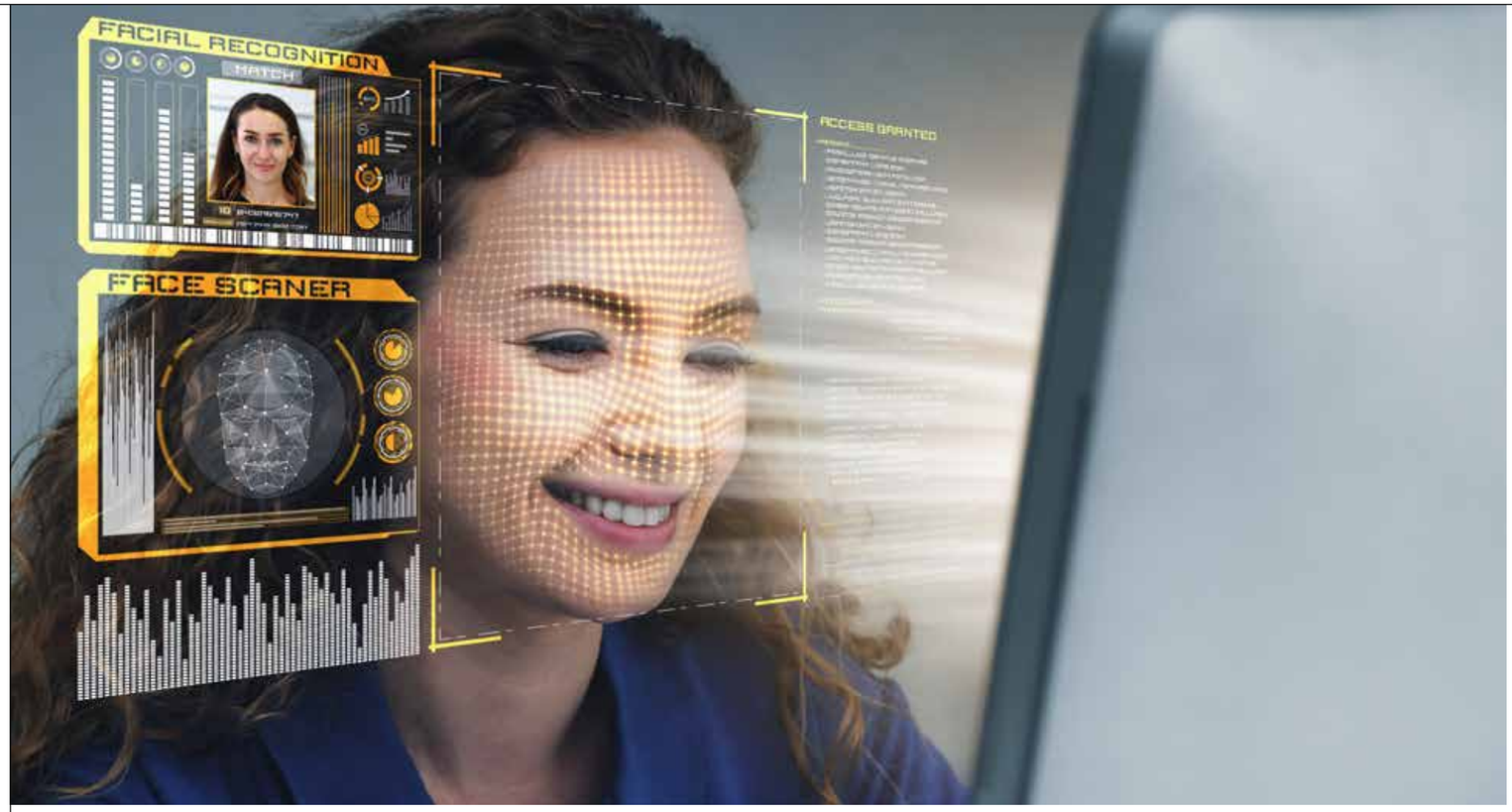

Picture credit: AdobeStock

LOOKING FORWARD

Sam Stockwell *and* Megan Hughes *explore future Biometric trends for policing and law enforcement*

This article explores how future developments in biometric technology could provide new opportunities for policing and law enforcement agencies. As the integration of AI into biometric systems expands the types of data and applications available, organisations using this technology could, in the future, pre-empt whether someone is concealing a weapon or conducting hostile reconnaissance in crowded areas. Other trends will also see smaller biometric devices fitted onto drones and the ability to obscure biometric data samples, which are compromised through unauthorised access. However, with many of these developments involving uncertainty over their scientific validity, it will be critical for operators to ensure that novel systems used are robustly tested and audited. Failure to do so risks causing unintended harm to the public and eroding confidence in the potential benefits of this technology.

