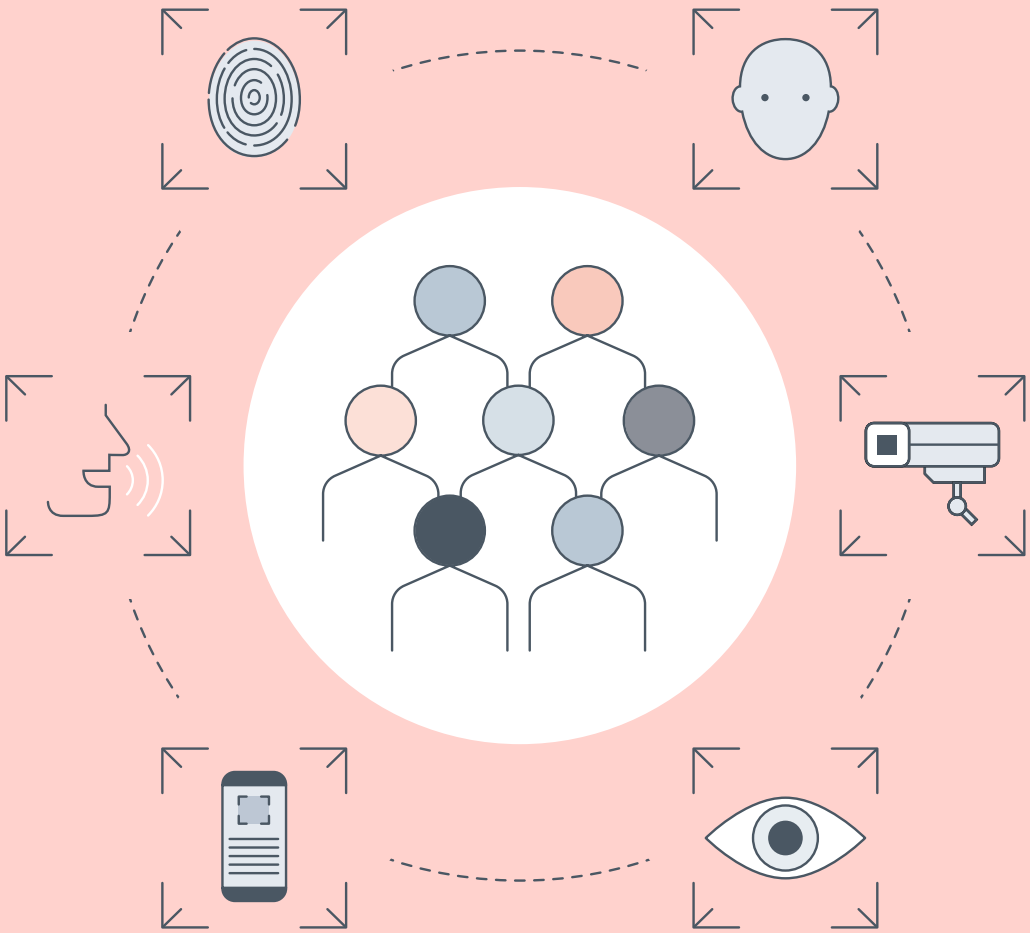
Ada Lovelace Institute

Biometrics

Countermeasures

The need for new legislation to govern biometric technologies in the UK

June 2022



Contents

Executive summary

Biometric data is uniquely personal. It captures our faces, fingerprints, walking style (gait), tone of voice, expressions and all other data derived from measures of the human body. It is inherently linked to who we are and cannot be easily changed, hidden or separated from our personal identity.

These types of biometric data are now being collected and used in a wide range of situations for many distinct purposes. We unlock smartphones with our faces or fingerprints, and can pass through border security by presenting our passports and faces to a camera that automatically matches the two. Police can deploy live facial recognition technology to monitor football matches and protests. Shops can use similar technology to monitor customers. Companies have proposed using facial expression analysis to detect whether students are paying attention in online class. And employers have used facial expression and tone analysis to decide who should be selected for a job.

Alongside a proliferation of biometric technologies, a number of issues have been raised about their impact on people and society, in particular regarding their impact on human rights. If people's identities can be detected by both public and private actors at any time, that may significantly infringe on someone's privacy as they move through the world, which may result in a chilling of free expression, free association and free assembly. Similarly, if people's traits, characteristics or abilities can be automatically assessed on the basis of biometrics, often without a scientific basis, this may affect free expression and development of personality.

Entangled with these potential harms are issues of bias and discrimination, which arise from the fact that some biometric technologies – and facial recognition technology, in particular – function less accurately for people with darker skin. This differential inaccuracy is itself a clear form of bias, which may be addressed as the technology improves. Solving the technical problems does not make these technologies safe: the use of biometrics can lead to bias and discrimination that stem not from the technology itself but from the way it

is used in context, for example to over-police marginalised communities, or to use stereotypes to make unfounded judgements about people in situations like hiring or education.

Recognising the importance of the evolving use of biometrics and the concerns raised, the Ada Lovelace Institute (Ada) has undertaken a three-year programme of public engagement, legal analysis and policy research, to explore the complex ethical challenges raised by biometric technologies and consider what governance is necessary to ensure biometrics are being used with public legitimacy. This report brings together the conclusion of that programme.

Ada's public engagement research shows that context matters greatly in people's comfort with biometrics. In a few cases, there are perceived benefits. However, across use cases, there are concerns about individual and societal harms. Given these concerns, people want to see a stronger legal framework with independent oversight and minimum standards to prevent harm, create accountability and transparency, and ensure proportionate use.

The independent legal review that Ada commissioned, led by Matthew Ryder QC,[1] finds that the legal protections in place are not fit for purpose. Current governance structures and accountability mechanisms are fragmented, unclear and not wholly effectual. The regulatory body governing police use of biometrics is not adequately empowered.

Furthermore, the Review finds that the legal frameworks that might be expected to cover biometric data and technologies are not fit for purpose because they are not fully comprehensive. While biometric data is covered under data protection law, as it constitutes personal data, only biometric data which *identifies* individuals is deemed special category data and subject to the highest safeguards. This leaves a growing set of biometric technologies that categorise individuals into groups subject to comparatively lower safeguards. Human rights law is of relevance to biometric technologies, but does not adequately cover non- public-service uses of biometric technologies. The Review also notes that human rights and equalities law are not set up to address biometrics-related harms *before* they arise in practice.

1 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales.* Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

In light of the demonstrable fact that existing governance of biometrics has failed to keep pace with public expectation or technological uses, we recommend the following (see Recommendations on page 53):

1. **Government should pass new, primary legislation to govern the use of biometric technologies.** New legislation must address uses of biometrics for both categorisation and identification, and should apply to the deployment of biometric technologies by both public and private actors.

2. **The oversight and enforcement of this legislation should sit within a new regulatory function focused on biometric technologies, which is national, independent, and adequately resourced and empowered.** The regulatory function should publish a register of public-sector uses of biometric technologies, monitor trends and have an ombudsperson to receive public complaints.

3. **This regulatory function should oversee the assessment of biometric technologies on two levels:**

    - **It should require that *all* biometric technologies meet scientifically based and clearly established standards of accuracy, reliability and validity.**

    - **It should assess the proportionality of biometric technologies in their proposed contexts, *prior to use*, for those that are used by the public sector, in public services, in publicly accessible spaces, or that make a significant decision about a person.** This proportionality test should consider individual harms, collective harms and societal harms that may arise from the use of biometric technologies. If approval is granted, the regulatory function should monitor the technology during its deployment and implementation stages, and continuously as long as the system is in use.

In addition, the regulatory function should undertake monitoring of the development and use of all biometrics technologies. This monitoring could trigger the creation of codes of practice that may include bans or moratoria.

In developing approaches to standards and the human rights-based proportionality test, the regulatory function should explicitly consider, account for the experiences, and seek the direct participation of marginalised and minoritised groups of people.

4. **There should be a moratorium on the use of biometric technologies for one-to-many identification in publicly accessible spaces and for categorisation in the public sector, for public services, and in publicly accessible spaces until comprehensive legislation is passed.**

In this report, we provide background on the definition of biometrics, contextualise our research activities in wider research on recent policy developments, synthesise the findings from our public engagement research and the independent legal review, and propose policy recommendations to address public concerns and legal gaps.

Overall, we contend that if biometric technologies are to be used, they must be governed by a legal framework and a regulatory approach that align their use with the expressed needs of people and society.

> 'They're not remotely attempting to keep up with [biometric] technology, and technology is far outstripping legislation. There's no urgency... I think they just need to bite the bullet and make this happen.'
>
> Citizens' Biometrics Council member, January 2022

How to read this report

If you are a member of the public

- This report presents evidence from two pieces of public engagement research on attitudes towards biometric technology. Ada began by conducting a nationally representative survey on UK public attitudes towards facial recognition technology (*Beyond face value*)[2] and convened the Citizens' Biometrics Council,[3] a public deliberation involving 50 UK adults assembled to learn about and then deliberate on biometrics in greater depth. The Council process also included a series of three Community Voice workshops focusing on communities particularly affected by biometrics.

- We contend that a call for policy action should be directly informed by the views of the public and the perspectives of marginalised and minoritised individuals and groups, as well as by expert analysis. Our policy recommendations, on page 53, are based on the conclusions reached in the Citizens' Biometrics Council in combination with Matthew Ryder QC's independent legal review.

- Evidence of what members of the public thought about biometric technologies and their governance is represented in findings from Ada's public engagement research on page 36. Quotes from the Citizens' Biometric Council are highlighted throughout the report.

2 Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

3 Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

If you are a policymaker

- This report makes the case for new legislation to govern biometric technologies in the UK. We provide evidence from public engagement research showing the public want safeguards, and present evidence from the Ryder Review that existing safeguards are not fit for purpose.
- We make recommendations on page 53 (reproduced in the Executive Summary above) for new legislation that would address this gap and would ensure data and AI work for people and society.
- In addition to the recommendations, 'Issues raised by biometric data and technologies' are discussed on page 21.

If you are a researcher, advocate or journalist

- This report begins with an overview of emerging issues in biometric technologies, noting the increased use in biometrics by actors beyond police, for purposes beyond identification, and based on inputs beyond face data, (see 'Issues raised by biometric data and technologies' on page 21).
- These shifts inform the policy actions we later recommend, which seek to regulate biometric technologies both on the basis of accuracy and validity, and the proportionality of their use in context.
- In coming to these policy approaches to these issues, we present evidence from both public engagement research and legal review.
- We seek to contribute to the many existing efforts to address the issues biometric technologies raise, some of which are presented in the section entitled 'Civil society, industry, and policy responses' on page 28.
- In addition to the recommendations on page 53 (reproduced in the Executive Summary above), for findings from the public engagement research see page 36, for 'Issues raised by biometric data and technologies' see page 21, and for 'Case studies' see page 56.

Introduction

This report represents the culmination of Ada's three-year programme of work on biometrics governance. It draws from Ada's public engagement research on attitudes towards biometric technologies, an independent legal review led by Matthew Ryder QC,[4] and desk research to provide background on current developments in the realm of biometric technologies and their governance. It puts forward a set of ambitious policy recommendations, that are primarily for policymakers and will also be of interest to civil-society organisations and academics working in this contested area.

We begin by defining biometric data and biometric technologies, listing examples and noting distinctions within the term biometric data. This leads to the issues that biometric data collection and biometric technologies raise, charting the shift in use from police and law enforcement to use in supermarkets, schools and job recruitment.

This commentary and analysis is based on desk research and seeks to outline the background information relevant to understanding the public engagement research findings that follow. It also notes significant responses to biometric technologies from civil society, companies, governance institutions and policymakers, with the intention of situating this report's recommendations among those interventions.

The public engagement research evidence surfaces findings from two Ada publications: 1) A nationally representative survey on UK public attitudes towards facial recognition technology called *Beyond face value*;[5] and 2) The report of the Citizens' Biometrics Council,[6] a public deliberation involving 50 UK adults assembled to learn and then deliberate on biometric governance in greater depth. The Council process included a series of three Community Voice workshops focusing

4 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

5 Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

6 Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

on communities particularly affected by biometrics. Both the survey and the Citizens' Council highlighted public support for stronger safeguards on biometric technologies.

This is followed by substantive points from Matthew Ryder QC's independent legal review of biometric data in England and Wales. The Review finds that the current legal framework for governing biometrics is not fit for purpose and that the accountability mechanisms in place are fragmented and ineffective. The Review identifies the need for a new, technologically neutral, statutory framework to govern biometrics. To ensure that legislation is enforced, the Review suggests the establishment of a national Biometrics Ethics Board.

Examining calls from the public and evidence from the legal review, we have formulated a set of recommendations on how to build policy and legislation to ensure that biometrics work for people and society.

What are biometrics?

The question of what exactly counts, and what should count, as biometric data and biometric technologies (at least for the purposes of law and regulation) is the subject of some debate, with different jurisdictions adopting distinct definitions of biometrics.

In the UK, biometric data is defined in law by UK General Data Protection Regulation (UK GDPR), as: 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data' (UK GDPR Article 4(14)).

Under the UK GDPR, biometric data counts as special category personal data when it is used or collected for 'the purpose of uniquely identifying a natural person'. This special category status is important because UK GDPR prohibits the processing of special category data except under specific conditions (these conditions are supplemented and elaborated on in the Data Protection Act 2018).

In Scotland, the Scottish Biometrics Commissioner Act 2020 defines biometric data slightly differently as: 'information about an individual's physical, biological, physiological, or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual'.

For the purposes of the evidence and arguments presented in this paper, we will use the following, inclusive definitions of biometric data and biometric technologies. These definitions explicitly include data derived from the human body that can be used to identify or categorise people.

***Biometric* data** is data that relates to the physical characteristics of a natural person that can be measured, recorded and quantified. Biometrics is a shorthand for biometric data.

