analysis. NLP facilitates extracting meaningful information from natural language content, such as identifying keywords, sentiment trends, and contextual themes within criminal communications. For example, in fraud investigations, NLP can detect deceptive language patterns across emails and financial documents, uncovering fraudulent schemes that might otherwise remain hidden (Fernandez-Bassoet al., 2024).

Knowledge Repository (KR)

The KR is a dynamic, centralised repository for processed knowledge continually updated to reflect new data and evolving investigative insights. This repository enriches analytical processes by providing historical context and cross-referencing capabilities, allowing investigators to trace patterns over time. For instance, correlating data from past cybercrime cases with current incidents can reveal recurring threat actors or tactics, enhancing predictive capabilities (Fernandez-Basso et al., 2024).

Knowledge Discovery (KD) Tools

The system integrates KD algorithms, such as association rule mining, to uncover latent patterns and relationships within collected data. These tools identify complex interconnections that might not be immediately apparent, guiding investigators toward more informed conclusions. In narcotics trafficking investigations, KD tools can reveal distribution networks and transactional linkages between suspects, supporting targeted interdiction efforts (Fernandez-Basso et al., 2024).

Data Visualisation Interfaces

Immersive human-machine Interfaces (HMIs) transform analytical outputs into intuitive visual representations, facilitating the interpretation of complex data. These interfaces enhance situational awareness, enabling LEAs to discern trends, anomalies, and critical insights. For example, visual heat maps depicting crime hotspots can assist in resource allocation decisions and optimising patrol strategies in urban environments (Fernandez-Basso et al., 2024).

Early Warning/Early Action (EW EA) Mechanism

The EW/EA mechanism actively addresses emerging threats by identifying “weak signals” indicative of nascent criminal activities. By detecting subtle anomalies and precursors to organised crime, this system empowers LEAs to implement preventive measures before threats fully materialise.
For instance, early detection of unusual

financial transactions might preempt money laundering operations linked to terrorist financing (Fernandez-Basso et al., 2024).

Scenario-Based Use Cases

To contextualise the system's functionality, scenario-based use cases, such as those involving firearms trafficking, are incorporated. These practical examples demonstrate how the system's tools can be applied in real-world investigations, providing LEAs with operational blueprints for leveraging AI capabilities effectively. Such scenarios illustrate technical applications and highlight strategic considerations in complex investigative environments (Fernandez-Basso et al., 2024).

By equipping law enforcement with these advanced tools, AI-based systems streamline data collection, processing, and analysis and generate profound, actionable insights. This technological synergy enhances investigative operations' precision, efficiency, and overall efficacy, fortifying LEAs' capacity to combat evolving criminal threats (Fernandez-Basso et al., 2024).

Problem Statement

Crime remains an omnipresent and evolving phenomenon that transcends socio-economic boundaries, afflicting both affluent and impoverished nations with equal severity. It encompasses a broad spectrum of offenses that undermine individual safety, community cohesion, and societal stability. These criminal acts range from minor infractions such as threats, harassment, and petty theft to more egregious violations, including domestic violence, illegal possession of firearms or narcotics, cybercrimes, and heinous offenses like sexual assault, homicide, and human trafficking. The Global Organised Crime Index 2023 paints a stark picture of the global crime landscape, revealing that an alarming 83% of the world's population lives in environments characterised by high levels of criminality (The Global Initiative, 2024). This statistic underscores modern criminal enterprises' escalating complexity and transnational reach, often employing sophisticated, technology-driven methodologies that outpace traditional law enforcement capabilities.

As crime evolves, adopting more intricate and globalised dimensions, the need for innovation within law enforcement agencies and crime-fighting organisations becomes increasingly urgent. Traditional investigative paradigms, while foundational, are frequently inadequate for addressing the dynamic, borderless nature of contemporary criminal activities. This research study investigates the transformative potential of integrating artificial intelligence (AI) and geo-profiling into law enforcement strategies. Geo-profiling, a spatial analysis technique grounded in criminology, psychology, and geographic information systems (GIS), provides a nuanced framework for analysing crime patterns, elucidating victimology, and identifying emerging trends among criminal actors. The conceptual premise of this study posits that the synergy between AI and geo-profiling can significantly enhance the precision and efficiency of crime detection, investigation, and prevention efforts. By processing vast datasets to uncover latent patterns and contextualising these insights within specific geographical locales, AI-driven methodologies can facilitate the prediction of criminal behaviors and the identification of crime hotspots, leaving past understanding of techniques of hot spot identification that led to undermining police legitimacy and upturning law-abiding community members living or functioning in the identified hot spot (Braga & Weisburd, 2012). Precision identification of offenders in hot spot locations have shown positive results in overall crime reduction as demonstrated a 42% reduction in all violent crimes and 50 % reduction in violent felonies (Groff, 2015).

Ultimately, this research seeks to contribute to the evolving discourse on crime prevention, offering empirical insights into how technological advancements can fortify global efforts against crime while bolstering public health and safety infrastructures (Haley & Burrell, 2024).

Aim of the Inquiry

The primary aim of this inquiry is to critically examine the efficacy of integrating artificial intelligence (AI) with law enforcement methodologies as advanced tools in combating contemporary crime. This research explores how AI's robust data-processing capabilities, when coupled with the spatial analytical prowess of geo-profiling, can enhance the precision of crime detection, the efficiency of investigative processes, and the effectiveness of preventative strategies. Specifically, the study aims to elucidate how AI-driven algorithms can identify latent criminal patterns that may elude traditional investigative techniques. Furthermore, the inquiry will investigate how geo-profiling and other AI tools can contextualise crime patterns, trends, and evidence within distinct geographical and socio-environmental contexts simultaneously considering the aspects of artificial intelligence applied to predictive models may not necessarily correlate with a reduction in violence if the predictive model is presented from biased data (Fernandes & Zekic, 2023).

By examining this technological synergy, the research aspires to contribute novel insights into optimising law enforcement practices, particularly addressing organised crime's escalating complexity and transnational dimensions. Additionally, this study explores the implications of AI-driven crime prevention strategies on public health and safety, recognising that effective crime reduction has profound ripple effects on community well-being and societal resilience (Healy & Burrell, 2024).

Significance of the Inquiry

The significance of this inquiry lies in its potential to address a critical gap in contemporary law enforcement methodologies amid an increasingly complex and globalised crime landscape. With 83% of the world's population residing in environments marked by high criminality (The Global Initiative, 2024), the demand for innovative, data-driven crime-fighting tools has never been more pressing. Traditional investigative approaches often falter when confronted with modern criminal enterprises' sophisticated, borderless nature, necessitating the adoption of technologies that can process and analyse large volumes of diverse data efficiently and accurately. This research is pivotal as it explores how the convergence of AI and geo-profiling can revolutionise crime prevention strategies, offering law enforcement agencies enhanced capabilities for proactive interventions, strategic resource allocation, and identifying emergent criminal trends. Moreover, the implications of this inquiry extend beyond the realm

of criminal justice to encompass broader public health and safety outcomes. Crime is not merely a legal issue; it is a public health crisis that affects mental health, community stability, and overall quality of life. High crime rates are associated with increased stress, trauma, and health disparities within affected communities. By enhancing the precision and timeliness of crime prevention efforts, AI and geo-profiling technologies can reduce violence-related injuries, mitigate the psychological toll of crime on individuals and communities, and foster safer, more resilient environments. Ultimately, this inquiry seeks to fortify the global discourse on crime prevention, providing empirical foundations that could inform policy development, improve public safety outcomes, and strengthen the resilience of justice and public health systems against evolving threats (Haley & Burrell, 2024).

Method

This conceptual paper explores innovative solutions to contemporary law enforcement challenges through the strategic application of geo-profiling augmented by artificial intelligence (AI). Drawing from emerging and established scholarly literature, the paper seeks to bridge theoretical paradigms with practical implications, offering a nuanced understanding of how AI-driven geo-profiling can transform investigative methodologies. As a distinguished genre within the academic literature, conceptual papers have experienced a surge in scholarly prominence, serving as critical platforms for synthesising disparate strands of knowledge, fostering interdisciplinary integration, and advancing theoretical discourse (Jaakkola, 2020).

In contrast to quantitative studies, which are grounded in empirical data collection and statistical analysis, conceptual papers operate within a framework that prioritises intellectual synthesis over numerical validation. They meticulously curate and analyse existing research, drawing upon theoretical constructs, historical insights, and fragmented academic dialogues to elucidate complex phenomena (Jaakkola, 2020). This methodological approach allows for the interrogation of abstract concepts, the proposition of novel theoretical models, and the exploration of multifaceted issues that may not be readily quantifiable.

Within this scholarly tradition, the present paper harnesses a rich tapestry of interdisciplinary literature to dissect the evolving landscape of law enforcement, particularly in the context of rising global crime rates and the escalating sophistication of criminal networks. By examining the convergence of AI technologies with geospatial analytical techniques, the paper aims to illuminate pathways for enhancing crime detection, predictive policing, and strategic resource allocation. Through this conceptual lens, the study aspires to contribute meaningfully to the academic discourse on law enforcement innovation, offering theoretical insights that could inform future empirical investigations and policy development (Jaakkola, 2020).

Research Question

The following research question guided the inquiry: "*How can artificial intelligence (AI) enhance law enforcement's capabilities for crime detection, investigation, and prevention, and its broader implications for public health and safety?*" This question is designed to explore both the operational efficacy of these technologies in combating crime and their potential to mitigate public health risks associated with criminal activities.

Key Search Terms

To capture relevant literature, a comprehensive set of key search terms was developed based on the core concepts of the study. These terms include:

- Artificial Intelligence (AI)
- Geo-profiling
- Crime Detection
- Predictive Policing
- Crime Prevention
- Public Safety
- Organised Crime
- Law Enforcement Technologies
- Criminal Justice Innovation
- Spatial Analysis in Crime

Boolean Search Strategy

To refine and expand search results, Boolean operators (AND, OR, NOT) were employed strategically:

- ("artificial intelligence" OR "AI technologies") AND ("geo-profiling" OR "spatial analysis") AND ("crime detection" OR "crime prevention")
- ("predictive policing" AND "law enforcement") OR ("AI in criminal justice" AND "public safety")
- ("organised crime" AND "data-driven policing") NOT ("non-violent crimes")

These combinations were designed to capture literature that addresses both the technological and criminological aspects of AI and geo-profiling.

Criminal Justice Databases

A targeted search was conducted across reputable academic and criminal justice databases to ensure the inclusion of high-quality, peer-reviewed sources. These databases include:

- ProQuest Criminal Justice Database
- National Criminal Justice Reference Service (NCJRS)
- Criminal Justice Abstracts with Full Text
- PsycINFO (for criminological psychology studies)
- Scopus
- Web of Science
- IEEE Xplore (for AI and technology-focused studies)
- Google Scholar
- ResearchGate
- Academia.edu

Article Inclusion Strategy

The inclusion criteria were meticulously defined to ensure the relevance and quality of the literature reviewed:

Publication Date

Articles published between 2010 and 2025 capture recent advancements in AI and geo-profiling technologies in policing and law enforcement.

Language

Only articles published in English were considered.

Peer-Reviewed Sources

Preference was given to peer-reviewed journal articles, conference papers, and government reports.

Content Relevance

Studies on applying AI and geo-profiling in law enforcement, crime detection, crime prevention, public safety, and public health were included.

Screening Process

The screening process involved two stages:

Title and Abstract Screening

Initial screening to identify studies that meet the inclusion criteria based on titles and abstracts.

Full-Text Review

Selected articles were then subjected to a full-text review to confirm their relevance to the research question.

Data Extraction and Synthesis

Data was extracted using a structured template capturing key elements such as study objectives, methodologies, key findings, technological applications, and implications for law enforcement and public health. A narrative synthesis approach was employed to integrate findings from diverse studies, identify recurring themes, and highlight gaps in the existing literature.

What is Geo-Profiling

Geo-profiling represents a sophisticated form of predictive analytics that harnesses the power of geographic information to delineate areas with a heightened probability of criminal activity occurrence, particularly in identifying patterns linked to specific crimes such as sexual assaults (Suguna et al., 2022; Willmott et al., 2021; Glass & Herbig, 2021). This advanced analytical method transcends traditional investigative techniques by providing law enforcement with spatial insights that pinpoint "hotspots," which are geographical zones where crimes are statistically more likely to transpire. For example, in cases of sexual violence, geo-profiling aids in isolating neighborhoods with recurrent incidents, thereby enabling law enforcement agencies to strategically concentrate their resources, optimise patrol routes, and expedite the apprehension of offenders (Suguna et al., 2022; Willmott et al., 2021; Glass & Herbig, 2021). Empirical evidence underscores the efficacy of geo-profiling in augmenting case closure rates for rape and sexual assault cases, thus reinforcing its value as a pivotal tool in modern criminology (Haley & Burrell, 2024).

