INVESTIGATION · SCIENTIFIC AND TECHNICAL INVESTIGATION

Emerging Biometric and Sensor Technologies in Investigation

Face recognition, DNA phenotyping, genetic genealogy, wearable devices and networked sensors are giving investigators new ways to identify people and reconstruct events. This article explains what these technologies can do, their accuracy limits, the legal and ethical concerns they raise, and the safeguards needed.

ModQu research article · 845 words · 9 references (APA 7th edition)

Biometrics are measurable physical or behavioural characteristics, such as fingerprints, faces, irises, voices and DNA, that can be used to recognise people. Sensors record the physical world: cameras, microphones, location receivers, accelerometers and heart-rate monitors. Both are spreading rapidly, built into phones, cars, buildings, streets and the devices people wear. For investigators, they offer new ways to identify people and reconstruct events. They also raise serious questions of accuracy, bias and privacy. This article reviews the main emerging technologies and the safeguards they require.

How biometric recognition works

A biometric system captures a sample, extracts features and compares them with stored templates, producing a similarity score. A match is declared if the score passes a threshold. Jain et al. (2004) explain that every biometric system makes two kinds of error: false matches, in which different people are judged the same, and false non-matches, in which the same person is not recognised. Changing the threshold trades one error for the other. In investigations, false matches are the more dangerous, because they can point to an innocent person.

Face recognition

Face recognition is the most widely used emerging biometric in investigations. Police compare images from cameras or social media against databases of custody photographs, and some forces use live recognition to scan crowds for people on watch lists. Accuracy has improved greatly, but testing by the National Institute of Standards and Technology found that many algorithms had higher false match rates for some demographic groups, with large differences between algorithms (Grother et al., 2019). Buolamwini and Gebru (2018) found similar disparities in commercial facial analysis systems.

An independent review of live face recognition trials by the London Metropolitan Police raised concerns about the accuracy of matches in practice and about the legal basis and oversight of the deployments (Fussey & Murray, 2019). In *R (Bridges) v Chief Constable of South Wales Police* (2020), the Court of Appeal held that a police force's use of live face recognition was unlawful because the legal framework left too much discretion to officers and the force had not

done enough to check the technology for bias. The European Union's AI Act restricts real-time remote biometric identification in public spaces for law enforcement to narrowly defined circumstances (Regulation (EU) 2024/1689, 2024).

DNA-based technologies

Beyond standard DNA profiling, two DNA technologies are changing investigation. Investigative genetic genealogy uses consumer genealogy databases to find relatives of an unknown offender and build family trees; Erlich et al. (2018) estimated that most Americans of European descent could be identified this way through a relative. Forensic DNA phenotyping predicts externally visible characteristics, such as eye, hair and skin colour, and biogeographic ancestry from crime scene DNA. Kayser (2015) reviewed the method and concluded that some traits can be predicted with useful accuracy, but that predictions are probabilistic and should be used only to guide investigations, not to identify individuals.

Sensors and wearables

Phones, fitness trackers, smart watches, connected cars and smart home devices record movement, location, heart rate, sleep and activity. Such data can corroborate or contradict accounts of where a person was and what they were doing. Interpretation requires care: devices may not be worn, may be worn by someone else, and record estimates rather than precise measurements.

Emerging biometric and sensor technologies

Each can add knowledge, and each carries a characteristic risk

	What it can add	Main risk
Face recognition	Leads to identity from images	False matches; uneven accuracy across groups
Genetic genealogy	Identifies offenders through relatives	Privacy of relatives who did not consent
DNA phenotyping	Predicts appearance from DNA	Probabilistic; can reinforce stereotypes
Wearables and sensors	Activity and location over time	Device not worn, or worn by someone else

ModQu analysis based on Grother et al. (2019), Erlich et al. (2018) and Kayser (2015) ModQu.com

Figure 1. Four emerging technologies, what each can add to an investigation and its main risk. Diagram by ModQu.

A short example

The following hypothetical case shows these safeguards in practice. A retailer's security team investigates repeated thefts by a man caught on store cameras. A face recognition search against images of previous offenders, run under the company's documented policy, returns a possible match with a moderate score. Knowing that such scores can produce false matches, the team does not confront the person named. Instead it compares the times of the thefts with loyalty card records and finds that the suggested person was shopping in another city on two of the dates. The team records the search as a false lead and continues with other enquiries. Weeks later, a payment card used in one of the stores at the time of a theft leads to a different man, whose appearance matches the footage and who is later identified by staff. Had the first match been treated as proof, an innocent customer would have been accused.

Safeguards

Biometric data are especially sensitive because they cannot be changed if they are misused. Some laws, such as the Illinois Biometric Information Privacy Act (2008), require consent before biometric data are collected. Investigators should use technologies that have been independently tested, know their error rates for the population concerned, treat biometric matches as leads requiring independent confirmation, limit collection and retention to what is necessary, obtain lawful authority, and record how each technology was used.

Conclusion

Emerging biometric and sensor technologies can identify people and reconstruct events in ways that were impossible a decade ago. Their accuracy varies, some perform worse for certain groups, and they raise serious privacy concerns. Treated as sources of leads rather than proof, tested independently and used under clear legal rules, they can add reliable knowledge to investigations.

References

Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2008).

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*, 77–91.

Erlich, Y., Shor, T., Pe'er, I., & Carmi, S. (2018). Identity inference of genomic data using long-range familial searches. *Science*, *362*(6415), 690–694. https://doi.org/10.1126/science.aau4832

Fussey, P., & Murray, D. (2019). *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology*. University of Essex Human Rights Centre.

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

Kayser, M. (2015). Forensic DNA phenotyping: Predicting human appearance from crime scene material for investigative purposes. *Forensic Science International: Genetics, 18*, 33–48. https://doi.org/10.1016/j.fsigen.2015.02.003

R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union, L*.