Biometric technologies, by extension, use biometric data to derive information about people: most often to establish the presence of a person, to verify or to establish a person's identity, or to make other determinations about a person, such as their mood, gender or other characteristics. These technologies generally use machine learning or artificial intelligence to both collect biometric data and to automatically analyse or assess it.

In this report, we discuss the governance of both biometric data (what is collected or detected) and biometric technologies (how that data is used).

Open questions about how exactly to define biometric data and technologies will be explored below. The purpose of this exploration is to draw distinctions that become relevant in defining the scope of future legislation.

> 'Biometric technologies are fundamentally about bodies – what we do with them and how we allow them to be used.'
>
> Citizens' Biometrics Council member, 2020

Types of biometric data

Common biometrics include:


— Face


— Eye (iris and retina)


— Ear


— Fingerprint


— Hand geometry


— Vein pattern in hand or finger


— DNA


— Heartbeat pattern


— Gait (how someone walks)


— Voice (sound and tone)


— Typing or keystroke pattern


— Facial expressions

Distinctions within biometric data

These types of biometric data can be characterised by a variety of commonly used terms:

Identity-linked biometric data
Some biometric data is primarily useful as a marker of identity, whereas other data reveals additional information. For example, fingerprint data can be used to identify a person, but is not used to infer any additional information. DNA data, on the other hand, can be both linked to identity and be used to reveal things like heritable traits.

Raw (or unprocessed) and processed biometric data
A legally important distinction is between raw (or unprocessed) biometric data and processed biometric data. Raw biometric data is data that has the potential to be used for biometric identification, but that has not yet been subjected to the technical processing to enable such an identification. For instance, a photograph clearly showing a person's face could be considered raw biometric data.

By contrast, the digital analysis and representation of that person's face which can be derived from the photo (known as the template, facial geometry or faceprint) would be considered processed biometric data. Likewise, an audio recording in which a person's voice is audible could be considered raw biometric data, whereas the abstracted 'voice print' that can be derived from it would be considered processed biometric data. The distinction is important because, in some jurisdictions, data protection regulations apply only to processed biometric data.

Static versus dynamic biometric data
Static biometric data includes data derived from physical features of human bodies, such as fingerprints, facial geometry and iris patterns, usually at a single point in time. Dynamic (or behavioural) biometrics use data about patterns of behaviour. This might be the particular way a person walks (gait analysis), the cadence with which they type (keystroke analysis) or how they move a mouse cursor or swipe a touch screen (gesture analysis). In contrast to static biometric data, dynamic data is collected over a longer period of time to pick up on patterns and changes.

Hard and soft biometrics

Hard biometrics refers to features which are unique to an individual and therefore can identify them without the need for further data. This includes fingerprints and faceprints. Soft biometrics refers to features which are generic and cannot be linked to any specific individual, such as eye colour. They tend to be ancillary characteristics that provide some information, but not enough to identify a person by themselves.

Strong and weak biometrics

Biometrics such as DNA and fingerprints, which are unique and permanent, are considered strong biometrics, whereas weak biometrics (such as voice and gait) are features that are less unique or less stable.

Technologies that use biometric data

Biometric data can be used in a range of technologies for various ends. This report explores biometric technologies that detect, verify, identify and categorise, in the analysis below. Across these purposes, sometimes it is obvious that biometric data is being collected, because a person has to present their data physically, such as using a fingerprint to unlock a phone. Other technologies operate *remotely*, or without people readily knowing that the technology is in operation, such as in a shop or at a protest. Remote biometric technology can present a unique risk because people may not be aware that biometric processing is taking place – and so may not be in a position to exercise their rights.

> ‘It all feels a bit secret. People are taking your picture, you don’t know why, you don’t know what they’re doing with it, you don’t know if the information’s correct or not, and there’s really nothing you can do about it.’
>
> Citizens’ Biometrics Council member, 2020

Common and emerging biometric technologies

- **Facial recognition technology (FRT)**: a camera detects a person's face through a computer system that has been trained to detect human faces. The computer translates that face into a set of data points (the faceprint). That set of data points can then be compared to an existing database of faces to make a match.
    - Live facial recognition (LFR): FRT can be used in real-time by analysing people on a live video.
- **Emotion recognition or identification:** systems that advertise themselves as emotion recognition or identification often use video or static pictures to capture facial expressions, tone of voice, speech, or other biometrics and then classify them as indicative of certain emotions (joy, sadness, etc.).
- **Gait analysis:** the way a person walks can be captured by cameras and, like facial recognition, can be turned into a set of data. That data can then be analysed, often to identify individuals based on the uniqueness of walking patterns, or to predict certain physical states, such as drunkenness or sickness.

Common applications of biometric technologies

Detection: is there anybody there?
This type of biometric technology includes the use of facial recognition technology to confirm the presence of a face in a digital image, or the use of motion sensors and other biometric data to detect the presence of a person. Many digital cameras use this functionality to determine what part of an image to focus on, and CCTV systems can use it to count the number of people in a particular location, or to track the movement of people through a space.

Example: UK border authorities have been known to use a range of biometric technologies to detect people crossing the border, including heartbeat monitors to detect people who are out of immediate sight, and carbon dioxide detectors to detect people breathing.[7]

7 BBC News. (2016). *Calais migrants: How is the UK-France border policed?*. Available at: https://www.bbc.com/news/uk-33267137

Verification: are they who they say they are?

Perhaps the oldest use of biometric data is for confirming the identity of a particular person (also referred to as 'one-to-one matching' or 'authentication'). In these cases, an individual presents themselves as a specific person. In order to find a match, the biometric verification system checks that individual's biometric data against a biometric profile that already exists on a device or in a database. The match is not necessarily a guarantee that the person is who they say they are, but rather reflects a degree of confidence that the biometrics match up. The threshold of similarity varies across different biometric systems and has important implications for accuracy. If the threshold for similarity is set very low, then the system may be very inaccurate.

Example: Using a face scan to unlock a smartphone, or going through electronic gates at the airport (Automated Border Control), which compares a picture of a person's face to the person's passport picture, which is transmitted when the passport's chip is scanned.[8] Though now paused, in 2021 schools in the UK were using facial recognition to verify students' identities as a cashless way to pay for lunch.[9]

Is it proportionate to use facial recognition in the school lunch queue?

For a more detailed case study on the use of facial recognition in school lunch queues, and an explanation of how Ada's proposed legislation would apply to this scenario, see page 56.

Identification: who are they?

Biometric data can also be used to determine the identity of an otherwise unknown person (this is also referred to as 'one-to-many matching'). Biometric identification systems work by comparing the biometric data of the person being identified with a database containing existing biometric profiles. Again, this type of matching reflects a degree of confidence in the similarity of the subjects – not a guarantee. Facial recognition for identification has been known to be

8 Air Industry Review. (2020). *Airport e-gates: could the pandemic save them from the scrap heap?*. Available at: https://airport.nridigital.com/air_may20/airport_egates

9 BBC News. (2021). *Schools pause facial recognition lunch plans.* Available at: https://www.bbc.com/news/technology-59037346

disproportionately inaccurate for people with darker skin.[10]

Example: Retail stores have deployed facial recognition on shoppers to match people's faces to an existing list of people 'previously observed engaging in potential criminal activity'.[11] The Southern Co-op supermarket chain has recently used live facial recognition in an attempt to identify customers of interest in a number of shops in England.[12]

Is it legitimate to monitor customers at the supermarket?

For a more detailed case study on the surveillance of shoppers at supermarkets, and an explanation of how Ada's proposed legislation would apply to this scenario, see page 57.

Categorisation: using biometrics to categorise people on the basis of correlation with characteristics, or to make other judgements about abilities, character or emotions, often involving pseudo-scientific assumptions

Developers now use biometrics to make inferences about people on the basis of observed biometric traits thought to be statistically related, or correlated (however tenuously), with particular characteristics. For instance, biometric systems have been developed that attempt to infer people's sexuality from their facial geometry,[13] or judge criminality from pictures of people's faces.[14] These systems have been criticised for using pseudo-scientific assumptions to draw links between external features and other traits.[15,16] Categorisation can also be referred to as classification.

10 Singer, N. and Metz, C. (2019). 'Many Facial-Recognition Systems Are Biased, Says U.S. Study'. *The New York Times*. Available at: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

11 Dastin, J. (2020). 'Rite Aid deployed facial recognition system in hundreds of U.S. stores'. *Reuters*. Available at: https://www.reuters.com/investigates/special-report/usa-riteaid-software/

12 Rollet, C. (2022). 'UK Grocer Facial Recognition With Hikvision Cameras, GDPR And Ethical Risks Examined'. *IPVM*. Available at: https://ipvm.com/reports/facewatch-coop

13 Levin, S. (2017). 'New AI can guess whether you're gay or straight from a photograph'. *The Guardian.* Available at: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

14 Wu, X. and Zhang, X. (2016). 'Automated Inference on Criminality using Face Images'. *arXiv*, 1611.04135 [cs]. Available at: https://arxiv.org/abs/1611.04135v1

15 Vincent, J. (2017). 'The invention of AI "gaydar" could be the start of something much worse'. *The Verge*. Available at: https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy

16 Bowyer, K. W. et al. (2020). 'The "Criminality From Face" Illusion'. *IEEE Transactions on Technology and Society*, 1(4), pp. 175–183. doi: 10.1109/TTS.2020.3032321

Other systems attempt to judge people's internal emotional state or intentions from their biometrics like tone, voice, gait or facial expressions (known as 'emotion recognition'). It is important to emphasise that the underlying science of 'emotion recognition' is unproven. A large-scale review of the psychological literature on the topic finds that there is no standard, universal link between external expression and inner emotions.[17,18] The unproven basis for emotion recognition have led many to consider this technology a form of pseudo-scientific physiognomy and phrenology.[19,20]

Example: With the increase in online learning during the pandemic, Intel developed a system that it claims can detect whether students in online classes are bored or paying attention, based on facial expressions.[21]

> 'I wonder whether we're all going to end up like robots because we're so frightened of changing our face [expression] and being penalised for something because we look a different way.'
>
> Citizens' Biometrics Council member, January 2022

Is it possible or fair for an algorithm to evaluate face and voice data in a job interview?

For a more detailed case study on the use of 'emotion recognition' in recruitment, and an explanation of how Ada's proposed legislation would apply to this scenario, see page 58.

17 Barrett, L. F. et al. (2019). 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements'. *Psychological Science in the Public Interest*. doi: 10.1177/1529100619832930

18 Heaven, D. (2020). 'Why faces don't always tell the truth about feelings'. *Nature*, 578(7796), pp. 502–504. doi: 10.1038/d41586-020-00507-5

19 Stark, L. and Hutson, J. (2021). *Physiognomic Artificial Intelligence*. SSRN Scholarly Paper 3927300. Rochester, NY: Social Science Research Network. doi: 10.2139/ssrn.3927300

20 Sloane, M., Moss, E. and Chowdhury, R. (2022). 'A Silicon Valley love triangle: Hiring algorithms, pseudo-science, and the quest for auditability'. *Patterns*, 3(2), p.100425. doi: 10.1016/j.patter.2021.100425

21 Kaye, K. (2022). 'Intel thinks its AI knows what students think and feel in class'. *Protocol*. Available at: https://www.protocol.com/enterprise/emotion-ai-school-intel-edutech

Examples of how and where biometrics can be used

Biometric data	Where	Why	Deployer	Affected individual	Use type	Data types
Fingerprint 	Computer	To unlock a computer in place of a password	Computer manufacturer	Computer user	Verification, one-to-one	Processed Strong Identity-linked Physically-linked Hard
Face 	Airport passport gates	To confirm a person is the passport holder	Border authorities or airline	Airport traveller	Verification, one-to-one	Processed Strong Identity-linked Physically-linked Hard
Face 	At big events, like protests, festivals, or football matches	To identify people of interest to the police based on an existing database	Police or private security service	The public	Identification, one-to-many	Processed Strong Identity-linked Physically-linked Hard
Tone of voice 	In an online job interview, via video	Using tone of voice to partially determine job suitability	Employer	Job applicant	Categorisation	Processed Potentially identity-linked Behaviour-linked Soft Weak
Facial expressions 	In an online classroom	Analysing facial expressions to determine whether students are paying attention	School staff	Students	Categorisation	Processed Potentially identity-linked Behaviour-linked Soft Weak
Gait and face 	Smart oorbells	To identify individuals or types of people at someone's door	Home-owner / resident	The public	Identification and potentially categorisation	Processed Potentially identity-linked Behaviour- and physically-linked Soft and hard Weak
Face 	On public streets	Identifying members of a minority group in an authoritarian context	Government, law enforcement	The public	Categorisation	Processed Potentially identity-linked Behaviour- and physically-linked Soft Weak

Issues raised by biometric data and technologies

Biometric technologies affect daily life in powerful and meaningful ways, and are proliferating in the UK without a comprehensive legal framework in place.[22]

The deployment of biometric technologies has been mirrored by an increase in research that identifies technical shortcomings and societal risks arising from this technology. Great attention has been paid to police use of facial recognition technology, but as we outline below, the use of biometric technologies extends beyond identification, beyond policing and beyond facial data, which brings new issues into focus. As older technologies improve, the question shifts from whether they work to whether they should be used. For newer technologies, questions of validity and accuracy emerge.

The following section traces some of the emerging issues that new biometric technologies raise, and provides the background relevant to understanding the evidence that the Ada Lovelace Institute has gathered on public attitudes towards biometric technologies.

Police use of facial recognition technology and accuracy concerns

Biometric data has traditionally been used to identify people in the law enforcement context, including everything from fingerprints and DNA samples to manual facial matching. Driven by the availability and capacity of computers to identify and match faces automatically, law enforcement began to use biometric technologies on a new scale: to identify individuals from automatic analysis of faces, also known as facial recognition technology (FRT).