Central to geo-profiling is the application of spatial analysis techniques, including Geographic Information Systems (GIS), crime mapping, and geographic profiling algorithms, which collectively enable the synthesis and interpretation of complex spatial data (Suguna et al., 2022; Willmott et al., 2021; Glass & Herbig, 2021). GIS technology facilitates the systematic collection, storage, manipulation, and visualisation of geographically referenced data, identifying crime-prone areas and deploying proactive preventive measures (Haley & Burrell, 2024). Crime mapping, as an extension of GIS, deciphers temporal and spatial crime trends, such as peak crime hours or crime type concentrations, thereby furnishing actionable intelligence for tactical policing. Furthermore, geographic profiling leverages these crime patterns to hypothesise the probable residential locations of offenders based on the spatial distribution of related criminal events, thus narrowing suspect pools with remarkable precision (Haley & Burrell, 2024).

Recent technological advancements have significantly enhanced the capabilities of geo-profiling. Artificial intelligence (AI) has emerged as a transformative force capable of processing voluminous datasets to uncover latent patterns imperceptible to human analysts (Haley & Burrell, 2024). AI-driven algorithms excel in detecting nuanced crime data correlations, such as spatial-temporal clustering of offenses, and generating predictive models that forecast potential crime hotspots (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021). Beyond pattern recognition, AI can infer behavioral profiles of suspects, drawing from geographic movement data to predict future actions and complementing AI, biometric technologies, which encompasses fingerprint analysis, iris recognition, and voice biometrics to enhance suspect identification accuracy. When integrated with geo-profiling data, biometrics construct a multidimensional view of suspect activities and geolocations, facilitating both real-time tracking and historical movement analysis (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021).

Geographic Information Systems (GIS) remain indispensable in crime prevention, offering a dynamic interface to correlate environmental variables with criminal activity. For instance, GIS can elucidate the interplay between crime rates and socio-economic indicators, urban infrastructure, or public transportation networks, thereby uncovering underlying criminogenic factors (Haley & Burrell, 2024). Predictive modeling within GIS frameworks anticipates emerging crime trends, enabling preemptive resource allocation. Parallel to GIS, big data analytics integrate diverse data streams, from police records and judicial databases to social media footprints, creating a holistic crime landscape analysis. This synthesis facilitates anticipating criminal behavior patterns and identifying at-risk locales (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021).

Predictive analytics further augments crime prevention strategies through machine learning algorithms that extrapolate from historical crime data to identify potential criminal activity hotspots (Haley & Burrell, 2024). This predictive acumen directs law enforcement efforts with surgical precision, optimising resource deployment to areas of highest need. Additionally, advanced wireless and satellite technologies have revolutionised suspect monitoring capabilities. GPS-enabled tracking devices, for instance, allow for continuous surveillance of suspect movements, while satellite imagery provides macro-level monitoring capabilities across vast terrains.

Collectively, integrating geo-profiling with cutting-edge technologies such as AI, biometrics, GIS, big data analytics, and satellite surveillance heralds a new era in law enforcement efficacy. This multidisciplinary convergence enhances the precision of suspect identification and apprehension and fortifies crime prevention frameworks, ultimately fostering safer communities (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021).

The Integration of Theoretical Frameworks with AI Tools

The synthesis of theoretical frameworks with artificial intelligence (AI) tools in criminal analysis unfolds through multifaceted mechanisms that significantly elevate the comprehension of criminal behavior and underlying motivations (Cekic, 2024). Foremost, applying learning theories, notably behaviorism, enables AI to dissect the intricate ways past behaviors predicate future actions. By processing voluminous datasets encompassing the histories of previous offenders, AI discerns entrenched behavioral patterns akin to identifying recurring motifs in an expansive narrative, which serve as predictive indicators of potential criminal conduct (Cekic, 2024).

Moreover, incorporating criminological theories, such as the general theory of crime, empowers AI to evaluate

how constructs like impulsivity, self-control, and the presence of opportunity coalesce to catalyse criminal activities. This theoretical infusion enriches algorithmic models, transforming raw data into nuanced psychological profiles and robust risk assessments that mirror the complexity of human decision-making (Cekic, 2024). Equally pivotal is utilising motivational theories, which AI leverages to unravel the psychological catalysts behind criminal actions. Through meticulous behavioral data analysis, AI isolates specific triggers, such as financial stressors or interpersonal conflicts, that amplify the propensity for criminality, thereby facilitating the design of precision-targeted intervention strategies (Cekic, 2024).

In addition, AI's prowess in systematic data analysis stands as a cornerstone of its efficacy. By amalgamating disparate data sources, including court transcripts, police records, and digital footprints. AI fosters a cohesive analytical framework that bridges theoretical paradigms with empirical realities. This integration fortifies the validity of psychological analysis and enhances its operational reliability (Cekic, 2024). Developing enhanced predictive models further exemplifies the synergy between theory and technology. Guided by established criminological knowledge, AI constructs sophisticated models capable of simulating complex behavioral scenarios, thereby refining the precision of criminal behavior forecasts with a degree of granularity previously unattainable (Cekic, 2024).

Crucially, embedding theoretical constructs within AI algorithms facilitates objective measurement of psychological traits and risk factors, mitigating the intrusion of subjective bias and bolstering the scientific integrity of profiling methodologies (Cekic, 2024). This objectivity is complemented by a dynamic feedback loop wherein AI-generated insights serve to validate, challenge, or refine existing criminological theories. Such iterative interplay fosters an evolving, evidence-based understanding of criminal behavior, continuously enhancing both theoretical constructs and practical applications (Cekic, 2024).

The confluence of theoretical frameworks with AI technologies in criminal profiling catalyses a transformative shift in the field. This integration deepens analytical rigor and predictive precision and equips law enforcement and psychological professionals with empirically grounded tools to devise more effective crime prevention and intervention strategies (Cekic, 2024).

Advantages of AI in Criminal Investigation

Integrating artificial intelligence (AI) into criminal investigation offers many transformative benefits that significantly enhance investigative processes' precision, efficiency, and objectivity (Cekic, 2024). AI's capacity for enhanced accuracy stems from its ability to process and analyse expansive datasets, uncovering complex patterns and correlations that often elude human cognition. For instance, AI can identify nuanced behavioral trends across thousands of case files, leading to more precise psychological profiles and a sophisticated understanding of criminal behavior that transcends traditional methodologies (Cekic, 2024) beyond assumptions based on past behaviors of a person of concern or a checklist of behaviors, known as profiling. More closely, criminal investigations seek atypical behaviors or contextually inappropriate behaviors for a specific person, isolating concerning behaviors known as pre-incident behaviors (Schweit, 2021).

In parallel, AI mitigates the pervasive subjective bias inherent in conventional profiling techniques. Whereas human analysts may unconsciously allow personal experiences and cognitive biases to influence judgments, AI employs objective algorithms and data-driven models that minimise the intrusion of such errors. This objectivity fosters a more impartial and scientifically grounded approach to criminal profiling (Cekic, 2024). Furthermore, AI's capability for real-time data processing revolutionises law enforcement's responsiveness to emerging threats. For example, AI can instantaneously analyse live surveillance feeds or social media activity, enhancing situational awareness and enabling rapid, informed interventions during critical incidents (Cekic, 2024).

The domain of predictive modeling is notably enriched through AI, as its algorithms leverage historical data and identified patterns to forecast potential criminal behaviors. This empowers law enforcement to allocate resources, proactively preventing crimes before they materialise (Cekic, 2024). Additionally, AI excels at detecting subtle, often imperceptible patterns within data. Advanced techniques such as deep learning reveal hidden connections in criminal activities, offering profound insights into offenses' psychological underpinnings and motives (Cekic, 2024).

Another critical advantage of AI is its scalability. It enables the analysis of voluminous information streams from diverse sources, including social media platforms, financial transactions, and surveillance footage.

This capacity ensures that AI can seamlessly integrate across various contexts within criminal justice systems (Cekic, 2024). Moreover, AI facilitates the integration of multidisciplinary theories from criminology, psychology, and sociology, fostering a holistic analysis of criminal behavior and enriching the interpretive depth of profiling efforts (Cekic, 2024).

From an economic perspective, AI enhances cost efficiency by automating labor-intensive data analysis processes. This automation reduces the temporal and resource expenditures traditionally associated with extensive investigations, optimising criminal justice agencies' operational efficacy (Cekic, 2024). AI also augments investigative procedures by analysing patterns in financial transactions, social networks, and communication records, thereby unearthing suspicious activities that might remain undetected (Cekic, 2024).

AI's integration with emotional intelligence algorithms proves invaluable in mental health assessment. It aids in evaluating witness testimonies, discerning micro-expressions, and identifying potential deceit, thereby enhancing the veracity of criminal investigations (Cekic, 2024). Additionally, AI's compatibility with other advanced technologies, such as blockchain, ensures secure data storage and sharing, thereby fortifying the integrity and transparency of the criminal justice process (Cekic, 2024).

In conclusion, the deployment of AI in criminal analysis markedly advances the field by elevating analytical accuracy, operational efficiency, and methodological objectivity. These enhancements provide law enforcement and judicial systems with formidable tools to understand, preempt, and mitigate criminal activities, ultimately contributing to a more effective and equitable justice system (Cekic, 2024).

Innovations in AI and Policing

The Automated Forensic Examiner (AFE) represents a conceptual advancement in digital forensic science. It is envisioned as an intelligent system designed to revolutionise investigative methodologies by automating data analysis, artifact identification, and evidence correlation through artificial intelligence (Al Fahdi et al., 2013). The AFE's architecture is predicated on integrating cutting-edge technologies that collectively enhance the efficiency and precision of forensic investigations.

Foremost among its capabilities is the automation of evidence processing, wherein the AFE employs advanced computational techniques to manage and analyse voluminous digital datasets. This automation facilitates the rapid extraction of pertinent information, enabling forensic examiners to discern critical artifacts with heightened accuracy while systematically filtering extraneous data. For instance, in a complex cybercrime investigation involving terabytes of email correspondence, the AFE can swiftly isolate communications containing suspicious keywords or anomalous patterns, significantly expediting the investigative timeline (Al Fahdi et al., 2013).

Integral to the AFE's functionality is incorporating artificial intelligence (AI), which augments its analytical prowess through sophisticated algorithms and machine learning models. One such AI technique is the application of Self-Organising Maps (SOMs), which adeptly manage large datasets by clustering related events based on inherent data relationships. This clustering mechanism not only streamlines the organisation of forensic data but also aids in constructing coherent evidence trails, thereby elucidating the sequence and interconnection of digital events within a case (Al Fahdi et al., 2013).

Another pivotal AI-driven feature is the deployment of concerning behavior in algorithms within the AFE framework. By integrating behavioral analysis techniques, the system can contextualise artifacts within the broader spectrum of criminal activity, offering insights into the modus operandi and psychological profiles of potential suspects. For example, when analysing digital footprints left by a cyberstalker, the AFE can correlate repetitive behavioral patterns with known profiling models, thereby refining suspect identification (Al Fahdi et al., 2013).

To further optimise investigative efficacy, the AFE incorporates technical competency measures, which assess the complexity of digital forensic cases based on the scope and depth of required analyses. This evaluative mechanism serves as a decision-support tool for investigators, guiding them in prioritising investigative tasks and allocating resources effectively. In scenarios involving multifaceted data sources, such as encrypted communications across diverse platforms, these measures assist in determining the most technically challenging aspects of the investigation (Al Fahdi et al., 2013).

The AI-based law enforcement systems delineated by Fernandez-Basso et al. (2024) signify a paradigm shift in crime investigation methodologies. They offer an array of innovative functionalities tailored to augment the operational capabilities of law enforcement agencies (LEAs). This sophisticated system is underpinned by a multifaceted framework integrating advanced technologies to streamline data acquisition, enhance analytical precision, and foster informed decision-making.

A cornerstone of this system is its data collection and processing capability, which leverages state-of-the-art automatic data crawling mechanisms coupled with natural language processing (NLP) algorithms. This dual approach facilitates the rapid aggregation and synthesis of voluminous datasets from disparate sources, including social media platforms, open web repositories, and the clandestine domains of the dark web. For instance, in tracking illicit activities, the system can seamlessly identify coded language patterns and emerging threats within encrypted communications, expediting the investigative process (Fernandez-Basso et al., 2024).

Central to the system's analytical prowess is the Knowledge Repository (KR), a dynamic database that archives processed intelligence, enabling LEAs to draw upon a reservoir of historical and contextual data. This repository is an intellectual nexus, enriching current

investigations with insights derived from past cases, analogous crime trends, and interlinked data nodes. For example, investigators can cross-reference contemporary cybercrime incidents with archived data to detect recurring modus operandi or suspect profiles, enhancing investigative continuity and depth (Fernandez-Basso et al., 2024).

Further amplifying its analytical capabilities are the Knowledge Discovery (KD) tools, which employ sophisticated algorithms to excavate latent patterns and correlations within the amassed data. These tools excel in unveiling obscured relationships, such as connections between disparate criminal networks or the evolution of illicit activities across geographical boundaries. The resultant insights are instrumental in pinpointing crime hotspots and anticipating potential escalations, thus empowering LEAs with predictive foresight (Fernandez-Basso et al., 2024).

To translate complex data into actionable intelligence, the system integrates immersive Human-Machine Interfaces (HMIs) that facilitate intuitive visualisation of analytical outcomes. These interfaces enhance situational awareness, offering law enforcement personnel real-time, interactive dashboards that depict crime heat maps, network linkages, and temporal trends. Such visual tools are pivotal in crisis scenarios, where rapid comprehension and swift decision-making are paramount (Fernandez-Basso et al., 2024).

