Written evidence submitted by Milestone Systems (GAI0132)

Facial recognition matches an individual's facial features with existing records to gauge similarity. It can be broken down into two broad categories. Live facial recognition allows an image captured by a live camera to be instantly compared with police watchlists. Retrospective facial recognition matches images after an event, such as identifying a suspect who has fled a crime scene.

If used irresponsibly, this technology may lead to privacy breaches, human rights infringements, wrongful arrests, and discrimination. However, through the responsible development, deployment, and regulation of facial recognition, the technology can serve communities without compromising public trust, a vital part of police work.

Milestone Systems, Europe's largest provider of video management software – which powers video security systems – is leading the charge for the responsible deployment of powerful technologies such as AI-powered video surveillance and facial recognition. We propose the following policies to support the UK's use of video surveillance technology to respect privacy, counter bias, and address other concerns whilst providing security for citizens.

Avoiding bias

Facial recognition is not just used for authentication or access. It is a critical tool for law enforcement and surveillance systems at large. By checking biometric identifiers against national and international databases (e.g. Interpol's Red Notices or Missing Persons List), it can help fight fraud, find missing people, and catch serious criminals.

According to Interpol, around 1,500 terrorists, criminals and missing people have been identified since the launch of their facial recognition system in 2016. The London Metropolitan Police's latest data shows the technology has been effective in freeing up resources for the police and benefitting public safety.

Yet there are challenges and limitations to the technology. False positives and misidentification can infringe innocent people's freedom, ultimately hampering public trust in its use and benefits to citizens. Facial recognition technology has been known particularly to misidentify people of colour.

Recommendation: To avoid bias and ensure facial regulation is used responsibly, law enforcement should adopt a 'four eyes principle'. This means at least two authorised individuals should verify decisions made by AI and use human review processes to check the accuracy of algorithms. This will help ensure fair use and prevent wrongful identification or punishment. Eliminating bias in the algorithms also requires the use of comprehensive data sets to ensure better representation across parameters such as ethnicity, disability, and gender.

Regulating use of biometrics in public spaces

The EU's AI Act outlines a series of safeguards for the use of biometric identification systems by law enforcement in public space. These include a full ban on biometric identification except in exhaustively listed and narrowly defined situations, such as a targeted search of a missing person or preventing a terrorist attack. Meanwhile, the UK has no specific regulation of biometric identification or even the use of live facial recognition in investigating minor crimes.

The threshold for the use of video surveillance and live facial recognition technology can be set anywhere from solving petty theft, disorderly conduct, or traffic misdemeanours, to catching wanted criminals or preventing terrorist attacks. Where the threshold is set is ultimately a political decision, but setting a threshold is important for ensuring public trust in the technology being used to the benefit of citizens.

Recommendation: We advocate clear rules for the use of biometric identification and live facial recognition. Regulation should aim for harmonized standards for how and when it is appropriate to use this technology in public spaces. These standards should address concerns like consent, data protection, and the specific circumstances under which live facial recognition measures are justifiable.

Data protection

Biometrics have emerged as a sophisticated means of personal authentication. Remote biometric identification – mainly facial recognition technology using AI-enabled video surveillance – leverage unique individual facial features and iris configurations for the swift and secure identification of individuals.

Such biometrics can also be used to identify people who have acted illegally and can save time and resources for domestic security services. However, there are understandable privacy concerns, such as the use of broader surveillance for tracking public protests and infringing on the right to peaceful assembly. Collecting and handling personal information must therefore be guided and restricted by a clear data protection framework. To ensure privacy and counter risks of data breaches and misuse, clear rules for storage and data security are needed.

Recommendation: Prioritize the duration of storage and implementation of security measures such as encryption. Regulation must mandate explicit, informed consent for the collection of biometric data for personal identification, along with transparency about how the data will be used, stored, and protected. Law enforcement agencies typically determine the need for video footage for retrospective use within a few days. To safeguard privacy, prevent potential data breaches or misuse, and considering the cost and energy intensity of video data storage, we recommend limiting the storage of video footage to a maximum of 30 days.

Ethical AI development

AI-powered video surveillance enables computers to understand the visual world. It excels in automating tasks that are labour-intensive, mundane, or those that surpass human visual capabilities.

However, the data used to train these models must be acquired ethically. Companies like Clearview AI have been punished for training their facial recognition algorithms with non-ethically sourced data, i.e., acquired without consent through web-scraping. Other sites, like PimEyes.com, and FaceCheck.ID, have similar features obtained from web-scraping using facial recognition technology without consent.

Recommendation: The UK should require robust and frequent computer vision training for all artificial intelligence technology overlayed onto video surveillance. Authorities should create audit systems where developers/providers of AI systems (including facial recognition) can be audited for compliance by national governing boards with regards to how data is obtained, used for training, and deployed.

24 April 2024