ICO Technology and Innovation Foresight call for views: Biometric Technologies

Open Rights Group and European Digital Rights welcome the opportunity to comment on the issue of biometric technologies, their adoption and their interaction with fundamental rights.

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK.

European Digital Rights (EDRi) is a network of 45 organisations from all around Europe that defend human rights online. EDRi has led civil society advocacy work on data protection and privacy since our creation almost 20 years ago.

1. **In your opinion, what emerging biometric technologies (defined as technologies processing biological or behavioural characteristics for the purpose of identification, verification, categorisation and profiling) are likely to be widely adopted in the market (i.e. likely to see market penetration of 20% +) in the next 2-5 years?**

Our core expertise relates to the impact of biometric systems on the rights and freedoms of individuals. We will address the uses of biometric data whose adoption is increasing, and whose uses we see as problematic.

Mass surveillance:

In the UK, biometric data were relied upon to carry out mass surveillance in at least the following manners:

- Live facial recognition is increasingly deployed to monitor public spaces and identify individuals.[1] In particular, the Metropolitan Police has been testing the use of live facial recognition[2] despite a Court judgment that ruled the lack of a legal basis for such use.[3]
- The private sector also deployed live facial recognition in public spaces, as in the case of supermarkets relying on these technologies to monitor customers and identify "thieves" and "antisocial behaviour".[4]

1 2018 Big Brother Watch, Face Off - The lawless growth of facial recognition in UK policing, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

2 See https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition/

3 See https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/

4 See https://bigbrotherwatch.org.uk/2021/01/co-op-facial-recognition-supermarkets-revealed/

- Further, it is worth mentioning that many video surveillance companies are selling biometric-ready CCTVs cameras.[5] This is particularly worrisome in a country like the United Kingdom, which has a vast network of surveillance cameras[6] that risk being repurposed with live facial recognition.

Identity checks and fraud detection:
We distinguish these from live facial recognition because biometric data is used to carry out identity checks against specific individuals. These include, in particular, the use of biometrics to conduct automated checks on the identity of drivers by Uber and other gig economy employers for fraud detection. [7]

Age estimation:
These technologies present the distinctive feature of using biometric data for the purpose of estimating internet users' age.

Identity providers and "safety tech" companies have been working on age estimation solutions. Further, we understand from their recent consultation that the ICO are considering the adoption of these technologies to implement the age assurance code.[8]

Worryingly, the BBC has reported on a public-private partnership between UK supermarkets and the UK Home Office to pilot biometric age 'verification' when purchasing alcohol.[9] Such an example also raises concerns of mass surveillance given the involvement of the state in such a project.

Biometric categorisation:
These technologies profile people's physical, physiological or behavioural characteristics to sort them into categories such as gender or even race, as advertised by Spanish company Herta Security.[10] They can form a component of identification systems or stand alone. Their use poses a severe risk of discrimination as well as risks of consumer manipulation, infringements on free choice and threats to people's dignity.

Emotion recognition:
Emotion recognition functions as a sub-set of biometric categorisation, whereby it analyses people's facial movements or other physical, physiological or behavioural signals in order to predict their emotional state or intention. Despite lacking a credible scientific basis, it has already been used widely by states for monitoring public spaces and at EU borders for attempted 'lie detection' (polygraph) purposes (iBorderCtrl). It is also increasingly used by companies as a way to profile, track and manipulate shoppers.[11]

---

5 See EDRi, The Rise and Rise of Biometric Mass Surveillance in the EU, p.23. Available at: https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf

6 See The Telegraph, One surveillance camera for every 11 people in Britain, says CCTV survey. Available at: https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

7 See 2021 Worker Info Exchange, Managed by bots. Available at: https://www.workerinfoexchange.org/wie-report-managed-by-bots

8 See 2021 ICO opinion: age assurance for the children's code. Available at: https://www.workerinfoexchange.org/wie-report-managed-by-bots