A distinctive feature of the system is its Early Warning/Early Action (EW/EA) methodology, which specialises in detecting "weak signals" indicative of nascent organised crime threats. By identifying subtle anomalies and emerging patterns, the system provides preemptive alerts, enabling LEAs to initiate proactive measures and mitigate risks before they escalate into significant security concerns. For example, slight shifts in darknet marketplace activities can trigger alerts about potential trafficking operations in their formative stages (Fernandez- Basso et al., 2024).

The incorporation of semantic technologies further refines the system's analytical accuracy. The system enhances data relevance through semantic filtering and representation models, ensuring that investigators are presented with the most critical and contextually pertinent information. This semantic layer aids in distilling vast datasets into coherent narratives highlighting key investigative leads (Fernandez-Basso et al., 2024). Lastly, the system's architecture is designed with interoperability in mind, facilitating seamless integration with other data-driven law enforcement initiatives. This collaborative framework enables synergistic partnerships with existing projects employing data mining and AI technologies, fostering a cohesive ecosystem for crime prevention and investigative excellence (Fernandez-Basso et al., 2024). In essence, this AI-based system represents a comprehensive, technologically advanced toolset that augments law enforcement agencies' analytical capabilities and transforms the strategic landscape of modern crime investigations.

Rawls' Theory of Justice

John Rawls' Theory of Justice, articulated through the principles of "justice as fairness," provides a foundational framework for evaluating the ethical implications of integrating artificial intelligence (AI) in policing and geo-profiling law enforcement. Rawls's Theory of Justice posits that societal institutions must operate under principles that ensure equal basic liberties and equitable opportunities, particularly benefiting the least advantaged (Said & Nurhayati, 2021). Applied to AI-driven crime prevention, this theory mandates that algorithmic models should not reinforce systemic inequalities by disproportionately targeting marginalised communities. For instance, predictive policing algorithms that rely heavily on historical crime data risk perpetuating biases against communities historically subjected to over-policing. Through the lens of Rawlsian justice, the ethical deployment of AI requires designing systems that mitigate such disparities, ensuring that technological advancements in law enforcement contribute to a fairer, more just society by promoting equal protection under the law and safeguarding civil liberties.

Distributive Justice Theory

Distributive Justice Theory emphasises the equitable allocation of resources, opportunities, and benefits within a society (Wolfe et al., 2018; Charman & Williams, 2022). In the context of AI and geo-profiling in crime prevention, distributive justice necessitates implementing these technologies in ways that do not exacerbate social inequities. For example, if crime prediction models direct disproportionate surveillance towards economically disadvantaged neighborhoods, this could result in over-policing and stigmatisation, undermining community trust and exacerbating existing social divides. Ethical implementation, guided by distributive justice, would require the equitable distribution of crime prevention resources, ensuring that all communities benefit from advancements in law enforcement technologies without bearing undue burdens of surveillance or criminalisation.

Procedural Justice Theory

Procedural Justice Theory focuses on the fairness of the processes through which decisions are made rather than solely on the outcomes of those decisions (Tyler et al., 2015; Nagin & Telep, 2020). This theory is particularly relevant in deploying AI algorithms in law enforcement, where automated systems increasingly influence decisions about surveillance, resource allocation, and suspect identification. Procedural justice demands transparency, accountability, and the inclusion of affected communities in decision-making processes.
For example, law enforcement agencies employing predictive policing tools should engage with the communities most impacted by these technologies, ensuring their voices are heard in discussions about data collection practices, algorithmic design, and policy implementation.
This participatory approach enhances the legitimacy of law enforcement efforts and fosters public trust, essential for effective crime prevention and community safety.

The Capability Approach

The Capability Approach shifts the focus of justice from distributing resources to enhancing individuals' capabilities to achieve well-being (Ayling & Grabosky, 2006; Worrall & Kjaerulf, 2018). In AI-driven crime prevention, this framework highlights the importance of ensuring that technological interventions do not infringe upon individuals' freedoms or capabilities. For example, extensive surveillance enabled by AI and geo-profiling could restrict personal freedoms, such as the freedom of movement and privacy, particularly in communities subjected to heightened scrutiny.
Ethical decision-making, guided by the Capability Approach, would involve

evaluating the broader societal impacts of these technologies, ensuring that they enhance rather than hinder individuals' abilities to lead secure, autonomous, and fulfilling lives.

Accountability and Transparency in AI Ethics (FAT Framework)

The Fairness, Accountability, and Transparency (FAT) Framework has emerged as a key model for addressing ethical concerns in deploying AI technologies (Agrawal, 2024; Matulionyte & Hanif, 2021). This framework emphasises the need for fairness in algorithmic decision-making, accountability mechanisms to address potential harms, and transparency to ensure that the functioning of AI systems is understandable to all stakeholders (Agrawal, 2024; Matulionyte & Hanif, 2021). Stakeholders include law enforcement, community organisations, and policymakers to ensure that biometric technology solutions are implemented responsibly and effectively (Tyler, 2004; Johnson et al., 2022) In law enforcement, the FAT Framework can guide the ethical implementation of predictive policing tools by ensuring that algorithms are regularly audited for biases, that decision-making processes are transparent to the public, and that there are clear avenues for redress in cases of harm or discrimination. For example, if an AI system disproportionately predicts higher crime rates in minority neighborhoods, the FAT Framework would require an investigation into the data and algorithms used, adjustments to correct any biases, and public disclosure of the findings to maintain trust and accountability. The investigation may include, and not limited to any number of criteria that exacerbate societal harm for example, a need for a unified international legal guidance to address significant gap in the accountability and regulation of AI system (Mulyana, 2023), improvements to regulatory oversight and single reliance on private sector AI corporations and a greater understanding of misuse in creating mis- and disinformation or manipulating emotions, especially in online spaces like social media (Pauwels, 2020).

Conclusions

AI-powered algorithms, particularly those leveraging machine learning and natural language processing (NLP), have emerged as transformative tools in the realm of criminal investigations, offering unprecedented capabilities in analysing vast datasets comprising victim statements, case reports, and forensic evidence (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021). These advanced analytical tools are adept at identifying intricate patterns related to victim characteristics, offender interactions, and trauma responses, thus facilitating the creation of comprehensive and dynamic victim profiles (Haley & Burrell, 2024). The ability of AI to process unstructured data, such as emotional narratives and qualitative accounts, enhances our understanding of the psychological and emotional impacts of crime on victims. This deeper insight enables the development of more empathetic, targeted support systems that address not just the legal but also the mental health needs of survivors, contributing significantly to public health by mitigating the long-term effects of trauma on individuals and communities.

Geo-profiling, a cornerstone of modern investigative techniques, gains new dimensions of efficacy when integrated with AI-driven geographic information systems (GIS). These systems analyse the spatial distribution of criminal activities, uncovering hidden connections and patterns that traditional investigative methods might overlook (Özkul, 2021; McDaniel & Pease, 2021; Rowe & Muir, 2021). AI enhances geo-profiling by pinpointing potential offender anchor points, mapping travel routes, and identifying crime hot spots with remarkable precision. This capacity not only aids law enforcement in narrowing search areas and optimising resource allocation but also serves as a critical tool for public health and safety planning. By predicting high-risk areas, public health officials can deploy preventative measures, mental health resources, and community outreach programs to mitigate the broader societal impacts of crime, such as fear, stress-related health conditions, and community disintegration.

For law enforcement agencies to fully harness the potential of AI tools in improving case closure rates, it is imperative to adopt best practices for successful implementation. Central to these practices is data-driven decision-making, which employs crime data and geographic information to create predictive models that can identify potential suspects and high-risk locations with greater accuracy (Haley & Burrell, 2024). This approach streamlines investigative processes, allowing for quicker suspect identification and more efficient deployment of resources. Moreover, integrating current, comprehensive data sources, such as crime databases and GIS, significantly enhances the accuracy of geo-profiling outcomes. Utilising the latest technologies ensures that law enforcement remains adaptive to evolving criminal tactics, thereby maintaining the efficacy of crime prevention and investigation strategies, for example, AI systems can be used for both legitimate purposes, such as in the entertainment and education industries, as well as for malicious activities, such as creating false evidence for criminal activities or spreading media manipulation and disinformation (Farid & Schindler, 2020; Labuz, 2024).

However, deploying geo-profiling technologies necessitates carefully considering ethical and legal implications, particularly concerning privacy and civil liberties (Fernandez-Basso et al., 2024). Aggregating and analysing extensive personal data raises profound privacy concerns, as these processes often occur without explicit consent, potentially infringing on individuals' rights to digital privacy. For example, mining mobile location data to identify crime hotspots could inadvertently expose sensitive information unrelated to criminal activity, compromising innocent individuals' privacy. Additionally, there is an inherent risk of algorithmic bias, where predictive models may disproportionately target certain demographics, leading to over-policing in marginalised communities and exacerbating existing social inequalities (Haley & Burrell, 2024).

To address these challenges, AI systems must prioritise transparency and actively mitigate discriminatory outcomes through robust governance frameworks (Fernandez-Basso et al., 2024). Key strategies include ensuring human oversight, where AI is an analytical assistant rather than an autonomous decision-maker. This approach guarantees that all AI-generated insights are critically evaluated and contextualised within ethical and legal frameworks. Additionally, algorithmic explainability is vital; AI tools must be designed to be interpretable by non-technical law enforcement personnel, fostering accountability and reducing the risk of bias in decision-making.

The dynamic Knowledge Repositories (KR) management further supports ethical AI deployment. Regular updates incorporating diverse, representative data sources help counteract algorithmic bias, promoting equitable analytical outcomes. Moreover, systematic ethical audits and bias

monitoring are essential to ensure that AI tools align with principles of fairness, justice, and non-discrimination (Fernandez-Basso et al., 2024). Emphasising the detection of "weak signals" represents a proactive approach to crime prevention, focusing on emerging threats rather than historical crime patterns, thus reducing reliance on potentially biased data.

In the broader public health and safety context, the ethical deployment of AI and geo-profiling technologies can significantly contribute to societal well-being. By enhancing crime detection and prevention capabilities, these technologies improve immediate law enforcement outcomes and support the development of safer, healthier communities. Effective crime prevention reduces the prevalence of violence-related injuries, alleviates community stress, and fosters environments where public health initiatives can thrive. Ultimately, the integration of AI in geo-profiling embodies a dual promise: advancing the frontiers of criminal justice while safeguarding the ethical principles that underpin a just and equitable society (Fernandez-Basso et al., 2024).

Recommendations for Future Research

Investigating crime as a complex societal phenomenon necessitates a multidisciplinary lens, integrating insights from criminal justice, legal jurisprudence, and public health to construct a holistic understanding of its underlying dynamics. This study's innovative application of artificial intelligence (AI) and geo-profiling underscores the transformative potential of technology in crime analysis. However, to cultivate a more comprehensive framework, future research must intertwine these quantitative methodologies with robust qualitative approaches that capture the nuanced, lived experiences of affected individuals and communities. The following recommendations delineate strategic research avenues to deepen our comprehension of crime and enhance interdisciplinary interventions.

Grounded Theory Approach

Future research should consider employing grounded theory to delve into crime survivors' lived experiences and perceptions, particularly focusing on the barriers they face in accessing support services and pursuing justice. Grounded theory's inductive methodology allows for the emergence of contextually rich, data-driven insights that illuminate the psychological, sociocultural, and systemic factors influencing survivors' journeys. For instance, examining narratives from diverse survivor populations could reveal patterns in how legal frameworks, community support structures, and cultural stigmas intersect to shape their experiences, thus informing more responsive policy and practice reforms.

Qualitative Focus Groups

Conducting qualitative focus groups with key stakeholders, including survivors, victim advocates, law enforcement officials, and mental health professionals, can foster in-depth dialogue on the multifaceted impacts of crime at both individual and community levels. These focus groups can serve as dynamic platforms for exploring divergent perspectives on critical issues such as trauma recovery, public perceptions of safety, systemic biases, and the efficacy of current intervention strategies. For example, discussions with law enforcement and survivor advocacy groups may uncover communication and resource allocation gaps, leading to more integrated and survivor-centered approaches to crime prevention and response.

Future scholarly endeavors can significantly enrich the existing knowledge on crime and public safety by embracing qualitative research methodologies such as grounded theory, focus groups, qualitative case studies, and phenomenological analyses. These approaches will complement the technological advancements presented in this study, facilitating a more comprehensive, empathetic, and context-sensitive response to the profound societal ramifications of crime. Such interdisciplinary integration is essential for crafting evidence-based strategies that address the symptoms of crime and tackle its root causes within diverse sociocultural landscapes.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license **(creativecommons.org/licenses by/4.0/)**.

New AI Tool to Identify Knives Could 'Transform' Policing of Knife Crime

13 February, 2025

MARTYN LANDI

independent.co.uk

Researchers at the University of Surrey have created a tool which can quickly identify weapons and help track their origins.

A new AI system trained to identify knives could help "transform" how police forces tackle knife crime, researchers have said. Knife Hunter, a system developed by the Institute for People-Centred AI at the University of Surrey, can help police forces identify weapons and then trace their origins more quickly, and has been developed in collaboration with the Metropolitan Police.