22 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

Unlike traditional surveillance cameras, which capture pictures or video for manual analysis by humans, facial recognition technologies can automatically compare people in crowds to databases and identify them in real-time or after the fact. Real-time and automatic analysis – live facial recognition (LFR) – has spurred concerns that FRT infringes on privacy, expands surveillance and discourages free expression, assembly and association.[23]

> 'If there's a CCTV camera, you're less likely to act outside of what's acceptable, because you're under observation. So you modify your own behaviour, you stop being as wild, or as wonderful, or as kinky, or as strange, or as bizarre, as beautiful as you could possibly be [...] And no-one has asked us if we want to live in that society.'
>
> Citizen from Brighton Community Voice workshop, December 2019

Notwithstanding the privacy and surveillance implications of FRT, there has been a functional issue with the accuracy of the technology in practice that leads to bias and discrimination. In 2018, a foundational study, *Gender Shades*, by Dr Joy Buolamwini and Dr Timnit Gebru demonstrated that FRT that designated gender (male or female in this case) was less accurate for people with darker skin, and performed especially poorly at identifying women of colour as women. This was largely because women with darker skin were not well-represented in the systems' training datasets.[24] Addressing a similar issue, in 2019, the US National Institute of Standards and Technology (NIST) conducted a test of different commercial FRT systems to assess how accurate the systems were for different demographic groups. That round of testing

23 UN High Commissioner for Human Rights. (2020). *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*. Available at: https://digitallibrary.un.org/record/3879547

24 Buolamwini, J. and Gebru, T. (2018). 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Conference on Fairness, Accountability and Transparency*, PMLR, pp. 77–91. Available at: https://proceedings.mlr.press/v81/buolamwini18a.html ; Phillips, P. J. et al. (2018). 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms'. *Proceedings of the National Academy of Sciences*, 115(24), pp. 6171–6176. doi: 10.1073/pnas.1721355115.

found that people classified as 'African American or Asian were 10–100 times more likely to be misidentified than those classified as white'.[25]

Being misidentified has significant consequences for a person and there is evidence that the use of this technology has already led to the false arrest of three Black men in the USA.[26] More broadly, racial bias in facial recognition may lead to needless 'stop and account' interventions on the basis of ethnicity alone – an automated version of racial profiling.[27] As noted on p. 28, the recognition of these accuracy-related harms has driven calls for bans on police FRT from civil society groups worldwide, as well as company-led moratoria on sales of FRT to police. A number of cities have also introduced moratoria or bans on public-sector use of FRT.[28]

Since the *Gender Shades* study and NIST's 2019 vendor test, some vendors have increased the accuracy of FRT for different demographic groups.[29] The potential for these technologies to become more accurate, however, leaves open the question of whether they should be used and if so, where and how.

> 'There is a stigma attached to my ethnic background as a young Black male. Is that stigma going to be incorporated in the way technology is used? And do the people using the technologies hold that same stigma? It's almost reinforcing the fact that people like me get stopped for no reason.'
>
> Citizens' Biometrics Council member, 2020

25 Grother, P. J., Ngan, M. L. and Hanaoka, K. K. (2019). 'Face Recognition Vendor Test Part 3: Demographic Effects'. *NIST*. Available at: https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects , summarised in: Castelvecchi, D. (2020). 'Is facial recognition too biased to be let loose?'. *Nature*, 587(7834), pp. 347–349. doi: 10.1038/d41586-020-03186-4

26 Hill, K. (2020). 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match'. *The New York Times*. Available at: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

27 To note: the reason for this misidentification could be a differential inaccuracy issue in the technology itself, or because of a bias in the way people are added to the database of suspected people. In the latter case, even if there is an equal error rate across demographic groups, if a disproportionate number of Black men were added to the database, then there would be a higher chance of a Black man being misidentified.

28 Simonite, T. (2021). 'Face Recognition Is Being Banned – but It's Still Everywhere'. *Wired*. Available at: https://www.wired.com/story/face-recognition-banned-but-everywhere/

29 NIST. (2022). *Face Recognition Vendor Test (FRVT) Ongoing*. Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

Beyond police, beyond identification and beyond facial recognition

Biometric technologies are now in use across a variety of contexts beyond police use of facial recognition – by actors outside the public sector, for purposes beyond identification, and using new types of biometric data – and this raises new issues.

Beyond police: Who?

From supermarkets and airports, to job interview platforms and housing developments, there has been a proliferation of biometrics designed to be used across day-to-day life – not just in policing. To date, much of the regulatory attention has focused on police use. Concerns are now being raised about a lack of oversight on private-sector use, which can also have life-affecting significance,[30] and is not subject to the same level of regulatory oversight, or due process protections afforded within the criminal legal system.

Beyond identification: Why?

New uses of biometrics aim to do more than just identify specific individuals and can instead aim to classify or categorise people, by advertising that they are able to guess characteristics like gender or age, and to detect emotion or predict criminality. This shift is significant because it changes the baseline task at hand. When using facial recognition technology to identify someone, for instance, the fundamental task at hand is clearly defined (does this person's face match the face in the database?). In contrast, the task at hand when classifying people's emotions or other traits is much more ambiguous. For instance, even for humans, it is not consistently possible to guess a person's traits, such as gender,[31] let alone someone's inner emotions from external features or expressions. Giving a machine that task may be bound towards failure not only because of embedded bias or technical shortfalls, but also because the task at hand is fundamentally subjective.[32, 33]

30 Information Commissioner's Office (ICO). (2021). *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*. Available at: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

31 Keyes, O. (2018). 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition'. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), pp. 88:1-88:22. doi: 10.1145/3274357

32 Barrett, L. F. (2022). 'Facial Expressions Do Not Reveal Emotions'. *Scientific American*. Available at: https://www.scientificamerican.com/article/darwin-was-wrong-your-facial-expressions-do-not-reveal-your-emotions/

33 Contributions by Brenda Leong in forthcoming Ada Lovelace Institute publication on four areas for further exploration in AI regulation.

Beyond facial data: What?

A wider range of biometric data is now being collected – from the way we walk (gait analysis), to the way we talk (voice and tone analysis), to the facial expressions we make. New patent applications by Meta (the parent company of Facebook) show that the company plans to collect biometrics like pupil movement and body poses, as a way to target advertisements in the metaverse or virtual reality.[34] As an increasing number of types of biometric data are collected in an increasing number of places, new questions have been raised about the validity of systems' underlying science and assumptions.[35]

These newer biometric technologies present new risks. Systems that use biometrics to analyse facial expressions or tone may introduce bias through accuracy problems, especially for people with disabilities, whose expressions or voice may not conform to ableist expectations or norms.[36,37]

Tools that use biometric data, such as tone of voice or facial expression, to assess internal state or competencies (e.g. biometrics in hiring for emotion recognition) are based on unproven underlying assumptions. The relevant psychology literature indicates that it is not possible to consistently infer internal emotional states from external facial expressions.[38] This lack of evidence has prompted many to consider emotion recognition technology pseudo-scientific physiognomy or phrenology.

There is evidence that use of biometric tools in hiring, which analyse tone of voice in relation to communication skills, may favour a certain type of communication – that of a dominant demographic group,[39] or certain

34 Irwin, V. (2022). 'Meta is looking into eye-tracking and product placement to make money in the metaverse'. *Protocol*. Available at: https://www.protocol.com/bulletins/metas-tracking-you

35 See, for example: van Mastrigt, N. M. et al. (2018). 'Critical review of the use and scientific basis of forensic gait analysis'. *Forensic sciences research*, 3(3), pp. 183–193. doi: 10.1080/20961790.2018.1503579

36 Center for Democracy and Technology. (2022). *CDT Comments to OSTP Highlight How Biometrics Impact Disabled People*. Available at: https://cdt.org/insights/cdt-comments-to-ostp-highlight-how-biometrics-impact-disabled-people/

37 Access Now. (2022). *Joint civil society amendments to the Artificial Intelligence Act: Prohibit emotion recognition in the Artificial Intelligence Act*. Available at: https://www.accessnow.org/cms/assets/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf

38 Barrett, L. F. et al. (2019). 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements'. *Psychological Science in the Public Interest*. doi: 10.1177/1529100619832930.

39 Ajunwa, I. (2021). 'Automated Video Interviewing as the New Phrenology'. *Berkeley Technology Law Journal*. Available at: https://papers.ssrn.com/abstract=3889454

perceived personality traits. While this may or may not involve racial profiling or other protected characteristic-based profiling, it may lead to biased or arbitrary decision-making.[40]

Context matters: it's not just about accuracy

Across facial recognition and other biometric technologies, there are not only risks of bias based on differential accuracy and underlying pseudo-science, but also based on the context in which they are used. If and when biometrics become more accurate for all groups, they may still be used in ways that replicate existing systemic inequality or oppression, particularly through the oversurveillance of marginalised communities and groups. For instance, a recent report on facial recognition in the USA finds that in three New York City boroughs 'the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras.'[41]

A report on FRT in the UK posits that a similar dynamic could arise, given the extent to which Black and Asian British people are over-policed compared to white British people[42] (for example, Black British people are seven times more likely to be stopped and searched by police than white people).[43] Over-policing of marginalised communities and increased surveillance become a reinforcing, negative cycle where communities that are already marginalised are disproportionately subject to more surveillance, which leads to further marginalisation.

Biometrics that do not identify but attempt to classify people can also be used in harmful contexts to deepen existing forms of oppression. For example, the Chinese government has used facial recognition to distinguish Uighur individuals from the Han majority in order to track and

40 See: Stark, L. and Hutson, J. (2021). 'Physiognomic Artificial Intelligence'. *Fordham Intellectual Property, Media & Entertainment Law Journal*. doi: 10.2139/ssrn.3927300: 'Categories like "adventurous" or "benevolent" cannot be statically applied to a person's character; such broad and construed categories have little to do with a worker's potential suitability for a job; and individual physical manifestations of expressivity are practically useless proxies for either. While such assessments using "physiognomic vision" seem superficially easy and attractive, they are at best arbitrary, and at worse reifications of existing bias, animus, and stereotype'.

41 Amnesty International. *Inside the NYPD's Surveillance Machine*. Available at: https://banthescan.amnesty.org/decode/

42 Chowdhury, A. (2020). 'Unmasking Facial Recognition'. *WebRoots Democracy*. Available at: https://webrootsdemocracy.org/unmasking-facial-recognition/

43 Rhoden-Paul, A. (2022). 'Stop and search: Ethnic minorities unfairly targeted by police – watchdog'. *BBC News*. Available at: https://www.bbc.com/news/uk-61167875

control Uighur people's movements.[44] While this is an extreme example of biometrics used in the service of oppressive ends, it points to an important issue: that having the capacity to to classify people or groups facilitates targeting on the basis of those characteristics.

As biometric technologies advance, and accuracy and functionality improve, it is ever-more important to consider the human rights implications of this technology – in other words, to consider its proportionality in a specific circumstance in addition to its functionality.

44 Wakefield, J. (2021). 'AI emotion-detection software tested on Uyghurs'. *BBC News*. Available at: https://www.bbc.com/news/technology-57101248

Civil society, industry and policy responses

Ada joins a long line of organisations, advocates and policymakers calling attention to the risks of biometric technologies and proposing ways to address them through policy and legislative means. This section surfaces a number of those calls and proposals, not as an exhaustive catalogue, but to situate the recommendations proposed on p. 53.

Global civil society and industry responses underscore risks and harms of biometric technologies

Civil society and advocacy groups around the world have led the call drawing attention to the risks and harms of biometrics. Some of these groups call for bans on biometric surveillance on the basis that the harms the technology poses are so severe that they cannot be addressed through legal safeguards alone.

In the US, the Algorithmic Justice League, whose founder co-led the first piece of research that demonstrated bias in facial recognition systems, subsequently audited Amazon's Rekognition facial recognition system and again found lower levels of accuracy for women and people of colour.[45]

In 2018, this research informed a call from 70 US organisations, including civil rights, community and religious groups, for Amazon to stop selling the technology to the government.[46] In summer 2020, in the context of the Black Lives Matter movement, Amazon, IBM and Microsoft agreed to pause sales of their tools to police, either until legislation was passed or for a specified period of time.[47]

45 Buolamwini, J. (2019). Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces. Available at: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced

46 American Civil Liberties Union. (2018). *Letter from nationwide coalition to Amazon CEO Jeff Bezos regarding Rekognition*. Available at: https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition

47 Heilweil, R. (2020). 'Big tech companies back away from selling facial recognition to police. That's progress'. *Vox*. Available at: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Throughout this period, digital rights organisation Access Now has gathered support from over 200 organisations from around the world to ban biometric surveillance, defined as the use of facial recognition and remote biometric technologies in publicly accessible spaces. This campaign, drafted in partnership with Amnesty International, European Digital Rights, Human Rights Watch, Internet Freedom Foundation and Instituto Brasileiro de Defesa do Consumidor, calls for an outright ban on this technology.[48] There have also been important efforts to educate affected people about their rights in relation to biometric surveillance, such as training led by the Surveillance Technology Oversight Project in New York.[49]

In the EU, a parallel campaign led by 22 European organisations has gathered upwards of 70,000 signatures and calls on the European Commission to strictly regulate biometrics and prohibit uses which lead to unlawful mass surveillance.[50] Amnesty International has issued a campaign called Ban the Scan, which focuses on FRT in New York City and Hyderabad and calls for bans of tools that enable mass surveillance. In the UK, groups including Privacy International, Liberty and Big Brother Watch have echoed these calls for bans.[51]

International policy responses: momentum towards the governance of biometric technologies

There are emerging efforts to address specific uses of facial recognition technology and other biometric technologies through existing data-protection regimes, and proposals for more wide-reaching AI legislation in the EU.