Historically, biometrics has involved the use of physical samples (eg hair follicles) to identify a specific individual or verify their identity. Yet the integration of Artificial Intelligence (AI) into biometric systems over the last decade has transformed the nature of the technology. Today, biometric systems can process two types of data. The first is *physiological* data, or measurements of someone's physical characteristics (eg DNA, fingerprints or facial features). The second is *behavioural* data, or measurements of behavioural characteristics (eg facial expressions, walking style or vocal tone) which are collected over a period of time to identify patterns.

AI allows the capture of biometric samples from individuals without needing their direct involvement

Traditional biometric systems obtained physical samples from an individual (eg a fingerprint mark) that human experts analysed to extract unique features (eg fingerprint ridges). This was a time-consuming process which could be prone to error, due to poor quality samples or human factors such as fatigue. In contrast, AI systems extract and compare unique features more quickly, accurately, securely and against a larger database of other features. In addition, AI now allows the capture of biometric samples from individuals without needing the *direct* involvement of the subject, such as with remote facial recognition (FR) systems, which process images of individual faces.

Biometric systems convert the relevant features extracted from a sample into a 'biometric template', which stores the necessary information in a convenient form for comparison. The term 'biometric data' is often reserved to refer to these resultant templates, rather than the initial sample. The process of converting a sample (which may be physical or digital) into a template is not necessarily immediate and may itself be subject to errors and uncertainties. The probabilistic nature of statistical analysis, inherent to biometric processing, means there is a risk of false positives and false negatives.

AI has also expanded the range of biometric data and system types available. New systems have been developed that use statistical correlations between biometric characteristics and traits, with the aim of either classifying individuals into different demographic categories (eg age or ethnicity) or to infer emotions and psychological states. These systems have proved controversial due to issues over their scientific validity and ethical implications. This includes uncertainty over whether systems can accurately infer emotions from data such as facial expressions, or the potential discriminatory implications of labelling people according to categories like race or gender.

There are several well-established biometric data types which have been used to uniquely verify or identify individuals (DNA, face, fingerprint, voice, iris etc). Nevertheless, the emergence of new biometric systems that rely increasingly on behavioural characteristics is leading to interest in other data types. These include keystrokes, gait (walking pattern), facial expressions and gaze. Some characteristics (eg facial expressions) are particularly contentious in terms of scientific validity. There is therefore a need for further research to determine both the validity and benefits of emerging biometric characteristics.

In light of these developments, it is important to move beyond conventional notions of biometric systems and towards a more expansive definition that factors in the transformative effect AI has played. As such, we argue that biometric systems should now be understood as: "Computer-based systems which collect and process physiological data or behavioural data. This data can be used for numerous purposes, for instance to identify an individual, verify their identity, categorise them into different groups, or make inferences about their psychological or emotional states."

Our proposed new definition goes beyond traditional definitions of biometric technologies which focused only on the use of biometric data for unique identification or verification.

Despite the level of uncertainty surrounding new biometric trends, there are still several potential future opportunities to enhance public safety using this technology.

One area which will see significant change in the next 5-10 years is biometric formats. Border security may benefit from frictionless biometric methods owing to improved speed and convenience of fingerprint verification processes, in a similar manner to current FR systems. Policing operators using biometric systems to identify wanted suspects in crowded places could also gain enhanced sensor accuracy through multimodal processes, where several biometric data types are used to inform outputs (eg fingerprints and face). As new generative AI models increase the likelihood of sophisticated phishing and malware attacks, the ability to protect compromised data samples with cancellable biometrics will add an extra layer of security for biometric databases owned by law enforcement agencies.