The research team said it can allow police to more easily log weapons found, recovered or seized, trace retail or illegal import channels and monitor geographical trends – as well as see reports the system generates on knife crime patterns to help support policing and inform policymaking.

More than 50,000 knife crime offences were recorded in England and Wales in the 12 months to June 2024 – a 4% rise on the previous year.

Professor Miroslaw Bober, the project lead at the Institute for People-Centred AI at the University of Surrey, said he hoped the system could be rolled out widely to other police forces and local authorities, having been used in a trial as part of the Met's Operation Spectre, which aims to tackle knife crime.

"For the past three years, we've partnered with the Metropolitan Police to develop a system that we believe could revolutionise how forces across the country tackle knife crime in the not-too-distant future," Professor Bober said.

"Knife Hunter transforms the way police process and analyse images and videos, doing it faster and more efficiently.

"More importantly, it's a major step forward in helping uncover the origins of weapons in our communities.

"Looking ahead, we're excited about the potential for Knife Hunter and similar tools to work hand-in-hand with Police and local communities to create safer streets for everyone."

The system powering Knife Hunter has been trained on a dataset of over 25,000 images of 550 different knife types, and as a result is able to identify even the most subtle distinguishing features of a weapon, regardless of the viewing angle or lighting conditions, the researchers said.

Professor Adrian Hilton, director of the Institute for People-Centred AI said the project was a timely example of AI technology being used for societal good.

"This research innovation is timely. At a time when the UK Government is trying to rebalance their approach to AI,

from leading with risk management and safety to placing seizing the opportunities for AI to improve lives front and centre, we're showing how people-centred AI can transform lives and communities for the better," he said.

"Working with public sector and commercial partners across a range of grand challenges – in this case with the police to make the streets safer – we're harnessing the power of AI for good."

Science and Technology Minister Peter Kyle said: "AI has the potential to support police in stopping these awful attacks and save lives.

"This is just the tip of the iceberg of what AI could do for our nation, on top of transforming healthcare, boosting productivity and putting time back in people's hands – supporting our Plan for Change."

Knife Hunter transforms the way police process and analyse images and videos, doing it faster and more efficiently. More importantly, it's a major step forward in helping uncover the origins of weapons in our communities

Professor Miroslaw Bober

New York City Wants Subway Cameras to Predict 'Trouble' Before It Happens

April 30, 2025

DOMINIC PRESTON

The Verge

New York's MTA is exploring AI technology to detect and prevent dangerous behaviour on subway platforms before incidents occur.

New York's Metropolitan Transportation Authority says it's exploring the use of AI systems for "predictive prevention" of crime and dangerous behavior on the city's subway platforms.

MTA chief security officer Michael Kemper said that the agency is "studying and piloting technology like AI to sense potential trouble or problematic behavior on our subway platforms."

"If someone is acting out, irrational… it could potentially trigger an alert that would trigger a response from either security and/or the police department," he explained during an MTA safety committee meeting Monday, emphasising that the police response could come "before waiting for something to happen."

"AI is the future," he added, noting that the MTA is "working with tech companies literally right now" to investigate "what would work in the subway system." Kemper didn't detail which companies the MTA is working with, how AI will be implemented, or exactly what sort of behavior the AI-enabled cameras will be expected to detect.

However, MTA spokesperson Aaron Donovan confirmed to Gothamist that the new system won't rely on facial recognition.

"The technology being explored by the MTA is designed to identify behaviors, not people,"

Donovan said.

This isn't the first time the MTA has implemented AI. In 2023 it disclosed that it was using AI-powered surveillance software to track fare evaders on the subway, monitoring when, where, and how most fare evasion takes place.

AI Can Help Police Predict if Someone Is at Risk of Domestic Abuse

November 26, 2024

BEN ELLERY

Crime Editor, The Times

‘Lizzy’ gives probability of physical violence within three months with 84 per cent accuracy, and could be made available to British forces.

Police will be able to predict when a domestic abuse victim is most likely to come to harm by using AI software developed by Oxford researchers.

Officers responding to domestic incidents will ask victims a series of questions and enter the answers into the tool, nicknamed Lizzy, which will use AI to anticipate how an abusive relationship will develop.

The accuracy score — 84 per cent — is 30 percentage points higher than the tool being used by British police at present, according to the researchers.

People who score highly will be recommended to stay in a refuge or referred to victim support services.

The findings have been outlined in a research paper published by Lucy Trafford, a PhD candidate at the University of Oxford, and scientists from the German-based tech company Frontline.

Trafford said: “At 84 per cent, Lizzy’s ability to predict physical violence within the next three months makes her one of the most accurate risk-assessment tools used to counter domestic abuse globally.”

Since August, Lizzy has been deployed by Frontline workers in eight German states to diagnose and predict abuse experienced by victims of intimate partner violence.

Babatunde Williams, Frontline’s chief executive, said the company is in discussions with two British police forces about offering the tool, and profits will go towards making it available to charities.

Williams said: “When risk assessments are used to inform decision-making it cuts repeat domestic violence by 50 per cent. We’ve spoken to women who tell us that they are not likely to tell a police officer that they have just been raped by a partner because it could send them to prison for a long time, but they might reveal that they are being financially controlled.

“Our model recognises that someone being financially controlled has an 80 per cent chance of being physically abused, so those proxy questions are very important.

“Our model can predict how likely it is someone will be abused within three months — the current standard is 18 months. If an officer discovers that the probability of abuse is high then they can recommend that person goes to a refuge or refer them to victim support services.”

Conducted via the research firm YouGov, Lizzy’s research base is several times larger and significantly more representative than most police samples used to build risk assessments in Europe.

“Broad-based and nationally representative data collection is crucial to building machine-learning tools which do not replicate the biases humans are susceptible to,” said Ba Linh Le, Frontline’s chief data scientist.

Police cameras at the Real Time Crime Center inside the Modesto Police Department in Modesto.

Modesto Police Department Experimenting With AI Gun Detection: How Does It Work?

March 19, 2025

TREVOR MORGAN

The Tribune

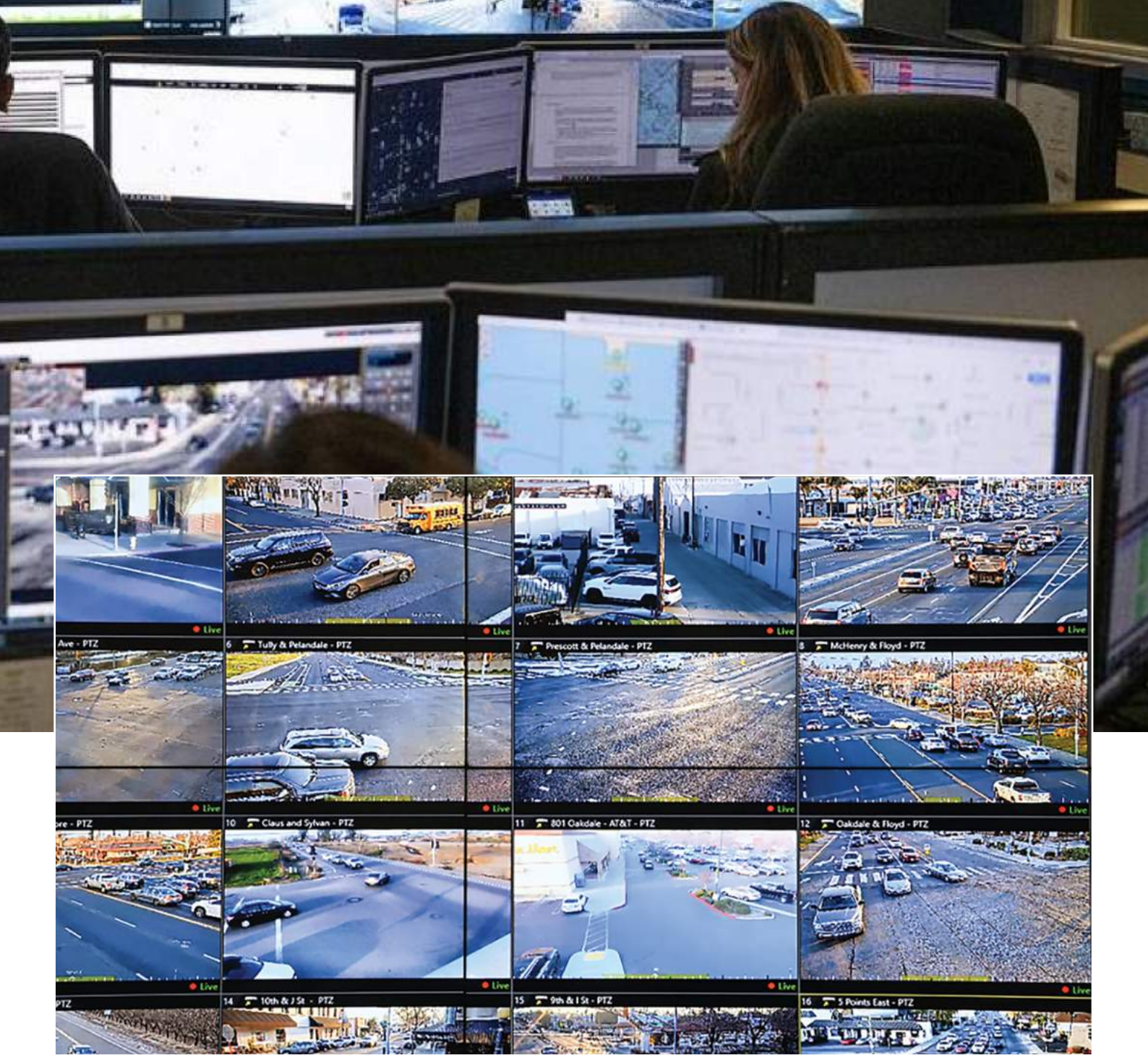
The Modesto Police Department is experimenting with gun-detecting artificial intelligence software as part of a pilot program that began last month, the agency announced.

ZeroEyes — a Philadelphia-based tech startup — gained access to several existing security cameras across the city, which will be monitored by AI until April. The software has the ability to detect what type of firearm someone is holding, where it's last known location was and notify law enforcement in about three to five seconds, according to the company.

But how exactly does it work?

"What basically happens is our algorithm says, 'Hey, I think it's a gun,'" co-founder Sam Alaimo said. "An image will be sent from the client location to our operating center. That human in the loop will verify if it is a gun, [and if it is] they'll dispatch it. If it is not, they will not dispatch it."

Having humans verify the AI-selected images sent into ZeroEyes is crucial to its effectiveness. Alaimo, a former Navy SEAL, said the command center where the detected images are sent is staffed every day, around the clock, by law enforcement and military veterans.



The human element could also prevent an overreaction. In 2022, the New York Times reported that ZeroEyes detected a weapon near a high school track meet in Louisiana. After the detection, the ZeroEyes team determined that it was just a replica airsoft gun. Instead of having law enforcement respond, local school district officials responded.

"We do not want to send false positives to the end user," said Alaimo. "That's how you begin to erode the performance and the trust."

A lot of security cameras don't have high image quality, so false positives by AI could happen. However, Modesto's real-time crime center has access to hundreds of live video feeds — some of which capture 4k-resolution images. Because the RTC is staffed only Monday through Friday from 8 a.m. to 6 p.m., ZeroEyes could monitor some of its cameras when no one is there.

To train its algorithm, ZeroEyes fed it over 1 million images in a variety of environments. The software was designed to prevent school shootings and is used hundreds of schools across the country. However, Alaimo said it could be used in practically any setting. ZeroEyes' website touts dozens of articles that show governments, religious institutions and private sectors have used its system, resulting in arrests.

After an image is detected, then human-confirmed, ZeroEyes alerts its client. It is plugged into the local 911 system, but it can also send out an mobile app alert, videos and a desktop dashboard. Alaimo said that from the moment a gun is seen, it should take about three to five seconds before boots on the ground gets the alert.

MPD did not release the specific locations where it will be testing ZeroEyes. But if it's happy with the product, it could expand it to local schools and Vintage Faire Mall.

MPD's demo began in mid-February and will last until mid-April. Afterward, MPD will have to decide "if the software is feasible to move forward with or not," said department spokesperson Sharon Bear.

Alaimo said Modesto approached ZeroEyes early last year, expressing interest in the program. The pilot came at no cost to the city, according to MPD.

BN HOMES
& DEVELOPERS

New Houses - Knock down rebuilds - Developments - Project management - Custom Builds - Tiling - Roofing - Bathrooms - Kitchens

Contact Us: 0421 343 369

Proudly supporting our police members locally

Cyborg 1.0

Apr 17, 2025

JIJO MALAYIL

Interesting Engineering

Thai Robocop Patrols Streets With 360° Eyes, Live Face-Tracking Power

Thailand introduces its first robot cop to patrols Songkran festival.

The new offering is a Robocop-style robot officer equipped with smart 360-degree AI cameras.

Thailand has unveiled its first AI-powered police robot, deployed during the Songkran festival in Nakhon Pathom province to boost public safety.

The Royal Thai Police (RTP) introduced the robot on April 16 via a Facebook post.