One of the more developed forms of redress for biometrics-related harms has been established under data protection frameworks. Data protection agencies in various jurisdictions, including in

48 Access Now. (2021). *Ban Biometric Surveillance*. Available at: https://www.accessnow.org/ban-biometric-surveillance/

49 S.T.O.P. - The Surveillance Technology Oversight Project. *Workshop: Know Your Rights*. Available at: https://www.stopspying.org/training

50 Reclaim Your Face. *Reclaim Your Face*. Available at: https://reclaimyourface.eu/

51 Privacy International. *Ban biometric mass surveillance*. Available at: https://privacyinternational.org/campaigns/ban-biometric-mass-surveillance ; Liberty. *Human Rights coalition calls for immediate ban on facial recognition*. Available at: https://www.libertyhumanrights.org.uk/issue/human-rights-coalition-calls-for-immediate-ban-on-facial-recognition ; Big Brother Watch. *Stop Facial Recognition*. Available at: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

Canada, Australia and the EU, have pursued action against one facial recognition technology (FRT) vendor in particular, Clearview AI, for breaching privacy laws in its collection and analysis of pictures of people's faces without consent.[52,53] Most recently, Italy's data protection agency fined Clearview €20 million and ordered that Italian data obtained without a legal basis be deleted.[54] In France, CNIL ordered Clearview to delete French data that had been illegally collected.

In the UK, the Information Commissioner's Office (ICO) issued a fine of just over £7.5 million to Clearview AI, on the basis that, among other breaches, the company collected people's information without a legal basis, without transparency and used it in a way beyond people's expectations.[55] In the USA, Clearview will now be banned from selling its database to private companies and citizens nationwide, and from selling to law enforcement in the state of Illinois. Notably, however, Clearview plans to continue to sell its facial matching *algorithm* in the USA – just not its database.[56]

These cases rest on Clearview's database, created through the unlawful collection of publicly accessible face data, partially scraped from social media platforms. Clearview customers, such as law enforcement, would compare people in a surveilled area to this database to identify individuals. Limiting access to the database represents one avenue through which to limit the use of FRT. It does not, however, fully address the overarching issue of use of the technology itself, or the algorithm that allows matches to be made.

In the realm of direct regulation, in the USA, there have also been a set of temporary, city-level bans on use of FRT by police in cities including Portland, San Francisco, Oakland and Boston. These bans

52 Whittaker, Z. (2021). 'Clearview AI ruled "illegal" by Canadian privacy authorities'. *TechCrunch*. Available at: https://social.techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/

53 Lomas, N. (2021). 'Clearview AI in hot water down under'. *TechCrunch*. Available at: https://social.techcrunch.com/2021/11/03/clearview-ai-australia-privacy-breach/

54 Lomas, N. (2022). 'Italy fines Clearview AI €20M and orders data deleted'. *TechCrunch*. Available at: https://social.techcrunch.com/2022/03/09/clearview-italy-gdpr/

55 Information Commissioner's Office. (2022). *ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

56 Hatmaker, T. (2022). 'Clearview AI banned from selling software widely in the US'. *TechCrunch*. Available at: https://social.techcrunch.com/2022/05/09/clearview-settlement-bipa/

are largely in place for discrete periods of time until safeguards are in place. Recent reporting highlights that these bans may soon expire or be rolled back.[57] Legislators are beginning to examine uses beyond law enforcement, such as a proposed ban on using biometrics, in place of a key, to enter public housing in the USA.[58] The most far-reaching biometrics legislation in the USA is Illinois' Biometric Information Privacy Act, which regulates how private entities collect and use biometric data, including a requirement for companies to obtain written consent for collecting biometrics.

In the EU, the European Data Protection Supervisor and the European Data Protection Board have issued a broad call for banning biometrics that use AI to identify or classify individuals.[59] This represents a stricter set of prohibitions than those currently in the proposed draft EU AI Act, which also creates provisions that would apply to biometrics.[60]

The Act sets out categories of risk (unacceptable, high, limited and minimal) for all AI systems and assigns some types of biometrics into these categories. For example, real-time biometric identification systems by law enforcement in publicly accessible spaces (i.e. police use of live facial recognition) falls into the 'unacceptable-risk' category and would be prohibited, with a number of potentially broad exceptions, such as preventing imminent harm. Other uses of biometrics, including to categorise people or for emotion recognition, fall into the lower-risk category.

57 Dave, P. (2022). 'U.S. cities are backing off banning facial recognition as crime rises'. *Reuters*. Available at: https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/

58 No Biometric Barriers to Housing Act, H.R.4008, 117th Cong. (2021). Available at: https://www.congress.gov/bill/117th-congress/house-bill/4360?s=1&r=87

59 European Data Protection Supervisor. (2021). *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*. Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

60 Burt, C. (2021). 'European data protection regulator argues biometric surveillance restrictions not strong enough'. *Biometric Update*. Available at: https://www.biometricupdate.com/202104/european-data-protection-regulator-argues-biometric-surveillance-restrictions-not-strong-enough

In the UK: a growing consensus around the inadequacy of existing legal protections

Amid these global responses to biometric technologies, there have been a number of calls in the UK for action to strengthen biometrics governance, but few concrete policy steps taken by Government to date to address harms raised.

While varying in tone and focus, committees in the House of Commons and House of Lords, the Biometrics and Surveillance Camera Commissioner (the office responsible for oversight of some aspects of law enforcement use of biometrics in England and Wales) and judicial opinion all coalesce around the idea that there is not a sufficient legal framework in place to manage the unique issues that biometrics raise.

In 2018, the Home Office published the Biometrics Strategy, which laid out its uses of biometric services in the UK.[61] Notably, the strategy did not set out a plan for oversight of emerging biometric technologies. The then-Biometrics Commissioner responded: 'Given that new biometrics are being rapidly deployed or trialled this failure to set out more definitively what the future landscape will look like in terms of the use and governance of biometrics appears short sighted at best.'[62] Similarly, the House of Commons Science and Technology Committee's 2018 report on biometrics and forensics identified 'an urgent and significant need for action on the governance and oversight of both forensics and biometrics.'[63] The Committee called for a pause on the deployment of facial recognition by police beyond then-current pilots until concerns about accuracy were addressed.[64]

A subsequent Committee special report identified the same issues, characterising the Government's response as inadequate, and called for additional research into public attitudes towards biometrics and into the legal landscape covering biometrics.[65] In its 2021 response

61 Home Office. (2018). *Biometrics Strategy*. Available at: https://www.gov.uk/government/publications/home-office-biometrics-strategy

62 Biometrics Commissioner. (2018). *Biometrics Commissioner's response to the Home Office Biometrics Strategy*. Available at: https://www.gov.uk/government/news/biometrics-commissioners-response-to-the-home-office-biometrics-strategy

63 House of Commons Science and Technology Committee. (2018). *Biometrics strategy and forensic services*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf

64 'Facial recognition technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved.'

65 House of Commons Science and Technology Committee. (2019). *The work of the Biometrics Commissioner and the Forensic Science Regulator*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003.htm

to the Committee's special reports, the Government noted that the complexity of legal frameworks governing biometric data may inhibit the confident adoption of new technologies.[66]

The 2019 Conservative Party Manifesto acknowledged that new police technologies including biometrics and AI need to be used safely and 'within a strict legal framework'.[67] The Government has not yet acted on delivering this strict legal framework. In March 2022, the College of Policing, which provides professional guidance to law enforcement, published an authorised professional practice (APP) on live facial recognition (LFR).[68] This guidance, however, does not meaningfully limit police use of LFR and is not legally binding.[69]

In February 2020, a Private Member's Bill was proposed in the House of Lords to prohibit the use of automated facial recognition technology for overt surveillance in public places and to provide for a review of its use. This Bill did not progress beyond the first reading, but did indicate an interest in addressing a particular use case of biometric technologies that is of significant consequence for people.[70]

In Scotland, the Scottish Biometrics Commissioner Bill was introduced in April 2020, with the explicit purpose of addressing new forms of biometric technologies and creating an independent regulatory body. The bill encompassed both 'first generation' biometric data like fingerprints and DNA, and new biometrics that identify people, such as facial recognition technology, as well as biometric data used to categorise people.[71]

In England and Wales, the issue of facial recognition technology was taken up further in August 2020 in the landmark court case *R (Bridges) v Chief*

66 House of Commons Science and Technology Committee. (2021). *Work of the Biometrics Commissioner and the Forensic Science Regulator: Government Response to the Committee's Nineteenth Report of Session 2017–19*. Available at: https://publications.parliament.uk/pa/cm5801/cmselect/cmsctech/1319/131902.htm

67 The Conservative and Unionist Party. (2019). *Get Brexit Done: Unleash Britain's potential.* Available at: https://assets-global.website-files.com/5da42e2cae7ebd3f8bde353c/5dda924905da587992a064ba_Conservative%202019%20Manifesto.pdf

68 College of Policing. *Authorised Professional Practice: Live Facial Recognition*. Available at: https://www.app.college.police.uk/app-content/live-facial-recognition/?s=

69 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

70 *Automated Facial Recognition (Moratorium and Review) Bill*. (2020). Parliament: House of Lords. Bill no. 87. London: Published by authority of the House of Lords. Available at: https://bills.parliament.uk/bills/2610

71 Scottish Parliament. (2019). *Scottish Biometrics Commissioner Bill – Explanatory Notes.* Available at: https://www.parliament.scot/-/media/files/legislation/bills/current-bills/scottish-biometrics-commissioner-bill/introduced/explanatory-notes-scottish-biometrics-commissioner-bill.pdf

Constable of South Wales Police. The case highlighted the lack of a holistic legal framework to effectively govern facial recognition technology (FRT), finding that there are 'fundamental deficiencies' in the legal framework surrounding the police use of FRT.[72] However, as noted in Matthew Ryder QC's independent legal review, the interpretation of this ruling varies widely across individuals and organisations, and therefore does not itself function as clear guidance on the lawful deployment of the technology.[73]

Amid these various developments, the Home Office merged the previously separate offices of the Surveillance Camera Commissioner and the Biometrics Commissioner into one single office that oversees police use of biometrics (defined narrowly as fingerprints and DNA) and police and local authority compliance with the surveillance camera rules. Recently, the Department for Digital, Culture, Media and Sport consulted on moving the combined office under the Information Commissioner's Office (ICO). Currently, the Government response to the consultation proposes to dissolve the Office of the Biometrics and Surveillance Camera Commissioner, and to distribute its functions to other regulators, potentially moving casework functions to the Investigatory Powers Commissioner and moving surveillance-related functions to the ICO. Moving surveillance-related functions to the ICO resurfaces the question of whether the ICO can effectively enforce aspects of surveillance oversight that may fall beyond the ICO's typical data protection remit.[74] So while on the one hand, the Government's new proposal simplifies the existing oversight structure, it may also weaken the oversight of surveillance technologies.

In March 2022, the House of Lords Justice and Home Affairs Committee published an inquiry into the application of new technology in the arena of law enforcement, including FRT, and found that this technology is not sufficiently governed by existing legislation. This cross-party committee issued a strong call for Government to fill this gap in the law.[75]

72 Courts and Tribunals Judiciary. (2020). *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police and the Secretary for the State for the Home Department*. Case No: C1/2019/2670. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

73 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, paragraph 7.8. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

74 Biometrics Commissioner. (2022). *Biometrics Commissioner praises government on a 'decent job', but warns it's 'only half done'* Available at: https://www.gov.uk/government/news/biometrics-commissioner-praises-government-on-a-decent-job-but-warns-its-only-half-done

75 House of Lords Justice and Home Affairs Committee. (2022). *Technology rules? The advent of new technologies in the justice system*. Available at: https://committees.parliament.uk/publications/9453/documents/163029/default/

The Ada Lovelace Institute's research on the governance of biometric technologies: studies and methods

In light of the urgent societal questions posed by biometric technologies, the Ada Lovelace Institute has undertaken a three-year programme of work on the governance of biometric technologies, comprising three separate pieces of primary research.

1. To understand public attitudes towards biometrics, Ada began by conducting a nationally representative survey on UK public attitudes towards facial recognition technology (*Beyond face value*)[76] and convened the Citizens' Biometrics Council,[77] a public deliberation involving 50 UK adults to learn and then deliberate on biometrics in greater depth. The Council process also included a series of three Community Voice workshops focusing on communities particularly affected by biometrics.

2. To assess the efficacy of existing safeguards, we commissioned an independent legal review by Matthew Ryder QC (the 'Ryder Review').[78]

3. This report, which synthesises the findings from our public engagement research and the Ryder Review and consolidates the findings into policy recommendations.

76 Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

77 Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

78 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

Beyond face value – the first national survey of public attitudes to the use of facial recognition technology

In 2019, the Ada Lovelace Institute conducted a nationally representative survey of 4,109 UK adults' attitudes towards the use of facial recognition technology (FRT). The survey was administered online by public opinion and data analytics company YouGov between 12 and 16 July 2019.

Respondents to the survey were given a brief definition of facial recognition technology and answered questions about the proposed, potential or actual use of facial recognition in the following cases: policing, schools, companies, supermarkets, airports and public transport.

The national sample was weighted to the following UK demographics: gender, age, region and social grade (a classification system based on occupation). A large overall sample size was chosen to ensure that Black, Asian and minority ethnic groups formed a subsample large enough for specific analysis, with an unweighted base size that formed 6% of the total survey response. Within the response from Black, Asian and minority ethnic individuals, there was a higher level of discomfort with police uses of facial recognition technology than the overall average.