9 See: https://www.bbc.com/news/technology-60215258

10 See: https://reclaimyourface.eu/wp-content/uploads/2022/01/Screenshot_2020-01-28-BIOMARKETING_2-pdf.png

11 See: https://visionlabs.ai/industries/retail

'Seamless' travel (closed-set biometric identification tunnels and kiosks):
There is also a growing recourse for 'seamless' biometric systems which aim to identify people without that person needing to make any intervention e.g. simply by walking through a tunnel which has been equipped with biometric cameras or sensors. An example of a closed-set biometric identification tunnel is the UK's 'Protect EU' project.[12]

Closed-set biometric identification kiosks are increasingly used by commercial entities, for example to speed up check-in for travel. One example is the December 2021 pilots of closed-set biometric identification kiosks at the St Pancras Eurostar terminal in London, about which many privacy and data protection concerns were raised.[13] Such kiosks are also appearing at sports venues around the world.

Such use cases pose big risks of normalising biometric technology, and entail many of the same risks as mass surveillance systems as well as issues surrounding data security and misuse / re-use of data (especially when implemented by commercial entities).

2. **What sets the emerging technology apart from existing solutions and approaches?**

Attempts to circumvent existing data protection laws and ethical values:

We are increasingly seeing attempts by vendors, researchers and companies to find loopholes and exploit grey areas in order to conduct the processing of biometric data, or physical, physiological or behavioural data which does not uniquely identify people but which still poses risks to their fundamental rights. For example:

- The increasing use of non-uniquely-identifying data in the advertising context (e.g. biometric categorisation via "smart" adverts / billboards) in an attempt to avoid the General Data Protection Regulation / Data Protection Act;
- Increasing transient processing / edge processing, leading to vendors claiming that it doesn't really count as processing;
- Word-of-mouth reports of attempts to develop biometric identification / processing hardware in order to avoid rules on software;
- There is a strong trend of companies re-framing closed-set biometric identification as biometric "authentication" so that people mistake it for biometric verification. A notable example is the Facebook platform which, upon announcing that it was ending its facial recognition services, stated that it was moving towards facial authentication.[14] Another is the Eurostar example.[15]
- 'Traditional' CCTV cameras being sold with 'biometric-ready' capabilities, meaning that they have the potential to be turned into systems which process biometric data, but may not have gone through the proper assessments for the processing of biometric data.[16]

12 See: https://twitter.com/protect_eu

13 See: https://www.independent.co.uk/travel/news-and-advice/eurostar-biometric-passports-identity-entrust-b1942522.html

14 See: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

15 See: https://www.independent.co.uk/travel/news-and-advice/eurostar-biometric-passports-identity-entrust-b1942522.html

16 See EDRi's 2021 report: https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/

3. **What forms of biometric data are these likely to capture and how?**

Companies are increasingly innovating with a wide range of biometric data as well as non-uniquely-identifying physical, physiological and behavioural data. For example, during the COVID-19 pandemic, companies have focused on making the identification of individuals via just their eyes and the areas surrounding the eyes (e.g. the part of the face left exposed when wearing a mask) more accurate, increasing their ability to covertly track people across time and place.

Furthermore, we have received reports of experimentations with the following features / methods:

- Identification via the way that someone's buttocks and thighs distribute pressure on a chair / other surface
- Identification via breath print
- Identification via tongue
- Identification via ear canal
- Identification via pheromones / body odour
- Categorisation of people into protected groups on the basis of their physical, physiological or behavioural data
- Categorisation of consumers for the purpose of tracking and advertising (bringing the features of the online AdTech ecosystem into physical stores via people's physical, physiological or behavioural characteristics)
- 'Emotion recognition'
- 'AI lie-detectors'

4. **Are these technologies likely to focus on verification/ identification or classification of individuals?**

As a general tendency, we are seeing closed-set identification applied in the commercial context for purported efficiency reasons (e.g. queue management / speedy check-in) and verification for purported security reasons. In the law enforcement context we are seeing a rise in identification uses. When it comes to classification, we are increasingly seeing it deployed for advertising / consumer manipulation to put consumers into categories; and for public / state uses (sometimes alongside identification) to classify people's emotional states.