THERE IS A REAL RISK OF FALSE POSITIVES AND FALSE NEGATIVES WITH BIOMETRIC PROCESSING

Alongside new biometric formats, there will be improvements in system design and performance capabilities that open up benefits for policing and law enforcement. As in other technical fields, increasing hardware miniaturisation could enable heightened portability, with biometric systems being integrated into body-worn cameras and drones. Further advancements in deep learning techniques may improve FR deployments in challenging conditions, such as reduced visibility and with low-resolution cameras, as well as with masked faces. This could allow for more flexible deployment of the technology, without compromising accuracy.

Finally, there is also a range of future applications for policing and law enforcement agencies. Three-dimensional (3D) FR could be useful for identifying or verifying a known individual. Future gait systems could indicate whether someone is concealing a weapon, while gaze estimation (which predicts where a person is looking) could be used to monitor suspicious behaviour; such as to detect whether someone is conducting hostile reconnaissance in a busy public space.

As debates continue over the merits of using new biometric systems to tackle crime, particularly live FR, it is also important to consider the ethical implications of police and law enforcement agencies choosing *not* to use them. This is especially if they are shown to better protect vulnerable individuals compared with existing tools. Voice recognition technology, in particular, is arguably under utilised for public safety purposes. INTERPOL's global voice database (SiiP) is its third-largest biometric database,

demonstrating the utility of this modality. More research into how the UK's policing and law enforcement bodies could better utilise voice recognition systems will therefore be beneficial.

There are clearly exciting avenues for policing and law enforcement to explore in relation to biometrics out to 2030. However, it is necessary to raise caution against the notion that these potential trends will offer a 'silver bullet' in protecting the public more effectively. Although they hold promise and are worthy of further consideration, many of the cited developments (for example gaze estimation) remain untested in relation to their scientific validity, intrusiveness or impact on human rights.

In our nationally representative survey with 662 members of the UK population, respondents repeatedly voiced concerns over emerging biometric systems. In particular, participants highlighted that emotion recognition technology could misinterpret the facial expressions of neurodivergent individuals or would be unable to discern between cultural variations in how individuals express their emotions. Especially within a law enforcement context, the implications of this can be significant; similar technologies in the form of polygraphs are being used by UK police forces to interview individuals arrested on suspicion of child sex offences or as a condition of release in certain domestic abuse cases.

Among our various policy recommendations, there is a need for scientific measurement and standards organisations to establish mandatory requirements that must be met in the design, deployment and evaluation of future biometric systems. These should include minimum error rates, demographic fairness requirements and operator considerations (eg when a human can contradict decisions made if they have doubts over the output). These factors should also be consistent across all environmental conditions.

Similarly, the same organisations should seek to test any early-stage biometric systems where there is a lack of a consensus on their evidence base. If such assessments cannot establish appropriate assurance, the system in question should be prohibited for use.

To end on a more positive note, the survey also revealed that the majority of the UK public are marginally optimistic (53 percent) about the benefits that biometrics could bring to society. Yet as this article has shown, ensuring sufficient testing and auditing safeguards are in place before using any new biometric systems will be an important step towards consolidating such public confidence ●

Sam Stockwell is a Research Associate at the Centre for Emerging Technology and Security (CETaS). His research interests focus on the intersection between national security and the online domain, particularly in relation to countering radicalisation and violent extremism through both policy and technical solutions.

Megan Hughes is a Research Associate at the Centre for Emerging Technology and Security (CETaS). Her research explores the impact of AI on intelligence tradecraft and the information environment.

Format trend	Summary
Frictionless biometrics	Where little (or no) physical contact or pausing is required to gather extensive biometric data, such as gaze tracking or fingerprint recognition at a distance via cameras.
Multi-modal biometrics	These systems collect data from several biometric modalities (such as keystroke analysis and fingerprint recognition) or use a single modality to extract multiple forms of data (eg extracting gaze estimation and pupil diameter data from a single eye image).
Cancellable biometrics	Biometric templates are transformed in such a way that, if they are compromised, the original feature cannot be determined. A new version would then need to be reissued (akin to resetting a password).

Border security may benefit from frictionless biometric methods owing to improved speed and convenience of fingerprint verification

Picture credit: AdobeStock