The Ada Lovelace Institute published analysis of the survey responses in *Beyond face value*. The full datasets from the survey are also available from the Ada Lovelace Institute's website.[79]

The Citizens' Biometrics Council – a public deliberation on biometric data and technologies

> 'We don't want to turn out to be like robots, and rely on biometrics. We have got human rights.'
>
> Citizens' Biometrics Council member, January 2022

79 Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ Data available at (opens spreadsheet): https://view.officeapps.live.com/op/view.aspx?src=https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Ada-Lovelace-Institute-Beyond-face-value-survey-results-for-publication-FINAL.xlsx&wdOrigin=BROWSELINK

In 2020, the Ada Lovelace Institute established the Citizens' Biometrics Council to deliberate on the use of biometric data and technologies. The Council's goal was to surface public perspectives to the debate on biometrics and build a deeper understanding of people's concerns, expectations and red lines.

The Council ran for eight months and involved 50 members of the public, who took part in over 60 hours of deliberative workshops (in-person and online). The process was designed and delivered in partnership with engagement specialists Hopkins Van Mil, with input from an independent oversight board of academics, technology developers, policing experts, regulators and researchers from the non-profit sector.

Council members were recruited to reflect different social and economic backgrounds, and political attitudes, as well as different perspectives on data and technology. We also conducted three focus groups with individuals from marginalised groups that existing research identified as most likely to bear a disproportionate burden of the risks of biometric technologies: people from Black, Asian and minority ethnic backgrounds, people who identify as LGBTQ+ and disabled people. Participants from these groups also sat on the Council.

During the workshops, Council members considered evidence about biometric technologies, heard from experts from a range of backgrounds, including civil society leaders, members of industry, regulators, law enforcement technologists and policy professionals, and participated in facilitated discussion. Throughout this process, Council members addressed a question they devised themselves: 'What is or isn't ok when it comes to the use of biometrics?'. The Council developed a set of recommendations to answer this question and conclude their deliberation, which Ada published in a report in March 2021.[80]

In January 2022, Ada reconvened a group of the Council's members in an independently facilitated online workshop, where we presented a draft of the recommendations presented in this paper. We sought their input on how we had represented the Council's recommendations in our policy-facing recommendations, and gathered feedback to further refine them.

80 Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

The Ryder Review – an independent legal review of the governance of biometric data in England and Wales

In 2020, the Ada Lovelace Institute commissioned Matthew Ryder QC to conduct an independent legal review of governance of biometric data in England and Wales. The Review had a remit to conduct an independent, impartial and evidence-led analysis of the governance of biometric data in England and Wales, and to reach conclusions and make recommendations on regulatory reform. The Review was led by Matthew Ryder QC, with a team comprising Jessica Jones, Javier Ruiz and Samuel Rowe.

The work of the Review involved three core strands: research undertaken by the Review team, interviews with various interested parties; and liaison with an Advisory Board.

The research undertaken by the Review team covered academic literature, articles from reputable media outlets on the uses of and debate around biometric data and technologies, and reports and papers from research institutes, think tanks, charities and advocacy organisations. The Review team also engaged with technical literature on biometrics. The scope of research was not limited to the UK, but also included analysis of international developments, predominantly in the USA and the EU.

The Review took evidence from 24 individuals over a series of interviews conducted between September 2020 and February 2021. Interviews lasted between an hour and an hour-and-a-half and addressed a series of themes identified by the Review team as being of particular interest, with sufficient flexibility to respond to the particular interests and expertise of interviewees.

The Review spoke to, among others, the Biometrics Commissioner, the Forensic Science Regulator, the Surveillance Camera Commissioner, Home Office ministers, the Information Commissioner's Office, the Metropolitan Police Service, West Midlands Police, the College of Policing, the Centre for Data Ethics and Innovation, AI Now, Liberty and Big Brother Watch.

The Review team was also assisted by several meetings with an Advisory Board,[81] consisting of experts in criminology, sociology, advocacy, digital and data policy, genetics and data protection law. The Advisory Board provided direction, resources and contacts, and asked questions that helped to steer the focus of the Review. The Review was published in June 2022, and can be found on our website.[82]

81 See: Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, Annex 3. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

82 Ryder, M. (2022).

Findings of public engagement research and legal review

This section groups thematically the findings of the public engagement research, followed by the findings of the independent legal review.

1. Public attitudes towards biometrics are highly contextual

> 'Using [biometric technology] for self-identification, for example to get your money out of the bank, is pretty uncontroversial. It's when other people can use it to identify you in the street, for example the police using it for surveillance, that has another range of issues.'
>
> Citizens' Biometrics Council member, September 2020

Our research found that there is not widespread public acceptance of, or support for, the use of biometrics without conditions, limitations and safeguards. People's comfort levels with biometrics largely depends on the context in which biometrics are used, and to some extent, on the degree to which they would be disproportionately affected by the harms of biometrics. Regardless of the context of use or background, members of our Citizens' Biometrics Council considered biometric data highly sensitive, based on its intrinsic link to personal identity.

People are generally uncomfortable with facial recognition technology (FRT) being used by private actors. For instance, in our 2019 survey, we found that 77% of people said they were uncomfortable with FRT being used in shops to track customers and 76% were uncomfortable with it being used by HR departments in recruitment. In the case of other services, the majority of people were opposed to the use of facial recognition in schools (67%) and on public transport (61%).

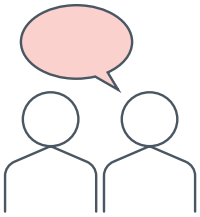
People do not trust companies to use facial recognition technology in an ethical way.

77%

of people are uncomfortable with the prospect that facial recognition technology could be used by shops to track customers.

70%

of these cite the reason as a lack of trust in companies to use the technology ethically.



76%

of people are uncomfortable with the prospect that facial recognition technology could be used in human resources for recruitment.

63%

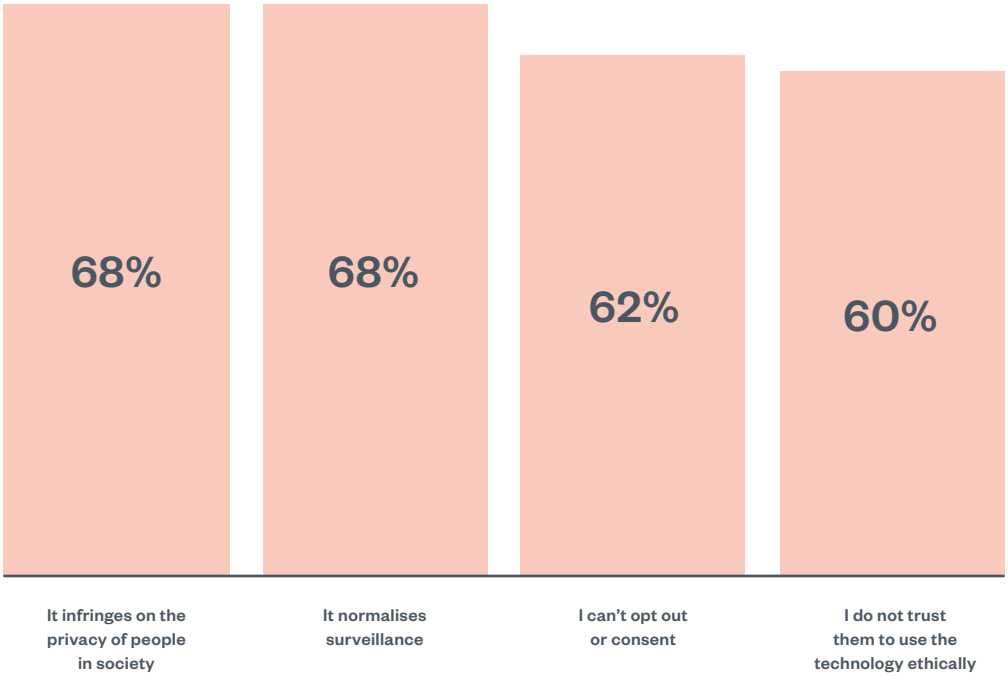
of these cite the reason as a lack of trust in companies to use the technology ethically.

When there is a perceived benefit, the public is more comfortable with uses of FRT – if appropriate safeguards are in place. For example, 54% of people were comfortable with the use of facial recognition for smartphone locking systems, and 50% were comfortable with the idea of facial recognition in airports to replace passports – again, assuming appropriate safeguards are in place.

When it comes to police use of facial recognition, 70% think police should be able to use FRT in crowds and in public spaces, if it helps them reduce crime. Simultaneously, however, 55% of people thought that the Government should limit the use of FRT so that the police can only use it in specific circumstances, like on CCTV footage from crime scenes. 29% of people were uncomfortable with police use of facial recognition.[83] Reasons for this included: infringement on people's privacy, the normalisation of surveillance, the inability to opt out or consent, and a lack of trust in the police to use the technology ethically.

83 The survey asked respondents: 'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with police using facial recognition technology in this way?', with 'uncomfortable' referring to people scoring 1 to 5 on this question.

The top four reasons given for discomfort around police uses of facial recognition technology relate to privacy, surveillance, consent and ethics.



Reasons for discomfort with police use of facial recognition technology as cited by those who are uncomfortable with this use (29% of respondents).

Importantly, within the response from Black, Asian and minority ethnic individuals, there was a higher level of discomfort with police use of facial recognition technology than the overall average.[84] Given that facial recognition can be less accurate on people of colour, and the well-documented over-policing of Black and Asian communities in the UK, this difference in level of comfort is not surprising. However, it does illustrate the limitation of using aggregate statistics as a standalone indicator of public attitudes towards facial recognition technology. In other words, in the present UK context, those most negatively affected are not in the majority.

84 34% of Black, Asian and minority ethnic respondents said that day-to-day police use of facial recognition should be permitted, with appropriate safeguards, compared to 50% of White respondents. See further: Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ | Data available at (opens spreadsheet): https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.adalovelaceinstitute.org%2Fwp-content%2Fuploads%2F2019%2F09%2FAda-Lovelace-Institute-Beyond-face-value-survey-results-for-publication-FINAL.xlsx&wdOrigin=BROWSELINK

In partial recognition of this key limitation, the Citizens' Biometrics Council sought to assess public attitudes towards facial recognition in a more deliberative way that allowed people to explain their reasoning, and in which risks to marginalised groups were explained and contextualised.

2. The public are concerned about particular harms arising from biometrics

Bias and discrimination that arises from differential accuracy and use

Our research demonstrated that people have serious concerns about the risks, bias and discrimination posed by biometric technologies. When considering evidence of differential accuracy, members of our Citizens' Biometrics Council were concerned that inaccuracy means technologies can cause erroneous or harmful outcomes. Many shared personal experiences where they, or someone they knew, had suffered because of a technical error. Accuracy is a particular issue for minority groups, who tend to be underrepresented in the training data.

Council members recognised that discriminatory experiences could be exacerbated by biometric technologies. They considered how biometric data has an 'intimate and permanent nature', relating to people's physical bodies and intertwined with people's experiences of their own identity. Not only does this heighten the sensitivity of the data – as is recognised by the inclusion of biometric data (when used for identification) as a special category in UK data protection law – but it heightens the sensitivity of the impacts on people when biometric technologies cause discrimination.

Harms resulting from bad science: problematic, stereotypical or unproven underlying assumptions

The Council expressed concerns about technologies that classify people according to reductive, ableist and stereotypical characteristics, causing harm both to people's wellbeing and as a result of being wrongly characterised within a database or data-driven system. One member shared:

> 'My voice is soft; I have a sibilant 'S'. I lisp slightly and this is often a way that people use to recognise my sexuality or to make an assumption about me. I've had that my whole life. Now, that makes me anxious about voice recognition technology, because I know that the average person in the street makes these assumptions about me, and I don't want technology making that assumption about me as well.'
>
> Citizens' Biometrics Council member, January 2022

Infringement on privacy and free expression

The potential for biometric technologies, particularly remote biometric technologies, to hamper free expression, assembly and association, and infringe on privacy – whether attending a protest, or participating in other civil expression – was of paramount concern.

Issues of oversurveillance and infringements on people's liberties and privacy were serious concerns of the Council. As well as references to 'Big Brother' and 'police states', Council members raised concerns about how other countries, both historically and in recent years, have oppressed people and diminished their privacy through surveillance. The phrase 'who watches the watchers' was raised more than once in discussions. Many Council members considered some loss of privacy through surveillance as a trade-off for living in a society which is kept safe from crime or other harms: 'If it's for national security reasons, and now COVID, then I'm not too bothered.' But they also recognised that trade-offs must be balanced carefully, and some rights must never be infringed.[85]

85 Ada Lovelace Institute. (2021). *The Citizens Biometrics Council,* p.26. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

> ‘What’s the point of it? Why do you feel the need to be able to control people or have these technologies in place? It’s all about control.’
>
> Citizens’ Biometrics Council member, January 2022

3. The public want robust safeguards, including comprehensive legislation, independent oversight and minimum standards

> ‘Legislation should be passed to stop abusive technology being used to victimise people.’
>
> Citizens’ Biometrics Council member, January 2022

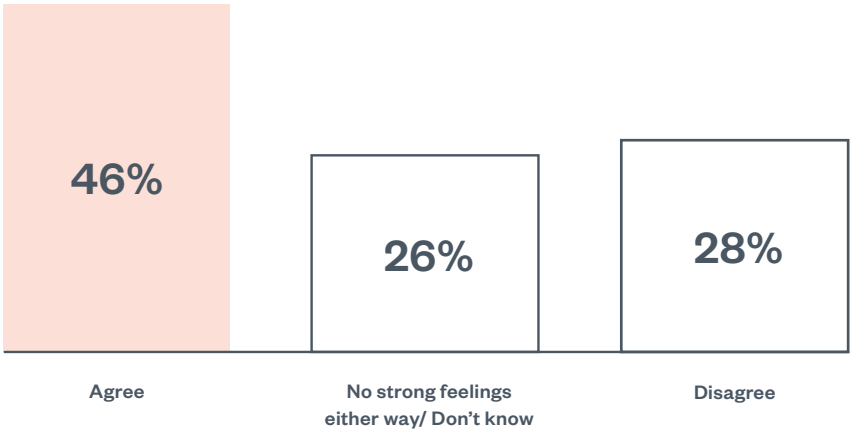
The Citizens’ Biometric Council recognised the potential benefits of tools like facial recognition in certain circumstances, such as addressing crime, but called for stronger legislation, regulation and oversight of the uses of biometric technologies and data.