5. **How might these technologies benefit individuals and the use of their personal data?**

The use of genuine verification use cases fully within a user's control may benefit individuals by allowing them to claim / prove their identity whilst keeping all their biometric data in a chip or device which they own, have control over, to which no third parties can access, which does not rely on any central or remote database / data repository. However, this will only be the case if such a use case is also fully compliant with the GDPR and the Data Act (including having a clear legal basis, a DPIA, evidence of necessity and proportionality and so forth) as well as human rights rules.

Any other biometric use case of which we are aware comes with risks to people's fundamental rights. Some of these risks may be mitigable via safeguards, but others are fundamentally incompatible in a democratic society (such as the use of remote biometric identification in publicly accessible spaces, by any actor, and whether real-time or post) This ranges from risks of discrimination, violations of privacy and abuse sensitive data to societal-level impacts such as the suppression of protest and a chilling effect. There are also risks relating to the security of their data and the normalisation of biometric systems.

Whilst the biometrics industry frequently claim that their technologies can improve efficiency, we reassert that efficiency is not a legal basis. Claims that biometric

technologies are useful in preventing serious crime also lack any objective evidence, instead relying on vendors' technosolutionistic claims about what their systems can do.

6. **How might these technologies present risks to individuals and the uses of their personal data? How could these risks be mitigated?**

We start by identifying the issues that arise with the use of biometric data generally. We then compare these risks against the uses outlined above.

Sensitivity: biometric data are intrinsically linked to the human body, and they are in principle inalterable throughout life. Their sensitivity is recognised by Article 9(1) of the UK GDPR, which classifies them as "special category data" and prohibits the use of biometric data for identification. Similar considerations underpin article 6 of the Modernised Convention 108 of the Council of Europe, which prohibits the processing of "biometric data uniquely identifying a person" unless appropriate safeguards against discrimination are enshrined in law.

It is also worth mentioning that biometric data may reveal other sensitive information, such as ethnicity, gender and health conditions. If this is the case, sorting or classifying individuals based on non-identifying biometric data may still constitute processing of "special category data".

Intrinsic errors: All biometric systems, without exception, have some intrinsic errors that affect their accuracy and efficacy. These can include errors concerning the processing of biometric data (false positives or false negatives) as well as errors in acquiring this data — for instance, in case of injuries, disabilities or other developmental traits of the individuals that do not allow the collection of the relevant biometric data.[17]

It follows that biometric systems need adequate supervision and suitable alternatives for those individuals who may be incapable or unwilling to hand over their biometric data.

Fairness: practical applications of biometric systems often include solely automated decision-making within the meaning of Article 22 of the UK GDPR. Further, and for reasons seen in the section above concerning "intrinsic errors", unsupervised biometric systems are in any case likely to be incompatible with the principle of fairness enshrined both in Article 5(1)a of the UK GDPR and Article 5(3)a of Modernised Convention 108. Indeed, it would be unfair to require data subjects to supervise the accuracy and resulting outputs of error-prone systems they do not control.

Legitimacy: processing personal data for lawful and legitimate purposes is a legal requirement under Article 5(1)a of the UK GDPR and Article 5 of the Modernised Convention 108.

Law enforcement and presumption of innocence: in the field of data processing for law enforcement purposes, data subjects must be treated differently according to whether they are convicted, investigated, or otherwise linked to an investigation. This principle is

17 2014 (edited 2020) Council of Europe PROGRESS REPORT ON THE APPLICATION OF THE PRINCIPLES OF CONVENTION 108 TO THE COLLECTION AND PROCESSING OF BIOMETRIC DATA, Section 6.1 p.48. Available at: https://rm.coe.int/biometrics-coeprogresreport2014-edited-2020/16809e5412

enshrined in Article 6 of the Law Enforcement Directive and Section 38(3) of the UK Data Protection Act 2018 (UK DPA). Further, processing biometric data of individuals in this context may breach the presumption of innocence.

