Policinginsight

FEATURE:

Compliance challenges: Testing artificial intelligence surveillance monitoring tools in the public domain

3rd July 2024 | Andrew Staniforth | Policing Insight

Picture © Gorodenkoff / Shutterstock

With police making increasing use of artificial intelligence (AI) in crime fighting – including facial recognition – a new compliance framework drawn up by the EU's PRECRISIS project will help to ensure that the testing of AI surveillance tools in the public domain will meet all the necessary ethical, legal and security guidance and legislation, as Policing Insight's Andrew Staniforth reports.

The use and application of artifical intelligence (AI) in policing tools remains a critical concern for those seeking to prevent the erosion of civil liberties.

The recently published thematic report by Policing Insight – *Facing the future: the rise of facial recognition in policing* – provides evidence of the mainstreaming of such AI-driven technologies, which fuels the highly divisive debate about the police use of facial recognition (FR).

> *"In a significant development of the use of AI in policing, the European Parliament had called for a full ban on FR systems, but softened its red line in response to the demands of countries such as France."*

In a significant development of the use of AI in policing, the European Parliament had called for a full ban on FR systems, but softened its red line in response to the demands of countries such as France.

Paris, which has suffered a series of deadly terrorist attacks over years, was among the European capitals that pushed hardest for exceptions that would allow wider FR use.

Police and security forces in Paris have even announced the use of AI to monitor suspicious activity during the 2024 Olympic Games to be held next month.

Ethics by design

It is being increasingly recognised by security policymakers – including those responsible for delivering a safe and secure Olympiad in Paris – that new approaches are needed to balance security provision with civil liberties, but which achieves this balance by preserving the need for policing to rigorously test and trial new and emerging AI tools, techniques and technologies in the public domain.

The real-time live examination of new AI tools in the public sphere serves to determine the efficacy of such tools within a controlled environment, being designed to deliver improvements in security for all in society.

The alternative to real-world testing is the use of simulated scenarios and data, none of which provide anywhere near the stress-testing rigour of live tests that readily expose fault lines and vulnerabilities.

> *"All engaged in the research and development of new AI Tools when collecting data should therefore collect only the data that they need to meet their research objectives; the fact that some data is publicly available does not mean that there are no limits to its use."*

Over recent years, security-related research and innovation activities have promoted an ethics-by-design approach, which seeks to embed privacy, ethics, and security compliance by design and default to ensure live testing where real-time data can be used.

Data security, data protection and information compliance are a central issue for research ethics in the UK and across Europe. The right to data protection is enshrined in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the European Union, which give effect to individuals' right to privacy by providing them with control over the way information about them is collected and used.

The General Data Protection Regulation (GDPR) states that data processing must be lawful, fair, and transparent, and that it should involve only data that is necessary and proportionate to achieve the specific task or purpose for which it is being collected.

All engaged in the research and development of new AI tools when collecting data should therefore collect only the data that they need to meet their research objectives; the fact that some data is publicly available does not mean that there are no limits to its use.

Data protection imposes obligations on researchers and developers to provide research subjects with detailed information about what will happen to the personal data that they collect.

It also requires the organisations processing the data to specify the purpose for which they do so, ensuring the data is properly protected, minimised, and destroyed when no longer needed for the specified research purpose. The failure to protect personal data may also have serious legal, reputational, and financial consequences for the data controller and/or processor.

For UK policing, the application and use of AI in systems also needs to comply with the AI Police Covenant endorsed by the National Police Chiefs' Council (NPCC) last year. The Covenant outlines a set of principles that police forces have agreed will define how they use AI in their business, ensuring it's use is lawful, transparent, explainable, responsible, accountable, and robust application.

Pilot testing

Recognising compliance challenges when testing AI tools and technologies, the PRECRISISproject (*PRotECting public spaces thRough Integrated Smarter Innovative Security*), funded by the EU's Internal Security Fund, has designed a unique Compliance Framework.

The aim of the PRECRISIS project is to enhance the situational awareness and investigative capability of law enforcement agencies through the development of an AI-based surveillance monitoring platform to better protect public spaces from terror attacks.

To further develop the AI platform, three pilot tests will be conducted later this year, and the framework comprises self-assessment questionnaires and documents that mirror the reflective processes of compliance each of researchers engages in.

The self-assessment questionnaires are designed to prompt each researcher to evaluate how their internal procedures match legal, ethical and security requirements. To do

this, all researchers must engage with their Data Protection Office which forms an integral part of the PRECRISIS project's obligations on research integrity, accountability, and transparency.

Additional documents within the framework are designed to record compliance, and there are other documents on agreements on data sharing and processing arrangements involving two or more partners, offering a full package and pathway to compliance.

The compliance documents of the framework have three sections relating to the questions researchers must ask themselves to understand how they are complying with fundamental rights, data protection and secure information processing, as well as ethical research and data management.

This provides a comprehensive structure to ensure compliance is both thoroughly considered and achieved throughout the full programme of development and testing.

Compliance checks

It's important for all engaged in the research, development and testing of AI surveillance monitoring tools and FR systems that the PRECRISIS Compliance Framework process needs to be understood as a whole, and foundational values and principles are recognised as complementary and inter-related.

> *"The provisions of the Act will categorise the use and application of AI surveillance monitoring tools for public use as 'high-risk', requiring greater controls, independent scrutiny and oversight."*

Nothing in the PRECRISIS Compliance Framework may be interpreted as replacing, altering or otherwise prejudicing individual and organisational obligations or rights under international law, or as for any state, other political, economic, or social actors, group, or person to engage in any activity or perform any act contrary to human rights and fundamental freedoms.

Moreover, the challenge to comply with a growing library of fundamental rights and freedoms legislature on the statute books will be amplified by the introduction of the new EU AI Act.

The provisions of the Act will categorise the use and application of AI surveillance monitoring tools for public use as 'high-risk', requiring greater controls, independent scrutiny and oversight.

To prepare to meet these new provisions, the compliance framework developed by PRECRISIS – which is now being adopted and adapted for use across multiple security research and innovation projects which are developing AI tools – will best serve the efficacy of the security community conducting important tests in the public domain, while safeguarding and maintaining fundamental rights, freedoms and civil liberties for all.

Link to article in Policing Insight: https://policinginsight.com/feature/compliance-challenges-testing-artificial-intelligence-surveillance-monitoring-tools-in-the-public-domain/

Andrew Staniforth *is Director of Innovation at SAHER (Europe), a security research consultancy operating at a global level, supporting police forces and private sector organisations to identify and implement innovative security technologies to maximise impact. He is the Project Coordinator of the PRECRISIS project, funded by the ISFP-2022-TFI-AG-PROTECT-02-101100539. As a former Police Counter-Terrorism Detective and Intelligence Officer, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch.* Andy@saher-eu.com

PRECRISIS is funded by the European Union Internal Security Fund (ISFP-2022-TFI-AG-PROTECT-02-101100539)