Named "Pol Col Nakhonpathom Plod Phai," meaning "Nakhon Pathom is safe," the robot was stationed at the Tonson Road festival venue in Muang district.

In March, China introduced humanoid robots in Shenzhen to patrol with police, interact with pedestrians, respond to voice commands, and wear high-visibility vests, drawing public attention.

Surveillance gets smarter

The robot, named "AI Police Cyborg 1.0," made its debut during the Songkran festival in Nakhon Pathom province. Developed collaboratively by Provincial Police Region 7, Nakhon Pathom Provincial Police, and Nakhon Pathom Municipality, this Robocop-style unit is equipped with advanced surveillance and threat detection technologies.

AI Police Cyborg 1.0 uses onboard AI to immediately process and analyze data by integrating real-time data from aerial drone footage and local CCTV networks. Rapid reaction coordination is made possible by the robot's in-built 360-degree smart cameras, which are immediately connected to the province's Command and Control Center and backed by video analytics software, according to The Nation.

The robot's facial recognition capabilities enable it to recognize people who have been marked as high-risk or wanted. Its technology can identify and locate people in busy event locations by analyzing a variety of visual clues, such as gender, body shape, clothing, and face features. Additionally, the robot is taught to recognize offensive activities, including fighting, physical altercations, and other disturbances.

Together with behavioral analysis, the robot can recognize possible weapons like knives and blunt objects like wooden sticks while deftly ruling out innocuous devices like water cannons, which are frequently used during Songkran celebrations.

RTP claims that the cutting-edge patrol system is a major advancement in Thailand's use of AI in public safety operations.

Future police now

Humanoid robots have already begun assisting police patrols in neighboring China, capturing public interest with their interactive functions. In Shenzhen, PM01 model robots developed by EngineAI have been deployed alongside officers, wearing high-visibility police vests. These robots have been seen engaging with pedestrians—waving, shaking hands, and responding to voice commands—according to local media reports.

A recent video shows a PM01 robot waving to a crowd, sparking curiosity about its purpose in law enforcement. First launched in December 2024, the PM01 features agile mobility, an interactive touchscreen, and an open-source platform. This design allows developers worldwide to contribute to its evolution by adding new features and capabilities through secondary development.

The deployment of these humanoid robots is part of China's broader strategy to integrate robotics into public safety, emergency services, and law enforcement. This initiative also includes the testing of other advanced robotic systems. In the same month, Chinese authorities trialed the RT-G robot, an autonomous spherical unit created by Logon Technology.

Built for tough conditions, the RT-G can traverse both land and water at speeds of up to 22 mph (35 km/h) and endure impacts of up to 4 tons (8,818 pounds), making it ideal for use in extreme environments.

Together, these developments signal countries' growing investment in robotic assistance for public safety and policing.

Thind Transport Group is one-stop solutions for providing logistics, warehousing, refrigeration, for the last 15 years within Australia.

Arrange a quote by visiting our website at www.thindtransportgroup.com.au

Call us on 0468 350 034 Or send us an email at info@thindtransportgroup.com.au

Proudly Supporting Our Police Members Locally

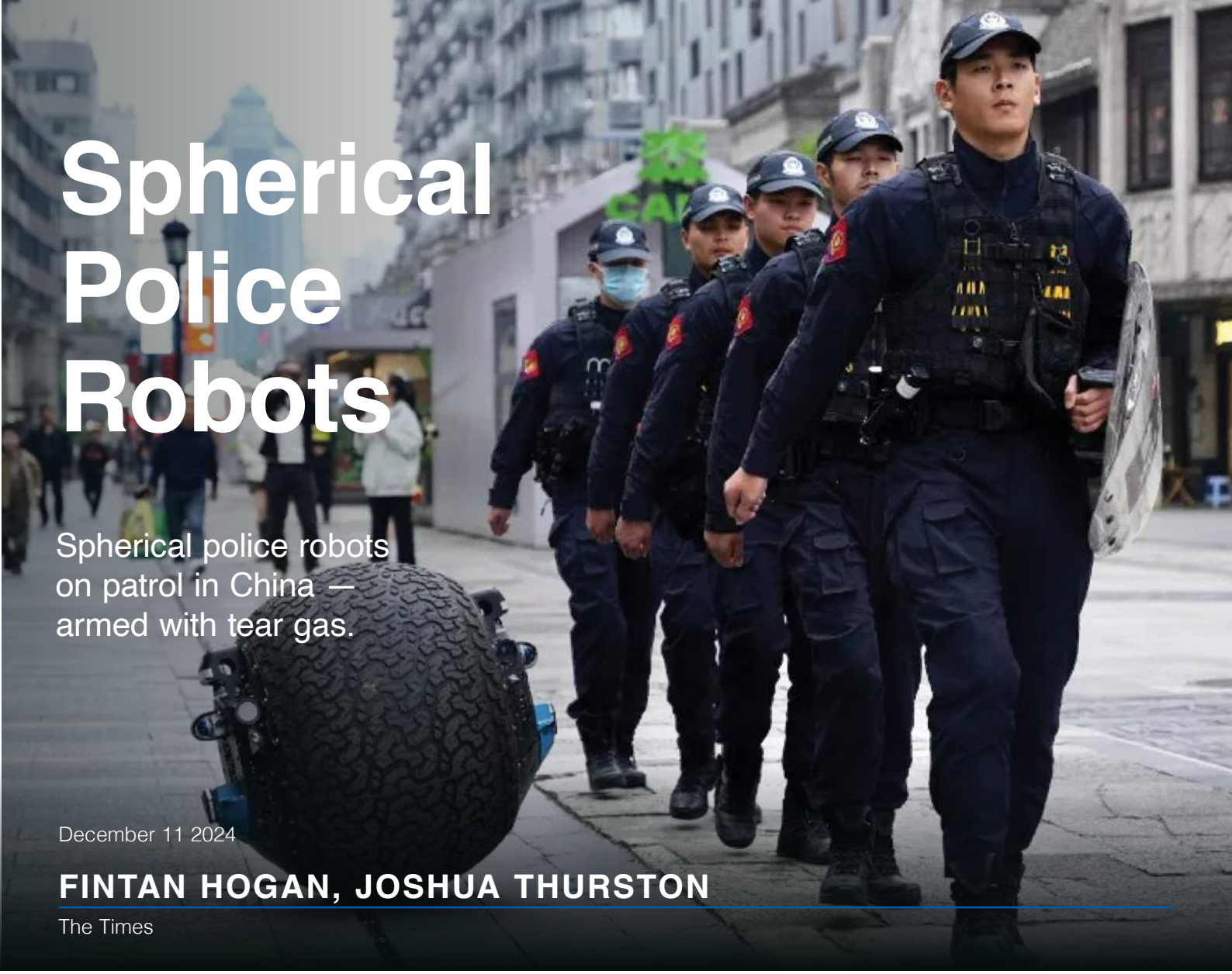
JD Interstate Transport can assist in transporting all sizes of freight, whether it's just one pallet or a B-double load, our experienced team ensures your freight is delivered safely and on time, and we offer excellent service at a competitive price.
We are renowned throughout the East coast of Australia for our professionalism and commitment to moving large quantities of freight between Brisbane, Sydney, Melbourne and Adelaide.

Phone us on (02) 4423 4366

www.dunntransport.com.au

Proudly Supporting Our Police Members

Spherical Police Robots



Spherical police robots on patrol in China — armed with tear gas.

December 11 2024

FINTAN HOGAN, JOSHUA THURSTON

The Times

The AI-controlled Rotun can travel at 22mph and be equipped with nets, loudspeakers and crowd dispersal devices.

They were originally designed to "replace humans" in hostile environments such as the moon or on Mars. Before that happens, however, China's army of rolling spherical police robots is being deployed to snoop on the streets.

Weighing in at 125kg with an AI brain, the robots are equipped with tear gas. Designed by Logon Technology, each has a ten-hour battery life and can be equipped with loudspeakers, nets or crowd dispersal devices.

Developers claim the RT-G, or Rotun, autonomous spherical robot can operate either on land or in water, reach a rolling speed of 22mph and withstand impacts of up to four tonnes. "We make fiction real!" the company declares on its website.

In footage shared by China's state-run media, an RT-G unit can be seen flanked by a Swat team patrolling a street in Wenzhou, Zhejiang province.

The Shenzhen robotics company behind the robots says that advanced AI allows each one to autonomously respond to threats with "tracking, combat and capture capabilities". Like something out of Blade Runner, the Rotuns use facial recognition to detect, pursue and immobilise suspected criminals.

Each unit can also alert other nearby RT-Gs to a potential threat and call for reinforcements in a pursuit. A promotional video released by Logon Technology shows several of the robots cornering a suspect and subduing them by firing a built-in netgun.

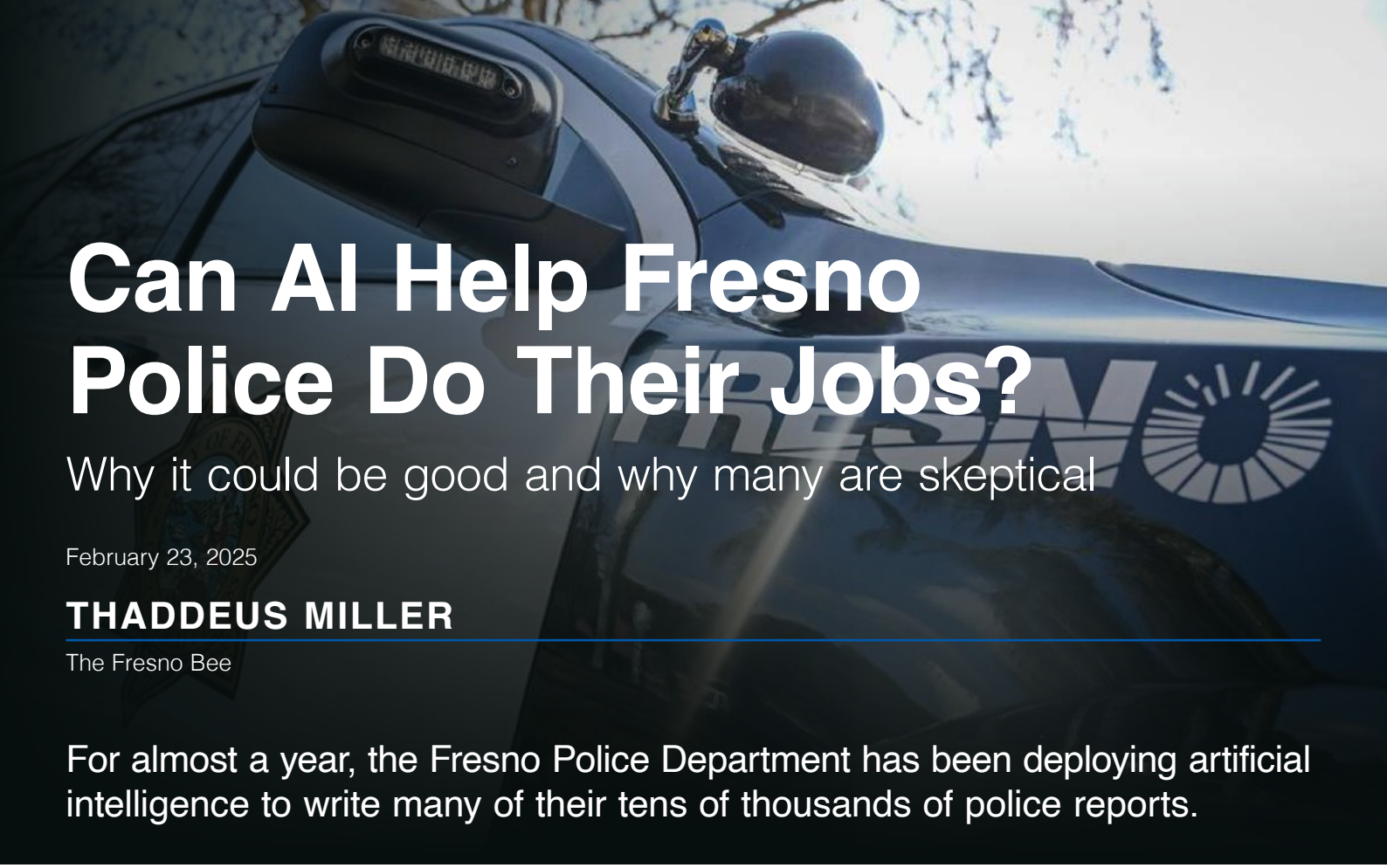
"Narrow terrain, extreme weather, dangerous work environments, violent conflicts and wars, all pose huge threats to human life and activities. Thus an amphibious, intelligent robot emerged to replace humans in these style environments. This is the Rotun spherical robot," the company's video announces.

The robot's design is based on a concept from Zhejiang University's State Key Laboratory of Industrial Control Technology. The original project aimed to create a robot capable of exploring "harsh environments and unknown environments, such as wildfire fields and underground caves".

But rather than focusing on the search and rescue or scientific potential, Chinese leaders have instead promoted military and law enforcement models.

As early as 2020, the People's Liberation Army (PLA) unveiled a go-kart-style device mounted with a machinegun which could operate autonomously. "They may in the future fight side by side with human soldiers on the front line of national defence," an official announced.