Risks related to age assurance applications:

- Sensitivity: we are concerned by the impact that widespread adoption of age estimation would have on the security of sensitive data. Even where biometric data is not used for identifying data subjects, the risk of this data being leaked and one's biometric features resulting compromised remains substantial. Processing biometric data to allow access to websites and internet services significantly increases the collection and transfer of this data, thus increasing the likelihood of leaks, for instance, as the result of data breaches or misuses.
- Intrinsic errors: making access to websites or services dependent on the processing of biometric data inherently exposes individuals to the risk of being unfairly denied access to such services, either for an error in the processing or because they are unable to provide the necessary biometric data.
- Fairness: age estimation inherently constitutes solely automated data processing under Article 22 of the UK GDPR: it automatically classifies internet users as above or below a certain age threshold, and it is unrealistic to expect that service providers would be able to provide meaningful supervision in real-time. Ex-post human review (for instance, an appeal against an erroneous age estimation) seems unsuitable for this particular application, as it would still frustrate and delay internet users' access to legitimate content for reasons that are ultimately outside of their control.

Risks related to identity checks and fraud detection:

All the issues mentioned above would still be present if not exacerbated by the impact that an accusation of fraud or criminal conduct may cause on the individuals being affected.

On top of that, we ought to stress that facial recognition has shown the potential to perpetuate biased outcomes against people of colour and other ethnic minorities. The issue is widely recognised even by the companies who develop facial recognition products,[18] which led to suspensions or moratoria against these systems due to the Black Lives Matter debate. Thus:

- On sensitivity: biometric data related to facial recognition are intrinsically revealing or suggestive of someone's ethnic background.
- On intrinsic errors: underrepresentation of ethnic minorities is a driver of errors in facial recognition, as models are trained on data sets that may reproduce or perpetuate pre-existing biases or unbalances.
- On fairness: discrimination based on one's ethnic background is an obviously unfair outcome.

Risks related to mass surveillance:

The use of live facial recognition to monitor public spaces exacerbates the issues concerning age estimation and identity checks for fraud detection. Live facial recognition raises further issues in relation to:

18 See Microsoft, Facial Recognition: It's Time for Action. Available at: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

- **Legitimacy:** supermarkets using live facial recognition to detect undesirable or arbitrarily defined "antisocial" individuals fail, prima facie, the most basic test of processing data for a legitimate aim. It is for law enforcement authorities to decide if someone's freedom of movement should be restricted and to what extent. While supermarkets or the management of other publicly accessible places may have a duty to block or to report individuals who are behaving in a certain manner, denying entrance in the absence of any problematic behaviour and on the sole basis of live facial recognition matchmaking hardly constitutes a legitimate use of biometric data. The same can be said about the purpose of identifying "thefts": if convicted individuals have not been subject to any security measure or restriction of their freedom of movement, preventing them from accessing supermarkets has no legal justification and ultimately serves an arbitrary and stigmatising purpose.
- **Law enforcement and presumption of innocence:** live facial recognition exposes everyone to mass monitoring in public spaces, regardless of their criminal record or any other condition listed by Section 38(3) of the UK DPA. We believe that live facial recognition breaches the presumption of innocence for the same reason.

7. **What do you believe may be the key regulatory challenges to deployment of the technologies?**
   (see answer to question n.8)

8. **How do you believe regulators such as the ICO can best support the delivery and implementation of these technologies in the future? For example, is sector specific regulation or guidance likely to be beneficial?**

We believe that the Council of Europe's 2011 Parliamentary Assembly report (Report) provides useful recommendations on how the ICO can best supervise and enforce the law against biometric technologies. Indeed, the United Kingdom is a member of the Council of Europe and a signatory of both the European Convention of Human Rights and the Modernised Convention 108. Further, the Report's recommendations are deeply rooted in the case-law of the European Court of Human Rights, and reflected in the Modernised Convention 108. These are:[19]

1. limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice;
2. providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification;
3. working with template data instead of raw biometric data, whenever possible;
4. enhancing transparency as a pre-condition for meaningful consent and, where appropriate, facilitating the revocation of consent;
5. allowing individuals access to their data, and/or the right to have it erased;
6. providing for appropriate storage systems, in particular by reducing central storage of data to the strict minimum;

19 2014 (edited 2020) Council of Europe PROGRESS REPORT ON THE APPLICATION OF THE PRINCIPLES OF CONVENTION 108 TO THE COLLECTION AND PROCESSING OF BIOMETRIC DATA, Section 3.1 p.10. Available at: https://rm.coe.int/biometrics-coeprogresreport2014-edited-2020/16809e5412

7. ensuring that biometric data are only used for the purpose for which they have been lawfully collected, and preventing unauthorised transmission of, or access to, such data.