Their recommendations included specific requirements for the destruction of biometric data beyond reasonable limits, including in policing contexts – as well as the development of more comprehensive legislation and regulation for biometric data and technologies, and the establishment of an independent, authoritative body to provide oversight of updated legislation and governance. They also raised concerns about data management and retention, bias and discrimination, and oversurveillance.

Council members felt that consent was both an important safeguard and a critical component in ensuring that the use of biometrics is ethical. They recognised the various technological and practical challenges around offering consent mechanisms, and accepted that in some circumstances consent might not be part of an appropriate legal basis, such as in health emergencies or where there is a serious threat to public safety.

However, where biometric technologies are used in other settings without such potentially serious consequences – such as age verification in shops, fraud prevention or membership systems – Council members considered explicit consent mechanisms and adequate opt-out options for individuals to be necessary. Similarly, nearly half (46%) of survey respondents thought they should be able to consent to, or opt out of, the use of facial recognition technology.

46% of people think the public should be able to opt out of or consent to facial recognition technology.



Q: How much do you agree or disagree with the following statement?

The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology.

Council members often expressed the view that uses of biometrics must be transparent and accountable. This is necessary to ensure that its uses are responsible, and to enable people to be sufficiently informed when consenting. Many Council members, however, felt that currently both accountability and transparency were lacking.

> 'If the technology companies break their promises... what will the implications be? Who's going to hold them to account?'
>
> Citizens' Biometrics Council member, January 2022

In terms of the public appetite for stronger Government action on biometrics, there is limited support for the Government to ban the use facial recognition technology (FRT). 65% of survey respondents disagreed with a Government ban on all facial recognition technology in policing. This is echoed by the Council, who did not call for sweeping bans.

However, as noted above, the majority of the UK public support the idea that the Government should *limit* the use of FRT: 55% of people agree that the Government should limit police use of facial recognition to specific circumstances, and 68% agree that the Government should limit schools' use of FRT.

There was also public support for a voluntary undertaking by companies not to sell facial recognition technology to police or to schools until there has been more public consultation: 50% of people agreed the private sector should not sell the technology to police and 70% of people agreed the private sector should not sell the technology to schools.

The Citizens' Biometrics Council concluded with a set of recommendations aimed at UK policymakers that clustered around three themes:

1. Developing more comprehensive legislation and regulation for biometric technologies.
2. Establishing an independent, authoritative body to provide robust oversight.
3. Ensuring minimum standards for the design and deployment of biometric technologies.

Their recommendations articulate clear public demand for updated and specific legal frameworks for biometric data and technologies that ensure they are developed and deployed to high standards. There is also public demand for uses of biometric technologies to be overseen or investigated by an independent body that has the 'teeth' to hold those using those technologies to account.

> ‘We want somebody to make sure that all this biometric data ... which is a great, powerful tool... is well maintained and regulated, and used responsibly.’
>
> Citizens’ Biometrics Council member, January 2022

Existing safeguards are not fit for purpose

Given the strong call from the public for safeguards around the use of biometrics, it is important to understand what existing safeguards do and do not cover, and the extent to which protections are in place in theory and practice. In regards to these questions, the Ryder Review finds that the current legal framework governing biometrics is not fit for purpose.

Current governance and regulatory structures are fragmented and unclear

The Review finds that the current governance of biometric data relies on a patchwork of overlapping laws addressing data protection, human rights, discrimination and criminal justice issues. Oversight and regulatory structures were also found to be similarly unclear and fragmented. This fragmentation of law and oversight leads to a lack of clarity on when and how biometric technologies can be lawfully deployed. For instance, police witnesses to the Review spoke of how difficult it is currently to know who to go to for advice and guidance on biometric data.

The Review notes that the gaps in current governance structures for biometrics are well-illustrated by the Court of Appeal’s judgement in *R (Bridges) v Chief Constable of South Wales Police*. The Court of Appeal found that South Wales Police’s use of live facial recognition (LFR) was a breach of law due the absence of a sufficient legal framework to govern its use. Specifically, the judgement stated that, while the police do have a common-law power to use LFR, the exercise of that power was not in accordance with the law, because there was an insufficient legal framework in place to protect individual rights – specifically, to provide adequate legal basis for interference with the right to privacy

as enshrined in Article 8 of the European Convention on Human Rights. However, as the Review highlights, there is not a unified understanding of this ruling, nor agreement about how this ruling translates into practice.

Existing Biometrics Commissioner lacks the powers and authority to comprehensively govern the use of biometric data

The experts informing the Review expressed concerns about whether existing regulatory bodies had the powers and authority required to effectively govern the use of biometric data in England. In evidence provided to the Review, the former Biometrics Commissioner wondered whether the commissionership 'does the job legislators intended' because it is 'too easy to side-line and there are no obligations on relevant bodies in Parliament or in Government' to meet with or take the Commissioner's recommendations into account. By contrast, there was some positivity about the approach adopted in Scotland, where the Biometrics Commissioner has greater independence, being appointed by the Scottish Parliament rather than the Executive.

The current framework fails to support effective *ex ante* regulation

A significant weakness raised by interviewees about the current legal system is that it only permits complaints to be raised once there has been a breach of a rule, but does not provide sufficient prior protection to prevent those breaches from occurring.

Data protection law does not consider biometrics for categorisation special category data

Under UK data protection law, biometric data is only given special category status where it is used for the purposes of uniquely identifying a natural person. A consequence of this is that biometric data used to categorise individuals, for instance, to determine a person's gender, race or emotional state, is not unequivocally subject to the most stringent legal restrictions placed on the same data when used for the *identification* of individuals.

It is important to note that biometric data used for categorisation or classification is considered as personal data under UK data protection law: if people can be identified indirectly or identified through additional information, then it is personal data. However, there may be emerging

uses of biometrics where it is not possible to link back to an individual in any case, which may fall beyond this definition. Furthermore, the fact that special category status is not automatically given to biometric data collected for categorisation or classification, was considered as a potential weakness by the Review team, as it could make enforcement subject to challenge.[86]

The Review suggests that the use of biometrics for classification or categorisation has the potential to be just as rights-intrusive as their use for unique identification and that similarly high safeguards should therefore apply.

Human rights law applies to public services

The Review observes that many of the protections provided by the current legal framework are derived from human rights law. This means that human rights law regulates the treatment of individuals by public authorities, but does not typically regulate the treatment of individuals by private entities. As noted in the Review: 'Private companies do not, generally, owe human rights obligations towards individuals, and this is a potential lacuna in the regulation of biometric data use by entities other than public bodies.'

Based on the above findings, the Ryder Review issued a set of 10 recommendations, reproduced in the Annex below.

86 Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, paragraph 8.14. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

Conclusions

In this report, we have aimed to produce a thorough study, by providing background on recent developments in biometric technology and governance, surfacing public engagement research on biometric technologies and summarising evidence from an independent legal review of biometrics governance.

Given our focus on the governance of biometrics in the UK, we have not addressed situations and solutions outside the UK, though we recognise that this is of huge importance. In particular we recognise that more research and attention is needed on the way militaries collect biometric data and use biometric technologies,[87] leading to the establishment of norms that uphold human rights for all.

Additionally, although we have raised the importance of biometrics in non-public services, there is currently a lack of evidence to draw from when it comes to biometric technologies in the private sector more broadly. In noting this gap, we echo the Ryder Review's recommendation that more research is undertaken with this explicit focus.

Within our evidence base, we highlighted the fact that the public considers biometric data uniquely sensitive due to its intrinsic link to an individual. Because of this sensitivity, even in cases where there is a perceived public benefit, such as in some instances of policing, people underscore the need for proportionality and safeguards. Polling shows that people's attitudes towards biometric technologies depend on the circumstances in which they are used. The majority of people are opposed to the use of facial recognition in schools, shops, public transit and in hiring.

There are significant public concerns about the negative impact of biometric technologies for free expression, free association, free assembly and privacy, as well as concern about biometrics being used entrench bias and discrimination. This concern not only stemmed from

87 Vallance, C. (2021). 'Afghanistan: Will fingerprint data point Taliban to targets?'. *BBC News*. Available at: https://www.bbc.com/news/technology-58245121

differential inaccuracy, but also concerns that biometrics would be used to make decisions on the basis of stereotypes and the potential for oversurveillance. Across the board, people wanted to see strong safeguards in place.

Matthew Ryder QC's assessment of the existing landscape of biometrics governance in England and Wales finds that legal frameworks are not fit for purpose. Existing oversight structures are found to be patchy and ineffectual. Legal frameworks do not currently account for preventing all harms before they take place, are set up to allow for redress only after the fact, and may not unequivocally cover all emerging uses of biometric data.

Based on our public engagement research and the Ryder Review, we ultimately make the case and provide a blueprint for new primary legislation to govern biometric technologies. Our recommendations follow below.

Policy recommendations

1. **Government should pass new, primary legislation to govern the use of biometric technologies. New legislation must address uses of biometrics for both categorisation and identification, and should apply to the deployment of biometric technologies by both public and private actors.**

   The Citizens' Biometrics Council considers biometric data intrinsically sensitive, because it relates to an individual's personal identity. As the Ryder Review identifies, the data collected by biometric technologies used for categorising people is not subject to the highest level of safeguards and existing data protection legislation does not provide adequate legal restrictions or individual control over these technologies. This legislation must also explicitly address the impact biometric technologies have on human rights, including privacy and free expression when used by private actors.

2. **The oversight and enforcement of this legislation should sit within a new regulatory function focused on biometric technologies, which is national, independent, and adequately resourced and empowered.**

   The Citizens' Biometrics Council emphasised the importance of an independent oversight body that operates with transparency and accountability. The Ryder Review characterises current oversight arrangements as overly complex and incomplete. This recommendation seeks to consolidate and strengthen existing powers, as well as to create new forms of public transparency and accountability. Recognising that the Information Commissioner's Office (ICO) is the regulator for the personal data aspects of biometric technology, this function could sit on its own statutory footing within the ICO, or at least work closely with the ICO to coordinate enforcement efforts. In any case, this regulatory function would need to deliver a unique agenda (see Recommendation 3), and would need its own features, including the below:

   a. This function should publish a register of uses of biometrics by the public sector, and should identify wider market trends in the public

and private sectors through an annual report made to Parliament. Relevant or specifically identified Government departments, including the Home Office, the Department for Digital, Culture, Media and Sport and Department for Education, should be required to respond to the report on an annual basis.

b. A part of its continuous monitoring, this function should set up an ombudsperson to receive complaints from people affected by biometric technologies.
c. This function should be accountable to multiple Government departments and ultimately to Parliament to reflect the use and scope of biometric technologies beyond law enforcement.

3. **This regulatory function should oversee the assessment of biometric technologies on two levels. Firstly, it should require that *all* biometric technologies meet scientifically based and clearly established standards of accuracy, reliability and validity. Secondly, it should assess the proportionality of biometric technologies in their proposed contexts, prior to use, for those that are used by the public sector, in public services, in publicly accessible spaces, or that make a significant decision about a person. In addition, it should undertake monitoring of the development and use of all biometric technologies, which could trigger the creation of codes of practice that may include bans or moratoria.**

Ensuring technologies meet technical standards may partially address issues of pseudo-science, bias and discrimination present in the systems themselves. Where systems do function accurately, reliably and on a valid basis, the proportionality test is in place to assess impact on human rights that stem from the context of use. In response to the finding that people's comfort with biometrics is highly dependent on the context, using a proportionality test allows the regulatory function to consider a technology's purpose of use. This also reflects the fact that the same modular biometric technology may be more or less harmful in certain contexts. Technologies which do not require a proportionality test will still be monitored, and the regulator will have powers to intervene in different ways.

a. The regulatory function should be responsible for informing the creation of standards, working with independent academic and research entities and/or international standards-setting

bodies. Standards should account for accuracy, reliability and the underlying scientific validity of biometric technologies. All technologies would need to meet standards once they are developed. In the meantime, the regulatory function could establish its own temporary standards that vendors would need to meet to establish the functionality of biometric technologies.

b. For uses in the public sector, public services, publicly accessible spaces or for making a significant decision about a person, where standards of accuracy, reliability and validity are met, the regulatory function must undertake a proportionality test prior to the procurement of or decision to use biometric technologies. This will assess proportionality in the proposed contexts of use on the basis of internationally recognised human rights standards. This proportionality test should consider individual harms, collective harms and societal harms that may arise from the use of biometric technologies. If approval is granted, the regulatory function should monitor the technology during its deployment and implementation stages, and continuously as long as the system is in use.

c. The regulatory function should undertake market monitoring of the development and deployment of biometric technologies, and assess uses on the basis of considering factors such as: one-to-one versus one-to-many matching systems; proportionality of impact and benefit versus potential harms to individuals or groups; and likely outcome of system failure, security breach or large-scale malfunctions. As well as reporting annually, the regulatory function could undertake investigation and request the creation of new sector-specific codes of practice informed by individual regulators and the biometrics regulator function. This could include legally binding guidance on the use of biometrics in specific settings, which could include moratoria for use, for example, of biometric technologies in schools.

d. In developing approaches to standards and the human rights-based proportionality test, the regulatory function should explicitly consider, account for the experiences, and seek the direct participation of marginalised and minoritised groups of people.