Earlier this year, the PLA launched a remote-controlled mechanical dog fitted with a rifle during its "Golden Dragon 2024" exercise with Cambodia. Two years prior, loudspeaker-equipped robot dogs were deployed by police in Shanghai to bark out lockdown rules during a Covid-19 outbreak.



Can AI Help Fresno Police Do Their Jobs?

Why it could be good and why many are skeptical

February 23, 2025

THADDEUS MILLER

The Fresno Bee

For almost a year, the Fresno Police Department has been deploying artificial intelligence to write many of their tens of thousands of police reports.

Officers monitor maps, street video cameras and police officer calls inside the Fresno police department's real time crime center at police headquarters on Monday. The department began using artificial intelligence to write some of their reports in the past year.

Fresno is believed to be one of the first and largest U.S. cities to deploy what's known as generative AI to write police reports informed by officers' body-worn cameras. But, while officials say AI has made the often time-consuming practice of writing police reports more efficient, the technology's use has drawn concerns from civil rights groups and defense attorneys.

Officers have been outfitted with body-worn cameras made by Axon Enterprises since 2015. Last April, the department began using Axon's First Draft program to start writing police reports.

The company and Fresno police say the program is meant to be a time saver in the more than 90,000 reports written by Fresno officers in a year. Neither police nor Axon provided proof the cameras save time.

Fresno Chief Mindy Casto said the department does not have a scientific way to calculate time saved, but has estimated a 20% savings.

Officials with Axon said departments average a savings of about 23 minutes per police report.

Casto said the department has rolled the program out slowly, only using the software on misdemeanors, excluding more sensitive crimes like domestic violence or resisting arrest.

"I think the value is only going to grow as we expand the program, but I want to be very cautious in the roll out to make sure we've mastered it before we start delving into the more serious crimes," Casto said.

Those working outside of law enforcement say they're concerned adding AI into the mix could violate the rights of citizens and complicate holding officers accountable.

How AI police reports work

The body cameras officers turn on during calls for service immediately send the information collected to the police department's cloud — remote servers that collect large amounts of information.

Axon's software then writes a "first draft" of the encounter into a format that fits police reports within about three to five minutes after an officer ends the recording, according to Noah Spitzer-Williams, Axon's senior principal product manager of generative AI.

The AI is not meant to do all of the work, he said. Each officer is supposed to review the report, add details and respond to prompts during the process.

"At the end of the day, the officer owns the final words of the report, but draft one is here to kind of give you a good head start," he said. "They make their edits, they sign off on it, and they're back out in the field."

Some officers may even dictate details they are seeing during the call so that the AI can include them in the first draft,Spitzer-Williams said.

Fresno's relationship with Axon

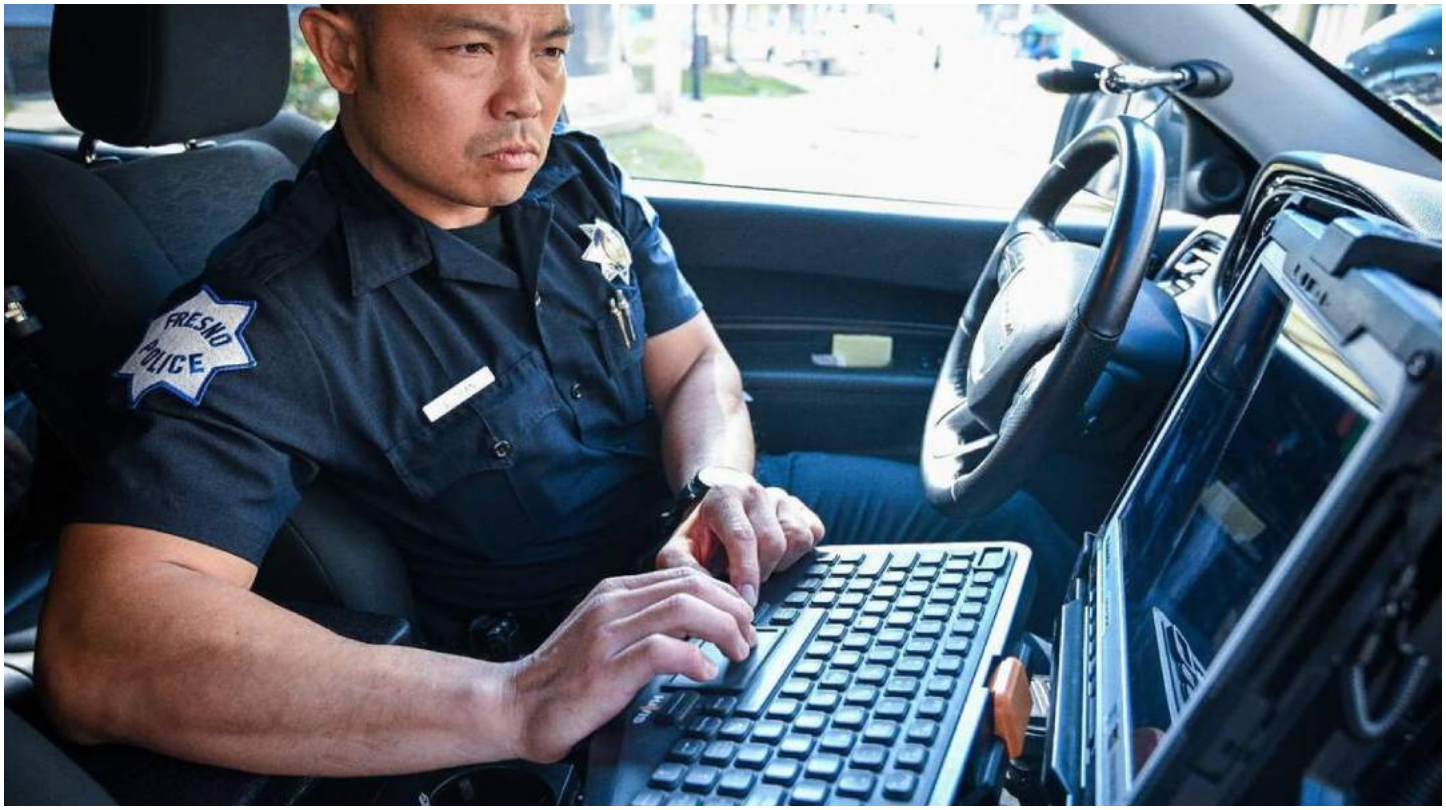
Axon has had a technology-testing relationship with Fresno Police Department in exchange for steep discounts. Fresno became a "development partner" with Axon in 2017 and has access to its new technologies for "little to no cost to the city," according to city records.

Former Police Chief Paco Balderrama discussed the Axon partnership during the June 2024 city budget hearings.

"We're very proud of that because we have been cutting-edge as far as technology, as far as tasers, body-worn cameras, drones," he said. "And we've even helped developed a lot of different products, three that I can think of right now, that we are one of the very first in the world to utilise."

He said the department gets "about a $19 million break" compared to agencies that do not have a development partnership.

The Fresno City Council approved a five-year $18.3 million contract with



Fresno police department public information officer Luke Tran logs into his vehicle computer system in his patrol car near police headquarters on Mariposa Mall in downtown Fresno. The department began using artificial intelligence to write some of their reports over the past year.

Axon last year, which included about $1.3 million for the First Draft program.

Axon representatives declined to say whether Fresno is the largest city using the AI reports, citing privacy concerns.

Some other cities known to be using the technology include California towns like San Mateo, East Palo Alto and Campbell, all of which are smaller than Fresno. Other cities include Fort Collins, Colorado; and Lafayette, Louisiana.

Potential pitfalls and concerns

Experts, defense attorneys and civil rights groups remain concerned about how AI reports are used and what that could mean for the civil rights of the accused.

The American Civil Liberties Union has come out against AI reports, citing the potential for warping the memories of officers, a potential for bias AI has shown and transparency, among other reasons.

The King County Prosecuting Attorney's Office in Washington was concerned enough to send a memo to police departments in September telling officers to not use AI in reports, citing the potential for errors.

Defense attorney Jeffery Hammerschmidt of Fresno said he has not seen an AI police report so far in court, but says attorneys often use AI themselves. But, as police should, attorneys must be diligent in double-checking the work.

"It can be a good tool but it can't substitute the officer's work," he said. "If an officer was using it as a shortcut, I'm going to find those errors and use it to my advantage to find the truth."

As a private defense attorney, he said he reviews reports and body-worn camera footage often to find inconsistencies. That could be harder on the Fresno County Public Defender's Office.

"It's very different for the public defender's office with their caseload to thoroughly review all the camera footage," he said.

Requests by The Bee to speak about the topic went unanswered by the Public Defender's Office.

An AI startup called JusticeText is also developing the use of AI in reviewing body-camera footage, which public defenders in places like Sacramento and Modesto have used.

Axon's program uses ChatGPT, but Axon's representatives say their version is stripped of the kind of creativity shown in the chatbot version available online.

It is not supposed to come to any conclusions, which are called "hallucinations" when they are inaccurate. That potential for hallucinations is a concern among skeptics.

The new technology has the potential to affect civil liberties and hurt the public trust, and that requires officers to be diligent and not take shortcuts, according to Paul D. Knothe, a partner with Liebert Cassidy Whitmore in Los Angeles. The firm advises police agencies across the state.

"The computer is trained on data generated by humans, so it will reflect our biases and, in some cases, magnify the biases," he said. "So that's why a human check on it is critically important."

He said many agencies would benefit from requiring police officers to save the first draft spit out by the program for comparison against the final draft submitted. That would show errors introduced by the program and, at the same time, prevent an officer who might try to blame their errant actions on the AI.

Casto, who was in an interim position until being announced as full-time chief on Feb. 13, has said she wants to improve Fresno officers' response to non-emergency calls.

"I think for any chief, (AI) is a fantastic tool, especially in a very large, busy agency," she said. "Here where we're just constantly under the gun on calls for service, it could be a game changer for the kind of service that we deliver."

Responsible AI in Policing

HELENA WEBB,
University of Nottingham, United Kingdom

NICHOLAS FITZROY-DALE,
Telemarq, United Kingdom

SAAMIYA AQEEL,
University of Nottingham, United Kingdom

ANNA MARIA PISKOPANI,
University of Nottingham, United Kingdom

QUENTIN STAFFORD-FRASER,
Telemarq, United Kingdom

CHRISTOS NIKOLAOU,
Telemarq, United Kingdom

LIZ DOWTHWAITE,
University of Nottingham, United Kingdom

DEREK MCAULEY,
University of Nottingham, United Kingdom

CHRISTOPER HARGREAVES
University of Oxford, United Kingdom

DOI: **https://doi.org/10.1145/3686038.3686070**
TAS '24: Second International Symposium on Trustworthy Autonomous Systems, Austin, USA, September 2024

The deployment of AI-driven technologies in policing is often welcomed as an opportunity to enhance efficiency in dealing with crime. At the same time, however, these technologies pose risks around data bias, data protection, accuracy and privacy. In addition, socio-organisational factors present challenges to their deployment. In this short paper we provide an overview of the opportunities and risks associated with AI in policing, focusing on current developments in the UK. We discuss what is necessary for a responsible approach to deployment and highlight some of our own project work in this context. The Trustworthy and Useful Tools for Mobile Phone Extraction project shows that tools for the analysis of mobile phone data can include AI-driven features that are both useful and trustworthy. However, tools alone cannot address all the tensions and constraints that police work under. Therefore, an essential component of responsibility is to avoid overstating what AI can achieve.

Introduction

Police work in the UK is carried out by 45 territorial police forces and 3 special police forces. Whilst these forces often conduct their activities very independently from each other (including in the procurement of new technologies), overall direction is set by the National Police Chief's Council (NPCC). In 2021 the NPCC appointed its first Chief Scientific Adviser and in 2024 its first lead for artificial intelligence (AI). These appointments demonstrate considerable enthusiasm for deploying novel technologies across forces. On taking up the role, the NPCC lead for AI said: "… AI presents opportunities for forces to test new ideas, be creative and seek innovative solutions to help boost productivity and be more effective in tackling crime".

Policing is an exemplar of the opportunities and risks associated with the deployment of AI. In this short paper we overview some of the current uses of AI-driven technologies in policing in the UK in order to highlight these opportunities and risks. We reflect on what is needed for a responsible AI approach in this context and discuss our own relevant project work. The Trustworthy and Useful Tools for Mobile Phone Extraction project focuses specifically on the use of mobile phone data for the investigation of crime. AI-informed tools can assist with the extraction and analysis of mobile phone data; however, their usefulness and trustworthiness may be limited by technical and non-technical factors. We describe our development of an open-source tool, RIME (Responsible Investigation of Mobile Environments) to explore how AI features can be usefully and responsibly embedded in analytic tools. We also highlight the importance of not overstating the capacity for technological innovations alone to address entrenched tensions and constraints that complicate police work.

Opportunities and risks for ai in policing

Opportunities

A prime motivation for bringing AI-driven technologies into policing is the promise of increased efficiency. Police forces across the UK have endured severe funding cuts, leading to claims that under-staffed forces are losing capacity to deal with crime. AI-driven technologies are often highlighted as a (partial) solution to this problem as they can conduct certain tasks with increased speed and accuracy. This improves task efficiency and allows human working hours to be targeted more strategically.

