GUEST ARTICLE

BIOMETRICS AND TRUST

EMMA BUTLER
DPO, YOTI

Biometrics is all over the global news, and not always in a good way. The last few months have seen negative reactions to law enforcement use of facial recognition technology, leading to some councils, towns, states and regulators banning or suspending its use [1].

The public perception of this technology is that it is intrusive and should require their permission [2], although this is often not the case. This has led to an increase in articles and discussions on the technology and its negative effects on individuals and society. The UK has always operated on the principle of 'policing by consent' [3]. It is fair to say that this has broken down with regard to facial recognition in many use cases and there is little trust in the technology.

What has been missing from the debates is that facial recognition has uses other than for surveillance or law enforcement and that biometrics is not only facial recognition. All face-based technology has been put in the same bucket and there is no balanced, nuanced debate about both the different biometric technologies that exist and the uses to which they are put.

A more balanced debate is needed that distinguishes technologies such as face detection, anti-spoofing, age estimation and facial recognition. And that distinguishes between uses such as security, anti-fraud, online safety, child protection, required ID and age checks, and where it is a voluntary option for individuals. Transparency and awareness of the different technologies and uses is one way to increase understanding and trust. Many uses of biometrics are non-contentious, such as using a fingerprint to access a smartphone, accessing a bank account using your face or voice, proving you are old enough to buy an age-restricted product, proving you are a real person not impersonating another, or proving your ID document belongs to you.

> "Technology develops quickly and we should be careful not to rush to regulate specific technologies as the solution."

Some are options individuals can choose to use, others may be mandatory because a higher level of security is needed, and some may run on the

back-end as an online safety measure. Context and purpose are key. Using biometrics for identification and authentication to provide greater levels of security, trust and assurance of who you are dealing with has different risks and benefits compared to covert police surveillance.

One criticism has been a lack of a regulatory framework. It is worth remembering that in many countries privacy and data protection laws govern the collection and use of personal information, regardless of the technology used. Technology develops quickly and we should be careful not to rush to regulate specific technologies as the solution. It would be more effective to focus on acceptable and unacceptable uses, and appropriate parameters and safeguards. We should also examine carefully whether there are genuine gaps in the regulatory framework, whether the issue is a lack of enforcement, or whether sector-specific codes of practice might be needed.

There has also been an increase in discussions about ethics and responsible data use, and different organisations are taking different steps to consider topics such as biometrics, AI and machine learning in the context of ethical frameworks. This alone though will not increase trust, as the public tends to be cynical about the motivations of corporates. Trust will come through the public seeing these frameworks and efforts put into practice and actual changes in behaviour.

Organisations involved in some way with biometrics need to better explain the different technologies, use cases, the risks and benefits, and the necessary parameters and safeguards. Organisations, governments, civil society and technology experts need to work together to make progress and increase trust.

Ultimately, trust in biometrics will come when people are informed rather than fearful, when corporates act ethically and responsibly and when government and law enforcement are able to show they really are policing with consent.

References:

1 https://www.biometricupdate.com/201909/morocco-places-moratorium-on-facial-recognition-california-limits-police-use
https://www.cnet.com/news/san-francisco-becomes-first-city-to-bar-police-from-using-facial-recognition/
https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech
https://edition.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html
https://www.zdnet.com/article/oakland-city-follows-san-franciscos-lead-in-banning-facial-recognition-tech/
https://komonews.com/news/local/portland-city-council-considers-ban-on-facial-recognition-technology

2 https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

3 https://www.gov.uk/government/publications/policing-by-consent