4. **There should be a moratorium on the use of biometric technologies for one-to-many identification in publicly accessible spaces and for categorisation in the public sector, for public services, and in publicly accessible spaces until comprehensive legislation is passed.**

Case studies

Verification: facial recognition technology in school lunch queues

As reported by the *Financial Times*, in October 2021, nine schools in North Ayrshire, Scotland started using facial recognition technology to verify students' identities in order for them to pay for their lunch.[88]

The idea behind the programme, according to the informational flyer sent to parents from the vendor CRB Cunninghams,[89] was to give students a contactless way to pay, without needing a PIN or card. The flyer advises: 'With Facial Recognition, pupils simply select their meal, look at the camera and go, making for a faster lunch service whilst removing any contact at the point of sale.'

In order to be compliant with data protection legislation, the schools gave families the choice to opt in. According to the FT, 97% of families opted in, but some later said they were not sure about what they were opting into.

After considerable pushback over privacy concerns, the ICO made enquiries about this practice and said that, 'Organisations should consider using a different approach if the same goal can be achieved in a less intrusive manner.'[90]

The central ethical question in this instance was whether it was proportionate and necessary to collect face data given the context of buying school lunch. In this instance, campaigners, school community members and the regulator expressed concern that it was not proportionate.

88 O'Murchu, C. (2021). 'Facial recognition cameras arrive in UK school canteens'. *Financial Times*. Available at: https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9.

89 CRB Cunninghams. 'We're introducing Facial Recognition!'. *North-ayrshire.gov.uk*. Available at: https://www.north-ayrshire.gov.uk/Documents/EducationalServices/facial-recognition-parental-flyer.pdf

90 Weale, S. (2021) 'ICO to step in after schools use facial recognition to speed up lunch queue'. *The Guardian*. Available at: https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk

Effect of proposed legislation:
Under Ada's proposed legislation, this consideration would have taken place *before* the technology was deployed in schools. The technology would have had to meet standards of accuracy, reliability and validity to be considered for procurement, and then the regulatory function would have directly assessed the human rights impact (including privacy) of such a system. The regulatory function would have had to consult with those who would be potentially marginalised by this system. Only if it had passed that test of proportionality and necessity would it have been rolled out.

Identification: surveillance of shoppers at supermarkets

In January 2022, the *Mail on Sunday* reported that the Southern Co-op supermarket chain used live facial recognition technology (LFR) in a number of shops to monitor customers as they shopped for groceries.[91] This followed reports in 2020 that the same company used LFR in 18 stores in southern England.[92]

The stated goal of the technology is to reduce shoplifting. Cameras scan the faces of customers and compare them to a database of individuals. If a match is made, store employees are notified on their smartphones. The technology vendor, Facewatch, explains in a blog post, 'The system alerts our store teams immediately when someone enters their store who has a past record of theft or anti-social behaviour.' [93]

It is not known exactly what constitutes anti-social behaviour or how a person ends up or contests their place on a watchlist. Facewatch does state that it combines watchlists across store locations into one central, national database. Matches made can then be used as evidence 'before entering in discussions with the local police'.[94]

In the same blog post, the company claims that their technology complies with data protection law because there are signs posted within

91 Ryan, J. (2022). 'Co-op are using cameras made by Chinese state-owned company'. *Mail Online*. Available at: https://www.dailymail.co.uk/news/article-10406421/Co-op-using-cameras-Chinese-state-owned-company-track-shoppers.html

92 Burgess, M. (2020). 'Co-op is using facial recognition tech to scan and track shoppers'. *Wired UK*. Available at: https://www.wired.co.uk/article/coop-facial-recognition

93 Greenfield, S. (2020). 'Facewatch at the Southern Co-op'. *Facewatch*. Available at: https://www.facewatch.co.uk/2020/10/05/facewatch-at-the-southern-co-op/

94 Greenfield, S. (2020).

stores alerting customers that this technology is in use. It is not clear that all customers are aware that this technology is present, nor can they opt out. Facewatch conducted an impact assessment of its own practices and states that they are necessary and proportionate, and therefore compliant with UK data protection legislation. [95]

The use of live facial recognition in supermarkets to catch suspected shoplifters based on a non-transparent list of suspects raises issues of privacy and due process, and potentially bias and discrimination if the technology produces a disproportionate number of false positives for minoritised groups. Even if the technology itself functions accurately for all demographic groups and skin tones, there may still be a disproportionately high rate of false positives for minoritised groups if store employees add a disproportionate number of minoritised individuals to the watchlist.

Effect of proposed legislation:
Under Ada's proposed legislation, a vendor would first need to prove that the technology meets technical standards of accuracy, reliability and validity. Given that this deployment is in a public space, the regulatory function would assess the human rights impact of the risks identified above prior to the use of such a system in supermarkets. This approval process would necessarily involve the consultation and direct participation of minoritised groups. Only if deemed necessary and proportionate, based on a human rights impact assessment, would the deployment be lawful.

Categorisation: emotion identification in hiring

In 2019, the *Washington Post* reported that technology that automatically analysed candidates' biometric data, like facial expressions and tone, in video job interviews was being used to determine who to hire.[96]

95 Privacy International. (2020). *Cooperating With Who?! Answers Needed as UK Retailer Southern Co-Op Tests Facewatch*. Available at: http://privacyinternational.org/advocacy/4342/cooperating-who-answers-needed-uk-retailer-southern-co-op-tests-facewatch

96 Harwell, D. (2019). 'A face-scanning algorithm increasingly decides whether you deserve the job'. *Washington Post*. Available at: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/

The system, made by US-based vendor HireVue, used artificial intelligence to assess thousands of datapoints from video interviews and scored candidates on characteristics like 'enthusiasm,' 'willingness to learn,' 'conscientiousness & responsibility' and 'personal stability'. These were then used to generate an overall 'employability' score, benchmarked against the performance of a company's existing top performers. At the time of the reporting, more than 100 employers used HireVue, including multinationals Unilever and Hilton.

In using this technology, employers intend to make hiring more efficient and to remove the human bias known to affect regular recruitment processes. But some AI researchers raised a fundamental issue with the functionality of the system, which was built on the premise that facial expressions can reveal inner qualities or job competencies.[97]

Challenging this premise, researchers cited scientific evidence demonstrating that it is not possible to accurately infer emotion from facial expressions. Attempting to link the two may involve the assumption that everyone expresses emotions in the same way, or favour certain dominant forms of expression.[98] Regardless of whether this leads to discriminatory decisions, the underlying scientific basis was known not to be valid, reliable or accurate. Given the high-stakes nature of gaining employment, using a pseudo-scientific basis for decision-making was considered a harm in and of itself.[99]

Based in part on lack of proven accuracy, validity or reliability, the advocacy group Electronic Privacy Information Center filed a complaint against HireVue with the US regulator for consumer protection and competition. HireVue later removed the facial expression analysis from its offering.[100]

Since HireVue's rollback, there have been a number of new products and systems that claim to be able to read an individual's inner state from

97 Harwell, D. (2019).

98 Engler, A. (2019). 'For some employment algorithms, disability discrimination by default'. *Brookings Institute*. Available at: https://www.brookings.edu/blog/techtank/2019/10/31/for-some-employment-algorithms-disability-discrimination-by-default/

99 Note: There was also a risk that this system could make bias worse through its algorithmic ranking of candidates. By rating new candidates based on the performance of existing high performers, the employer could end up screening out qualified candidates, not because of their employability, but simply because they looked or sounded different to the existing employees. HireVue conducted tests of its systems and did not find discrimination in this way.

100 Electronic Privacy Information Centre. (2021). *HireVue, Facing FTC Complaint From EPIC, Halts Use of Facial Recognition*. Available at: https://epic.org/hirevue-facing-ftc-complaint-from-epic-halts-use-of-facial-recognition/

external biometric data. In 2022, Intel advertised a new system that attempts to detect whether students are paying attention in a virtual classroom by reading their facial expressions.[101] Another vendor is attempting to monitor sales pitches made over Zoom in order to assess the 'emotional state' of the virtual interactions.[102]

Effect of proposed legislation:
Under Ada's proposed legislation, this vendor would have needed to demonstrate that its system meets standards of accuracy, reliability and validity prior to its use in a real-world hiring situation. An employer would be able to check whether a system they are considering buying meets standards. Were standards met, this particular use of emotion recognition in employment would be subject to a proportionality test because of the context of making a significant decision about a person. The regulatory function could issue a legally binding code of practice on emotion recognition in employment to address use cases more broadly. This code of practice could be drafted in concert with the Equalities and Human Rights Commission – the sector regulator for employment.

101 Kaye, K. (2022). 'Intel thinks its AI knows what students think and feel in class'. *Protocol*. Available at: https://www.protocol.com/enterprise/emotion-ai-school-intel-edutech

102 Kaye, K. (2022) 'Companies are using AI to monitor your mood during sales calls. Zoom might be next'. *Protocol*. Available at: https://www.protocol.com/enterprise/emotion-ai-sales-virtual-zoom

Annex 1: Ryder Review recommendations

Recommendation 1: There is an urgent need for a new, technologically neutral, statutory framework. Legislation should set out the process that must be followed, and considerations that must be taken into account, by public and private bodies before biometric technology can be deployed against members of the public.

Recommendation 2: The scope of the legislation should extend to the use of biometrics for unique identification of individuals, *and* for classification. Simply because the use of biometric data does not result in unique identification does not remove the rights-intrusive capacity of biometric systems, and the legal framework needs to provide appropriate safeguards in this area.

Recommendation 3: The statutory framework should require sector and/or technology-specific codes of practice to be published. Such codes should set out specific and detailed duties that arise in particular types of cases.

Recommendation 4: A legally binding code of practice governing the use of lifefacial recognition (LFR) should be published as soon as possible. We consider that a specific code of practice for police use of LFR is necessary, but a code of practice that regulates other uses of LFR, including use by private entities and public-private data sharing in the deployment of facial recognition products, is also required urgently.

Recommendation 5: The use of LFR in public should be suspended until the framework envisaged by Recommendations 1 and 4 is in place.

Recommendation 6: The framework envisaged by Recommendations 1 and 4 should supplement, and not replace, the existing duties arising under the Human Rights Act 1998, Equality Act 2010 and Data Protection Act 2018.

Recommendation 7: A national Biometrics Ethics Board should be established, building on the good practice of the London Policing Ethics Panel and West Midlands Police, and drawing on the expertise and experience of the Biometrics and Forensics Ethics Group. This Board should have a statutory advisory role in respect of public-sector biometrics use.

Recommendation 8: The Biometrics Ethics Board's advice should be published. Where a decision is taken to deploy biometric technology contrary to the advice of the Biometrics Ethics Board, the deploying public authority should publish a summary explanation of their reasons for rejecting the Board's advice, or the steps they have taken to respond to the Board's advice. The public authority's response should be published within 14 days of the decision to act contrary to the Biometrics Ethics Board's advice and prior to deployment.

Recommendation 9: The regulation and oversight of biometrics should be consolidated, clarified and properly resourced. The overlapping and fragmented nature of oversight at present impedes good governance. We have significant concerns about the proposed incorporation of the role of Biometrics and Surveillance Camera Commissioner into the existing duties of the ICO. We believe that the prominence and importance of biometrics means that it requires either a specific independent role, and/or a specialist Commissioner or Deputy Commissioner within the ICO. Wherever it is located, it must be adequately resourced financially, logistically, and in expertise, to perform the governance role that this field requires.

Recommendation 10: Further work is necessary on the topic of private-sector use of biometrics. While we consider that the statutory framework envisaged by Recommendation 1 must regulate private-sector use to some extent, many of those we interviewed had extensive knowledge about public-sector use of biometrics but much less experience and expertise in the challenges and issues arising in the private sector. There are plainly considerable, rights-engaging concerns around private-sector use of biometrics, but we have not received enough private-sector input to the Review to be able to propose detailed solutions. We recommend that further, private- sector-specific research and evidence gathering is undertaken. This is particularly important given the porous relationship between private-sector organisations gathering and processing biometric data and developing biometric tools, and public authorities accessing those datasets and deploying those tools.

Acknowledgements

We would like to thank the following individuals for taking time to review a draft of this report, or for offering their expertise and feedback on recommendations: multiple team members of the Information Commissioner's Office, Areeq Chowdhury (Royal Society), Professor Pete Fussey (University of Essex) and Brenda Leong (BNH.AI, Pennsylvania State University Law School).

The reviewers were not asked to endorse the conclusions or recommendations in this report, but rather provided expertise on the technical content. They acted in a personal and not representative capacity.

This report was lead authored by Madeleine Chang, with substantive contributions from Harry Farmer, Sohaib Malik, Imogen Parker, Aidan Peppin and Octavia Reeve.

Bibliography

Access Now. (2021). Ban Biometric Surveillance. Available at: https://www.accessnow.org/ban-biometric-surveillance/

Access Now. (2022). *Joint civil society amendments to the Artificial Intelligence Act: Prohibit emotion recognition in the Artificial Intelligence Act*. Available at: https://www.accessnow.org/cms/assets/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf

Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Available at: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/; Data available at (opens spreadsheet): https://bit.ly/ALIBfvDatasets

Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

Ada Lovelace Institute. (2022). (Forthcoming) publication on four areas for further exploration in AI regulation.