One early area in which AI was adopted in this sector involves the use of machine learning for predictive policing. This has included efforts to identify hot spots where crimes are likely to occur, individuals who are likely to offend/reoffend, and individuals who might become victims of crime. Advocates state that resources for crime prevention can then be directed towards the areas or individuals identified, and that this offers a more accurate and cost-effective approach than traditional policing methods.

Another area of interest lies in the automated analysis of images. One example is Automated Number Plate Recognition (ANPR) technologies, which capture a vehicle's number plate information when it passes a digital camera. The collected images are searched to identify vehicles of interest or to punish road traffic violations. The increased integration of AI techniques into ANPR has enhanced the accuracy and speed with which images can be analysed, including in changing and challenging environmental conditions. A second example is automated facial recognition (AFR) technology. As the algorithms to support facial recognition have grown more sophisticated, they can be applied to an increasing range of image sources - such as CCTV cameras, Ring doorbells, mobile phones etc. – and can be used for both real-time and retrospective analysis. Captured images are cross-checked against the Police National Database (PND) or an individual police force's own database to identify people of interest. In September 2023, the UK government Minister for Policing urged for the greater use of AFR in criminal investigations.

Risks

Despite this enthusiasm, AI in policing is associated with various risks. Machine learning for predictive policing has raised familiar concerns over bias, with commentators noting that predictions produced by such systems will reproduce any biases in the data they are trained on. In 2012 the Durham Police Force, in collaboration with the University of Cambridge, developed a decision support tool called HART (Harm Assessment Risk Tool). HART was designed to assist officers to determine whether to keep a suspect in custody or refer them to a crime diversion programme. The tool was trained on data from previous cases and used 34 categories of information about a suspect to determine their risk of committing further offences, which in turn determined their eligibility for the diversion programme. The categories included postcode data; this risked causing a feedback loop in which the system drove police attention towards existing high crime areas and away from low crime areas. Further criticisms of HART included its classification of offenders into 'crude groups' based on ethnic and socio-economic features, and its in-built avoidance of false negatives leading to an over-labelling of individuals as of at high risk of offending, meaning they would not be eligible for the diversion programme. Durham Police stopped using HART in 2021, on resources grounds.

Even though the UK government has been advocating its use, automated facial recognition in policing has raised data protection concerns. In 2019, the civil rights group Liberty supported a legal challenge against its use by South Wales Police. The practice was first ruled to be lawful but then unlawful on appeal. The appeal judgement found that the use of AFR incurred proportionate interference with human rights but that the police force had not done enough to ensure the technology did not have racial or gender bias, and needed to do more to document who they were looking for and what evidence they had that people of interest would be in the monitored area. The force paused its use of AFR until a 2023 report published by the National Physical Laboratory identified improved accuracy in facial recognition systems, including the capacity to mitigate for biases. Since then both the South Wales Police and Metropolitan Police have used AFR at public events such as concerts and sports matches. Discussions over the ethics and legality of AFR continue, with notes of caution highlighting the intrusiveness of taking and (temporarily) storing people's images and that, even if the technology is not biased, it will be disproportionately used to monitor certain demographics over others.

Wider socio-organisational factors also present risks to the deployment of AI in policing. Despite policy commitments to technological innovation, police staff in the UK have expressed dissatisfaction and low confidence in ICT provision and training,

with only 30% believing that their force invests wisely in technology. Public opinion is also nuanced. Research suggests that people see a benefit to the use of facial recognition technology but fear the normalisation of surveillance and want appropriate safeguards to be in place. The lack of transparency regarding algorithmic processes and decision-making is a barrier to confidence but can also lead to an over-trust in AI-based results. Meanwhile, public confidence in the police overall is low, a consequence of high-profile scandals concerning misconduct and the mishandling of cases. The deployment of non-trusted technologies by a non-trusted sector can be seen as a considerable risk – in particular when the stakes are high since errors can cause miscarriages of justice.

Ai in policing: the need for a responsible approach

The brief overview above demonstrates that a responsible approach is needed to balance the opportunities and risks of deploying AI in policing. A responsible approach involves taking a future-facing interest in identifying the intended and unintended impacts of innovation, plus attending to societal concerns to ensure the acceptability of innovation. Current evidence suggests that some unintended negative impacts of AI in policing have been identified but not necessarily mitigated. In addition, public perspectives and values do not fully align with current deployments. Vallor's 2023 declaration provides a useful means to conceptualise the attitudes that need to be adopted to foster responsible AI in policing, and to assess the degree to which shifts towards these attitudes have been made so far. Firstly, Vallor states that responsibility needs to be accepted. The NPCC can be seen to be taking steps to acknowledge its responsibilities through the publication of a covenant for using AI that includes ethical principles and mechanisms for governance. It can also be seen to understand responsibility as relational by emphasising the importance of transparency to secure public trust and confidence. The efforts to address potential biases in facial recognition technologies can be seen to attend to vulnerability but concerns remain over data protection and privacy intrusion as well as biases and feedback loops in predictive policing systems, Similarly, sustainability remains an issue, as seen in the ceased deployment of interventions such as HART and known problems around the retention of staff in policing.

Trustworthy and useful tools for mobile phone extraction: exploring responsible ai in policing

Our ongoing project Trustworthy and Useful Tools for Mobile Phone Extraction investigates digital tools in a particular area of policing. When police are investigating a crime, they may request (or compel) a suspect, witness or complainant to hand over their mobile phone. Data from the phone is collected and analysed. This process, known as mobile phone extraction (MPE), can identify important evidence to resolve cases. However, since modern phones typically hold very large amounts of data, processes of analysis can be slow and efficient. Failures to properly analyse data have been associated with the collapse of court cases, e.g. Digital tools to assist with analysis do exist but can be inaccessible due to cost and/or technical complexity. Additionally, collecting data can pose privacy risks. Until recently, the default was for all data on a phone to be extracted; this meant that large amounts of personal data might become visible to the police, defence and others across the criminal justice system, even if it is not relevant to the case. As highlighted by civil rights organisations and the Information Commissioner's Office, phone owners are often fearful of non-relevant data being seen and potentially used to undermine them. Even with new guidance stating that police should conduct a more selective extraction, especially when the phone owner is a witness or complainant, concerns remain over the handling of third-party data.

These problems have affected public confidence in MPE, in particular in the conduct of cases where phone owners may be vulnerable. Our project explores the capacity for trustworthy digital tools to address the problems by making MPE practices more efficient and more respectful of privacy. Our project is guided by a responsible approach and involves a series of activities including the development of a mobile phone extraction tool, RIME (Responsible Investigation of Mobile Environments). Complying with the new guidance, RIME attends to data privacy; it is designed to expose a subset of the contents of a phone for investigation, rather than a complete capture of all data on the device. The data subset can be filtered by criteria such as time and contact names for targeted, and efficient, analysis. The continuing development of RIME has allowed us to gauge the extent to which AI can help to address the problems associated with MPE. In the remainder of this section, we illustrate this with two examples.

Understanding limits to the potential for AI-driven features in MPE tools

Data availability limits the kinds of AI features that can be embedded in MPE tools. Ethical and legal considerations inhibit the collection of large personal mobile datasets for research purposes and synthetic data may lack quality. Consequently, it can be difficult to develop AI features that can make robust inferences since they are not trained on suitable data.

For example, we developed a pie chart feature for RIME, which categorises messages within a mobile phone dataset according to criteria such as ‘potential argumentative nature’ and ‘of evidentiary interest.’ This is intended to capture references to potential illegal activities and other terminology that might be useful when investigating a case. A machine learning model, a CNN text classifier, categorised the messages. However, when it came to training this model, the data used was problematic. The model, when trained, will pick up on positives based on its training dataset, but finding a dataset that captures unique nuances in language and naturalistic terminology is difficult. In the context of 'evidentiary interest,' people rarely mention crimes explicitly in messages, instead using slang or emojis. Slang can vary significantly by region, and favouring one region over another can introduce undesirable bias. Dataset creation is therefore highly complex and curating such a dataset takes time and research to reach suitable levels of specificity.

Despite the caution noted above, AI can offer significant benefits when it is used in a way that avoids the risks of implicit bias. In the development of RIME we have prioritised using well-tested AI techniques ahead of the most recent innovations. We have also chosen traditional, non-AI, techniques where they are shown to be quicker and/or more accurate. An example is RIME's pseudonymisation feature. When looking at a data subset, a user can select for real names and phone numbers to be replaced with autogenerated, but indexed, alternatives. If when the individual concerned becomes a person of interest

in the case, the pseudonymisation can be removed. This is a very useful feature to protect third-party privacy (which attends to vulnerability) and is partially AI-driven. RIME uses a Named Entity Recognition (NER) model to identify names, and traditional techniques to identify phone numbers and email addresses. RIME maps identified Personal Identifiable Information (PII) to a token, so the same anonymised token is re-used for the same PII. This works well for phone numbers and emails as they can always be canonicalised but is a challenge for names (e.g. 'Bob', 'B', and 'Robert' may all refer to the same person). We experimented with using large language models (LLM) to identify PII, but NER gave better results for the sizes of LLM that could be run locally.

The potential impact of AI-driven tools is contingent on the context in which they are used

Our stakeholder engagement work has revealed socio-organisational dynamics that influence how MPE practices are conducted. For instance, even when the police prefer a selective extraction, the defence and/or the Crown Prosecution Service (CPS) may seek a full one. This can lead to a full extraction being undertaken regardless of the existence of tools to support selective extraction. As another example, police staff can find the outputs of MPE tools very difficult to work with. Tools produce a report that captures the extracted data file formats such as pdf, excel or .ufd. These can be analysed manually or within the tools themselves. Given the amounts of data typically involved, these files can be extremely large. Consequently, police staff reviewing/analysing phone data as part of the investigation of cases find can them very difficult to interact with – particularly given that they may be working on relatively old and slow computers. When talking to stakeholders, a common request we hear is for RIME data reports to be in a more accessible size and format. So, we are aware there is a need to balance this kind request alongside exploration of state-of-the-art AI techniques.

Another important dynamic is the lack of trust around MPE. This is something we attend to in the development of RIME, prioritising openness and replicability. A dataset collected within RIME can be made available to third parties for analysis using their own tools. This allows the prosecution and defence, or even an independent authority, to conduct their own analysis of a dataset. In addition, RIME is an open-source tool, with the code publicly available on the University of Nottingham Horizon Digital Economy Github account. This is another transparency and trustworthiness measure since the source code is open to inspection. We also hope that it will be a measure for sustainability whereby interested community members support its ongoing development and add new features. This is particularly important as mobile phone technologies are always changing; it is necessary to ongoingly extend RIME's plugins to read data stored in previously unsupported formats or data generated by the latest mobile apps.

Conclusion

The deployment of AI in policing presents opportunities and risks. These relate to the features of AI-driven technologies themselves and to wider socio-organisational dynamics. A responsible approach to AI in policing requires attention to both these factors. Our project work highlights that the inclusion of AI in tools for mobile phone extraction needs to be carefully researched and scoped. It is important to consider the context in which tools will be used in order to maximise their usefulness and trustworthiness. Whilst AI undoubtedly offers benefits, it cannot alone address all the problematic issues associated with contemporary policing. It is important for a responsible approach to acknowledge this and not over-state the promise of AI.

Acknowledgments

We are grateful to all the project participants who have contributed to this study. The Trustworthy and Useful Tools for Mobile Phone Extraction project is funded by a pump prime award from the UKRI Trustworthy Autonomous Systems Hub (EP/V00784X/1). The initial development of RIME was funded by another UKRI Trustworthy Autonomous Systems Hub award, Digital Forensics Platform. Due to the ethical restrictions, supporting data in the research study cannot be made available.

Real specialists.
Real results.

Start your journey to a straighter smile with braces or Invisalign clear aligners at Lane Cove Orthodontics

OUR ORTHODONTISTS ARE SPECIALISTS IN THEIR FIELD

DR TERIKO REX

- Specialist Orthodontist with over 20 years experience
- Honorary Clinical Educator in Orthodontics at the University of Sydney School of Dentistry

TREATMENT FOR ADULTS, TEENS AND CHILDREN FROM **$50** PER WEEK

CALL 02 9427 8088 VISIT lanecoveorthodontics.com.au

lane cove orthodontics

Or contact us at your nearest practice location.

Hunters Hill Orthodontics 02 8054 2722
Port Macquarie Orthodontics 02 6583 8425
Taree Orthodontics 02 6551 2601

Proudly Supporting Our Police Members

I'M ON A MISSION TO SAVE LIVES.

Red25 is uniting with organisations like yours to achieve 25% of Australia's blood donations.

Call 1300 886 524 for more information.

RED25 UNITE TO SAVE LIVES

Australian Red Cross BLOOD SERVICE

ROY BUTLER MP

INDEPENDENT MEMBER FOR BARWON

Thank you to all the Police Officers and their families for the sacrifices you make. You dedicate your lives to ensuring we live safely and for that I say thank you.