Their relevance also stands out compared with the biometric data we discussed beforehand.

Age estimation:
The use of biometric data for age estimation raises issues with the principle of necessity, as:

- Biometric data breaches are irreversible, a risk that seems incompatible with the notion of establishing age verification "in the best interest of children".
- As reported by the ICO opinion on age assurance, there are alternatives to age estimation. As Open Rights Group argued in our submission on the issue of age assurance,[20] these can generally be regarded as less intrusive, and age verification does provide a suitable and more reliable alternative to high-risk scenarios (such as gambling websites).

Further, there is an obvious risk that children may not understand or underestimate the risks of providing biometric data. It follows that providing alternatives to those "unable or unwilling to provide biometric data" is unlikely to be effective in this field.

Fraud detection:
The use of facial recognition for identity checks and fraud detection sometimes result in exclusionary or discriminatory outcomes. Thus, the recommendation of providing "alternative methods of identification and verification" clearly applies. Further, we stress the importance of ensuring that companies who may need to carry out these identity checks provide alternatives that are as easy to use and accessible as biometrics checks. We believe that either penalising individuals who choose not to rely on biometric checks or forcing them to under the prospect of a cumbersome verification procedure (or any other adverse consequence) would frustrate the purpose of this recommendation.

Finally, we point out Workers Info Exchange report findings on the use of facial recognition by Uber, and the overall poor compliance of gig economy employers when it comes to respecting the right of access of their workers. The ICO should ensure that organisations understand and comply with their legal obligations.

Mass surveillance:
In general, we stress the incompatibility of the use of live facial recognition in public spaces with most of the Report's recommendations:

- Treating everyone as a suspect is, other than contrary to the presumption of innocence, clearly unnecessary and disproportionate;
- It seems unlikely that data subjects could be given "alternative methods" of mass identity checks, nor it is clear why these methods should be any more necessary or compatible with the presumption of innocence. Indeed, the decision not to introduce identity cards in the UK was underpinned by the principle that doing so would have meant treating everyone as a suspect;

20 Available at: https://www.openrightsgroup.org/publications/open-rights-group-submission-to-the-information-commissioners-office/

- Mass surveillance lacks transparency by definition, and individuals are unlikely to expect to be exposed to this kind of surveillance in a public street;
- There is no evidence that individuals are being given or could be given any meaningful right of access to live facial recognition data, even less considering that they would likely ignore their existence;
- Processing personal data of individuals who are not convicted nor linked with illegal activities is already incompatible with the purpose of law enforcement and crime detection, for which this data should have been collected.

On top of these considerations, we must stress that the Metropolitan Police is still using live facial recognition despite a Court judgement that found the absence of a legal basis for such use. Although such ruling did not ban live facial recognition, the fact that the MET is carrying out these activities without addressing the shortcomings that the Court raised denotes an apparent disregard for the law. It would be inappropriate to condone the use of highly intrusive technologies like live facial recognition by organisations that show their determination to operate beyond the boundaries of the law.

9. **What additional technological, legal and regulatory measures may be needed to realise the benefits of the biometric technologies across a wide spectrum of communities?**

We believe that any adoption of new technologies — and related legal and regulatory measures — should be wary of "technosolutionism". We appreciate the ICO's proactiveness in intervening against facial recognition for identity checks of pupils in schools' canteens,[21] and we believe that the focus should remain to rein in other problematic uses of biometric data.

Another action that the ICO could take is to issue further guidance on the strict and limited conditions in which the use of biometric systems might be necessary and proportionate, as was recently done by the Dutch data protection authority in response to unlawful attempts by the JUMBO supermarket chain to use facial recognition.[22]

21 See BBC, Schools pause facial recognition lunch plans. Available at: https://www.bbc.co.uk/news/technology-59037346

22 See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-supermarkten-op-regels-gezichtsherkenning (in Dutch)