Ajunwa, I. (2021). 'Automated Video Interviewing as the New Phrenology'. *Berkeley Technology Law Journal*. Available at: https://papers.ssrn.com/abstract=3889454

Air Industry Review. (2020). Airport e-gates: could the pandemic save them from the scrap heap?. Available at: https://airport.nridigital.com/air_may20/airport_egates

American Civil Liberties Union. (2018). *Letter from nationwide coalition to Amazon CEO Jeff Bezos regarding Rekognition*. Available at: https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition

Amnesty International. *Inside the NYPD's Surveillance Machine*. Available at: https://banthescan.amnesty.org/decode/

Automated Facial Recognition (Moratorium and Review) Bill. (2020). Parliament: House of Lords. Bill no. 87. London: Published by authority of the House of Lords. Available at: https://bills.parliament.uk/bills/2610

Barrett, L. F. (2022). 'Facial Expressions Do Not Reveal Emotions'. *Scientific American*. Available at: https://www.scientificamerican.com/article/darwin-was-wrong-your-facial-expressions-do-not-reveal-your-emotions/

Barrett, L. F. et al. (2019). 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements'. *Psychological Science in the Public Interest*. doi: 10.1177/1529100619832930.

BBC News. (2016). *Calais migrants: How is the UK-France border policed?*. Available at: https://www.bbc.com/news/uk-33267137

BBC News. (2021). *Schools pause facial recognition lunch plans*. Available at: https://www.bbc.com/news/technology-59037346

Big Brother Watch. *Stop Facial Recognition*. Available at: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

Biometrics Commissioner. (2018). *Biometrics Commissioner's response to the Home Office Biometrics Strategy*. Available at: https://www.gov.uk/government/news/biometrics-commissioners-response-to-the-home-office-biometrics-strategy

Biometrics Commissioner. (2022). *Biometrics Commissioner praises government on a 'decent job', but warns it's 'only half done'*. Available at: https://www.gov.uk/government/news/biometrics-commissioner-praises-government-on-a-decent-job-but-warns-its-only-half-done

Bowyer, K. W. et al. (2020). 'The "Criminality From Face" Illusion'. *IEEE Transactions on Technology and Society*, 1(4), pp. 175–183. doi: 10.1109/TTS.2020.3032321.

Buolamwini, J. (2018). *Audit of Amazon Rekognition Uncovers Gender and Skin-Type Disparities.* Available at: https://uploads.strikinglycdn.com/files/e286dfe0-763b-4433-9a4b-7ae610e2dba1/RekognitionGenderandSkinTypeDisparities-June25-Mr.%20Bezos.pdf

Buolamwini, J. and Gebru, T. (2018). 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Conference on Fairness, Accountability and Transparency*, PMLR, pp. 77–91. Available at: https://proceedings.mlr.press/v81/buolamwini18a.html

Burgess, M. (2020). 'Co-op is using facial recognition tech to scan and track shoppers'. *Wired UK*. Available at: https://www.wired.co.uk/article/coop-facial-recognition

Center for Democracy and Technology. (2022). *CDT Comments to OSTP Highlight How Biometrics Impact Disabled People*. Available at: https://cdt.org/insights/cdt-comments-to-ostp-highlight-how-biometrics-impact-disabled-people/

Chowdhury, A. (2020). 'Unmasking Facial Recognition'. *WebRoots Democracy*. Available at: https://webrootsdemocracy.org/unmasking-facial-recognition/

College of Policing. *Authorised Professional Practice: Live Facial Recognition*. Available at: https://www.app.college.police.uk/app-content/live-facial-recognition/?s=

Courts and Tribunals Judiciary. (2020). *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police and the Secretary for the State for the Home Department*. Case No: C1/2019/2670. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

Dastin, J. (2020). 'Rite Aid deployed facial recognition system in hundreds of U.S. stores'. *Reuters*. Available at: https://www.reuters.com/investigates/special-report/usa-riteaid-software/

Dave, P. (2022). 'U.S. cities are backing off banning facial recognition as crime rises'. *Reuters*. Available at: https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/

Electronic Privacy Information Centre. (2021). *HireVue, Facing FTC Complaint From EPIC, Halts Use of Facial Recognition*. Available at: https://epic.org/hirevue-facing-ftc-complaint-from-epic-halts-use-of-facial-recognition/

Engler, A. (2019). 'For some employment algorithms, disability discrimination by default'. *Brookings Institute*. Available at: https://www.brookings.edu/blog/techtank/2019/10/31/for-some-employment-algorithms-disability-discrimination-by-default/

European Data Protection Supervisor. (2021). *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*. Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

Greenfield, S. (2020). 'Facewatch at the Southern Co-op'. *Facewatch*. Available at: https://www.facewatch.co.uk/2020/10/05/facewatch-at-the-southern-co-op/

Grother, P. J., Ngan, M. L. and Hanaoka, K. K. (2019). 'Face Recognition Vendor Test Part 3: Demographic Effects'. *NIST*. Available at: https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects , summarised in: Castelvecchi, D. (2020). 'Is facial recognition too biased to be let loose?'. Nature, 587(7834), pp. 347–349. doi: 10.1038/d41586-020-03186-4

Harwell, D. (2019). 'A face-scanning algorithm increasingly decides whether you deserve the job'. *Washington Post*. Available at: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/

Hatmaker, T. (2022). 'Clearview AI banned from selling software widely in the US'. *TechCrunch*. Available at: https://social.techcrunch.com/2022/05/09/clearview-settlement-bipa/

Heaven, D. (2020). 'Why faces don't always tell the truth about feelings'. *Nature*, 578(7796), pp. 502–504. doi: 10.1038/d41586-020-00507-5.

Heilweil, R. (2020). 'Big tech companies back away from selling facial recognition to police. That's progress'. *Vox*. Available at: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police

Hill, K. (2020). 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match'. *The New York Times*. Available at: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

Home Office. (2018). *Biometrics Strategy*. Available at: https://www.gov.uk/government/publications/home-office-biometrics-strategy

House of Commons Science and Technology Committee. (2018). *Biometrics strategy and forensic services*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf

House of Commons Science and Technology Committee. (2019). *The work of the Biometrics Commissioner and the Forensic Science Regulator*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003.htm

House of Commons Science and Technology Committee. (2021). *Work of the Biometrics Commissioner and the Forensic Science Regulator: Government Response to the Committee's Nineteenth Report of Session 2017–19*. Available at: https://publications.parliament.uk/pa/cm5801/cmselect/cmsctech/1319/131902.htm

House of Lords Justice and Home Affairs Committee. (2022). *Technology rules? The advent of new technologies in the justice system.* Available at: https://committees.parliament.uk/publications/9453/documents/163029/default/

Information Commissioner's Office (ICO). (2022). *ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

ICO. (2021). *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*. Available at: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Irwin, V. (2022). 'Meta is looking into eye-tracking and product placement to make money in the metaverse'. *Protocol*. Available at: https://www.protocol.com/bulletins/metas-tracking-you

Kaye, K. (2022). 'Companies are using AI to monitor your mood during sales calls. Zoom might be next'. *Protocol*. Available at: https://www.protocol.com/enterprise/emotion-ai-sales-virtual-zoom

Kaye, K. (2022). 'Intel thinks its AI knows what students think and feel in class'. *Protocol*. Available at: https://www.protocol.com/enterprise/emotion-ai-school-intel-edutech

Keyes, O. (2018). 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition'. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), pp. 88:1-88:22. doi: 10.1145/3274357

Levin, S. (2017). 'New AI can guess whether you're gay or straight from a photograph'. *The Guardian*. Available at: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph

Liberty. *Human Rights coalition calls for immediate ban on facial recognition.* Available at: https://www.libertyhumanrights.org.uk/issue/human-rights-coalition-calls-for-immediate-ban-on-facial-recognition

Lomas, N. (2021). 'Clearview AI in hot water down under'. *TechCrunch*. Available at: https://social.techcrunch.com/2021/11/03/clearview-ai-australia-privacy-breach/

Lomas, N. (2022). 'Italy fines Clearview AI €20M and orders data deleted'. *TechCrunch*. Available at: https://social.techcrunch.com/2022/03/09/clearview-italy-gdpr/

NIST. (2022). *Face Recognition Vendor Test (FRVT) Ongoing*. Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

No Biometric Barriers to Housing Act, H.R.4008, 117th Cong. (2021). Available at: https://www.congress.gov/bill/117th-congress/house-bill/4360?s=1&r=87

O'Murchu, C. (2021). 'Facial recognition cameras arrive in UK school canteens'. *Financial Times*. Available at: https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9

Phillips, P. J. et al. (2018). 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms'. *Proceedings of the National Academy of Sciences*, 115(24), pp. 6171–6176. doi: 10.1073/pnas.1721355115

Privacy International. (2020). *Cooperating With Who?! Answers Needed as UK Retailer Southern Co-Op Tests Facewatch*. Available at: http://privacyinternational.org/advocacy/4342/cooperating-who-answers-needed-uk-retailer-southern-co-op-tests-facewatch

Privacy International. *Ban biometric mass surveillance*. Available at: https://privacyinternational.org/campaigns/ban-biometric-mass-surveillance

Reclaim Your Face. *Reclaim Your Face*. Available at: https://reclaimyourface.eu/

Rhoden-Paul, A. (2022). 'Stop and search: Ethnic minorities unfairly targeted by police – watchdog'. *BBC News*. Available at: https://www.bbc.com/news/uk-61167875

Rollet, C. (2022). 'UK Grocer Facial Recognition With Hikvision Cameras, GDPR And Ethical Risks Examined'. *IPVM*. Available at: https://ipvm.com/reports/facewatch-coop

Ryan, J. (2022). 'Co-op are using cameras made by Chinese state-owned company'. *Mail Online*. Available at: https://www.dailymail.co.uk/news/article-10406421/Co-op-using-cameras-Chinese-state-owned-company-track-shoppers.html

Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

S.T.O.P. – The Surveillance Technology Oversight Project.*Workshop: Know Your Rights*. Available at: https://www.stopspying.org/training

Scottish Parliament. (2019). *Scottish Biometrics Commissioner Bill - Explanatory Notes*. Available at: https://www.parliament.scot/-/media/files/legislation/bills/current-bills/scottish-biometrics-commissioner-bill/introduced/explanatory-notes-scottish-biometrics-commissioner-bill.pdf

Simonite, T. (2021). 'Face Recognition Is Being Banned—but It's Still Everywhere'. *Wired*. Available at: https://www.wired.com/story/face-recognition-banned-but-everywhere/

Singer, N. and Metz, C. (2019). 'Many Facial-Recognition Systems Are Biased, Says U.S. Study'. *The New York Times*. Available at: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

Sloane, M., Moss, E. and Chowdhury, R. (2022). 'A Silicon Valley love triangle: Hiring algorithms, pseudo-science, and the quest for auditability'. *Patterns*, 3(2), p.100425. doi: 10.1016/j.patter.2021.100425

Stark, L. and Hutson, J. (2021). 'Physiognomic Artificial Intelligence'. *Fordham Intellectual Property, Media & Entertainment Law Journal*. doi: 10.2139/ssrn.3927300

The Conservative and Unionist Party. (2019). *Get Brexit Done: Unleash Britain's potential*. Available at: https://assets-global.website-files.com/5da42e2cae7ebd3f8bde353c/5dda924905da587992a064ba_Conservative%202019%20Manifesto.pdf

UN High Commissioner for Human Rights. (2020). Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Available at: https://digitallibrary.un.org/record/3879547

Vallance, C. (2021). 'Afghanistan: Will fingerprint data point Taliban to targets?'. BBC News. Available at: https://www.bbc.com/news/technology-58245121

van Mastrigt, N. M. et al. (2018). 'Critical review of the use and scientific basis of forensic gait analysis'. Forensic sciences research, 3(3), pp. 183–193. doi: 10.1080/20961790.2018.1503579

Vincent, J. (2017). 'The invention of AI "gaydar" could be the start of something much worse'. *The Verge*. Available at: https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy

Wakefield, J. (2021). 'AI emotion-detection software tested on Uyghurs'. BBC News. Available at: https://www.bbc.com/news/technology-57101248

Weale, S. (2021). 'ICO to step in after schools use facial recognition to speed up lunch queue'. *The Guardian*. Available at: https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk

Whittaker, Z. (2021). 'Clearview AI ruled "illegal" by Canadian privacy authorities'. *TechCrunch*. Available at: https://social.techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/

Wu, X. and Zhang, X. (2016) 'Automated Inference on Criminality using Face Images'. arXiv:1611.04135 [cs]. Available at: https://arxiv.org/abs/1611.04135v1

About the Ada Lovelace Institute

The Ada Lovelace Institute was established by the Nuffield Foundation in early 2018, in collaboration with the Alan Turing Institute, the Royal Society, the British Academy, the Royal Statistical Society, the Wellcome Trust, Luminate, techUK and the Nuffield Council on Bioethics.

The mission of the Ada Lovelace Institute is to ensure that data and AI work for people and society. We believe that a world where data and AI work for people and society is a world in which the opportunities, benefits and privileges generated by data and AI are justly and equitably distributed and experienced.

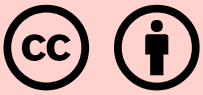
We recognise the power asymmetries that exist in ethical and legal debates around the development of data-driven technologies, and will represent people in those conversations. We focus not on the types of technologies we want to build, but on the types of societies we want to build.

Through research, policy and practice, we aim to ensure that the transformative power of data and AI is used and harnessed in ways that maximise social wellbeing and put technology at the service of humanity.

We are funded by the Nuffield Foundation, an independent charitable trust with a mission to advance social well-being. The Foundation funds research that informs social policy, primarily in education, welfare and justice. It also provides opportunities for young people to develop skills and confidence in STEM and research. In addition to the Ada Lovelace Institute, the Foundation is also the founder and co-funder of the Nuffield Council on Bioethics and the Nuffield Family Justice Observatory.

Find out more:

Website: Adalovelaceinstitute.org
Twitter: @AdaLovelaceInst
Email: hello@adalovelaceinstitute.org



Preferred citation: Ada Lovelace Institute. (2022). *Countermeasures: The need for new legislation to govern biometric technologies in the UK*. Available at: https://www.adalovelaceinstitute.org/report/countermeasures-biometric-technologies/

ISBN: 978-1-7397950-2-3