BROKEN HILL
1/142 ARGENT STREET
PH (08) 8087 3315

COBAR
11 BARTON STREET
PH (02) 6836 3722

NARRABRI
60 MAITLAND STREET
PH (02) 6792 1422

barwon@parliament.nsw.gov.au www.roybutler.com.au

To all NSW Police Force Officers, who serve Gloucester, Stroud, Dungog, Maitland, Cessnock, Singleton, Muswellbrook, Scone, Murrurundi & Merriwa.

Thank you for your service

Dave Layzell MP
Member for Upper Hunter

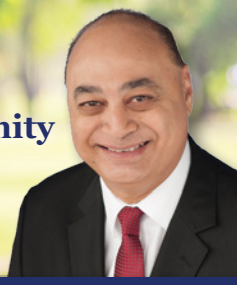
Authorised by Dave Layzell MP, 94 John Street Singleton NSW 2330 - Funded using Parliamentary entitlements.

R U OK?™

A conversation could change a life.

TO OUR POLICE OFFICERS & THEIR FAMILIES

Thank you for your hard work, sacrifice and dedication to the community



Edmond Atalla MP
MEMBER FOR MOUNT DRUITT

Phone: (02) 9625 6770 Email: mountdruitt@parliament.nsw.gov.au
Office: Suite 201, Westfield Shoppingtown, Carlisle Avenue, Mt Druitt

Authorised by Edmond Atalla MP, Suite 201 Westfield Shoppingtown, Mount Druitt funded using parliamentary entitlements.

ACLU Opposes AG Yost, Cleveland Police on Use of Facial Recognition in Murder Case

April 7, 2025

LUCAS DAPRILE

cleveland.com

CLEVELAND, Ohio - A civil rights group and defense attorneys have formally opposed Cleveland police's use of artificial intelligence to justify a search warrant in a homicide case.

On Friday, the American Civil Liberties Union and the National Association of Criminal Defense Lawyers filed a friend-of-the-court brief in a potentially precedent-setting case before the 8th Ohio District Court of Appeals in Cleveland.

The briefs are statements written by people or groups who are not directly involved in a case but will be affected by its outcome. Ohio Attorney General Dave Yost's office filed its own friend-of-the-court briefing last month, siding with the Cleveland Division of Police.

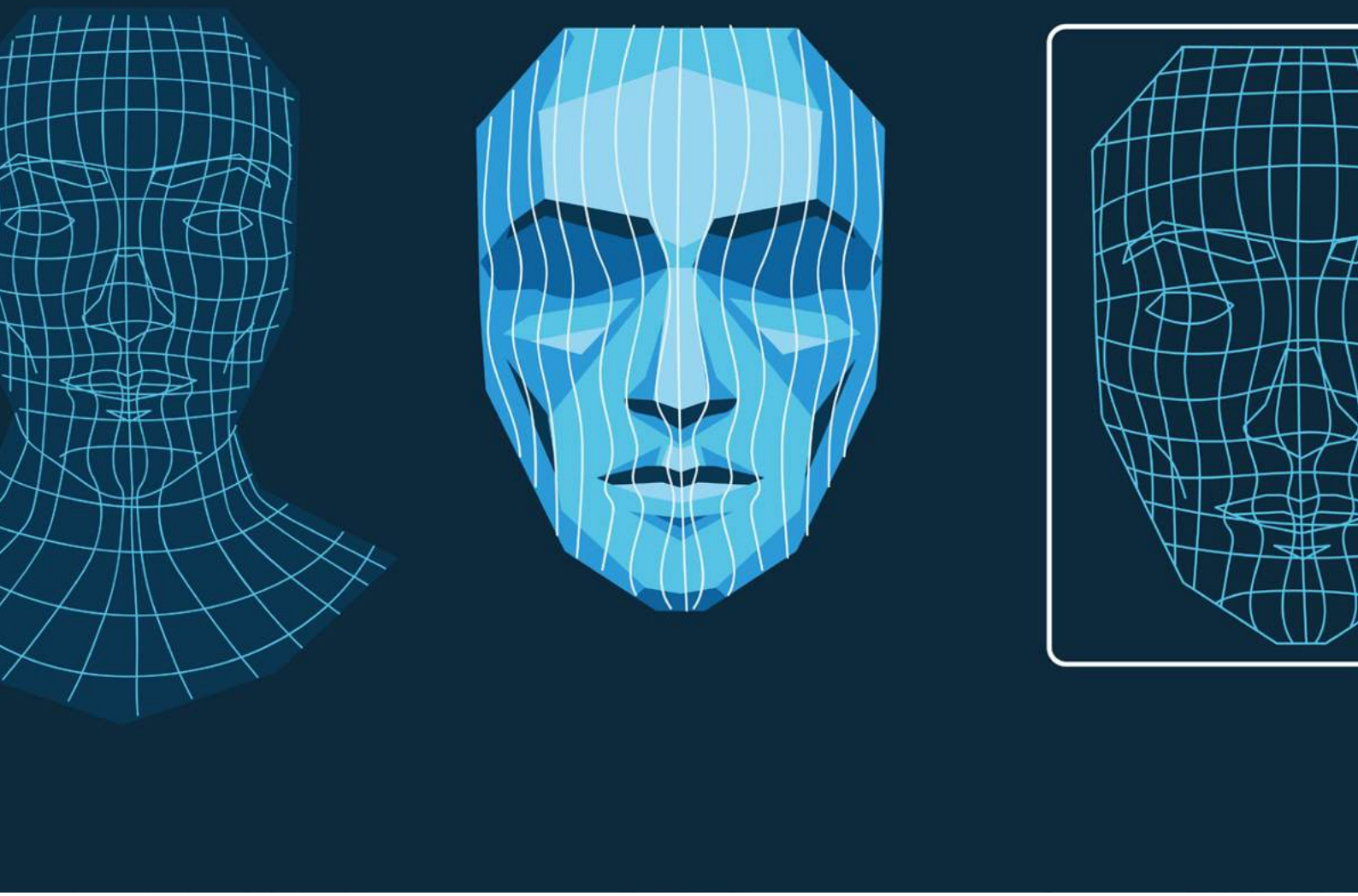
The filings involve the case of Qeyeon Tolbert, who was accused of robbing and killing Blake Story on Valentine's Day 2024. Cleveland police used facial recognition, powered by AI, as part of its justification for a search warrant of Tolbert's house, which uncovered what police say was the murder weapon.

Tolbert's attorneys, Brian Fallon and Daniel Tirfegnehu, noted police did not tell a judge they used the technology when officers sought a search warrant of Tolbert's home. The maker of the technology says the AI program must only be used to generate leads, and it is not supposed to be used in court filings.

Though the murder was caught on surveillance video, neither police nor the facial recognition program could identify the killer based on that alone. The facial match that pointed police toward Tolbert came from a video in a convenience store just a couple blocks from his house taken six days after the murder.

Judge Richard McMonagle, who served as a visiting jurist in Cuyahoga County Common Pleas Court, sided with Tolbert's attorneys, who argued the results of the search warrant should be excluded from the trial.

The ACLU and the defense attorneys group argue facial recognition programs are unreliable and especially biased against people who are not white and who are young. Tolbert, 23, is Black.



The groups also argue a Cleveland police detective misled a judge when he applied for a search warrant by not mentioning the use of facial recognition.

"When police hide their use of fundamentally unreliable face recognition technology from judges, it undermines the ability of courts to ensure protection of our constitutional rights," Nathan Freed Wessler of the ACLU said in a statement.

Police departments throughout Ohio use facial recognition technology in their investigations. But Cleveland's police department has no policy governing its use nor does it train detectives on how to use it, cleveland.com and The Plain Dealer has reported.

During the March Cleveland Community Police Commission meeting, a reporter asked co-Chair John Adams if the board has any plans to create a policy governing the department's use of AI and facial recognition.

While he expressed interest in regulating the technology and concern about its existing use, Adams said the board has multiple other priorities it needs to address. The commission oversees policy matters in the department as part of a federal consent decree with the U.S. Justice Department.

"They shouldn't be doing things in an official capacity without a policy in place," Adams said of Cleveland police's use of AI.

The lack of policy, training and transparency when facial recognition is used in an investigation is a recipe for disaster, Tolbert's attorneys wrote in court documents.

"This is equivalent to giving hand grenades to children without any instructions or supervision," Tolbert's attorneys said in court documents. "What could go wrong?"

Similar legal feuds over the use of facial recognition are playing out across the country between police and defense attorneys, the groups said in their brief.

Since AI and facial recognition are controversial and emerging fields, few judicial decisions exist regarding the usage. This raises the stakes of the Tolbert case, because an appellate court's ruling is likely to set precedent for future policing practices.

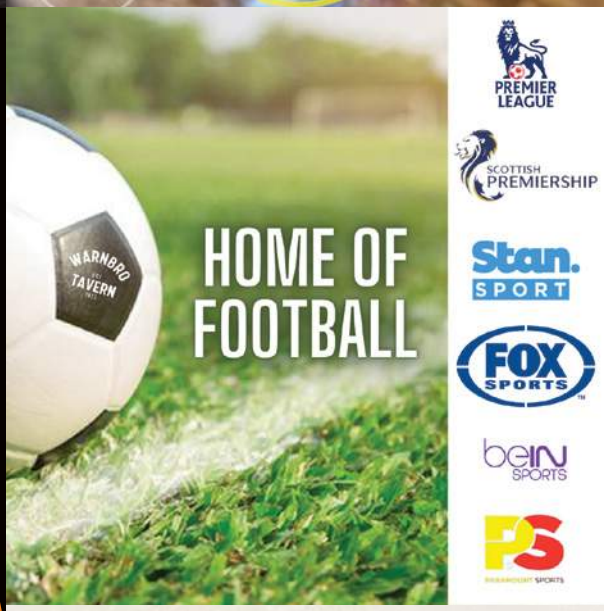
Last month, Yost's office filed his own friend-of-the-court briefing, arguing police did enough additional detective work to justify the search warrant even without facial recognition, which he says is highly accurate.

"The question for this court is whether the state can tell the jury the truth that the police found the gun used to shoot Story and other incriminating evidence in Tolbert's apartment," Yost's office wrote in a filing last month. "The answer should be 'yes.'"

Courts in Minnesota, New Jersey and Michigan have also heard arguments related to the constitutional and technological validity of facial recognition.

"The importance of this issue reaches far beyond this case," the ACLU and the defense attorneys association argued in their filing.

Dine Differently



The Warnbro Tavern is your go-to local spot, where friends and family gather for memorable meals and refreshing drinks. Whether you're popping in for a beer or a glass of wine or settling in for a feast in our restaurant, we're perfectly nestled in the heart of Warnbro, making us an ideal local venue for your evening.

Enjoy our live music and entertainment as you indulge in last drinks.
At The Warnbro Tavern, we're your prime destination for great times and great tastes.

10% Emergency Service Member **DISCOUNT!**

Reserve a table now at
www.warnbrotavern.com.au
or phone us on **(08) 9593 1597**

7 Hokin St Warnbro WA 6169

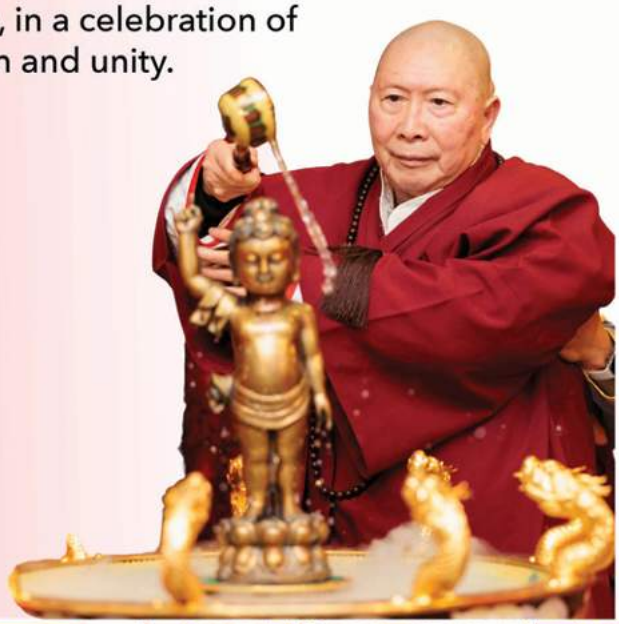
Proudly Supporting Our Police Members Locally

the ACADEMY NEWS
2025-05

EVENT RECAP

Celebrating the 2569th Birthday of the Holy Sakyamuni Buddha

On Sunday 4 May 2025, community leaders, religious representatives, and friends gathered to commemorate and celebrate the most sacred day on the Buddhist calendar - Buddha's Birthday (known as the Bathing Buddha Holy Ceremony), in a celebration of compassion and unity.



Guests participated in the solemn and traditional rituals, reenacting the sacred moment of Prince Siddhartha's arrival into the world.

The holy ceremony was an opportunity for attendees to practise realising Buddhahood in the current lifetime.

No matter the faith or ethinicity, we walk the path of unity, solidarity and harmony together.

more about us

Light of Tasmania on WeChat

The World of Jin Gang Dhyana

Academy Website

Academy Facebook Page

get in touch

facebook us
enquiry form on our website
email at contact@tascbaa.org