Innovation and Technology

Biometrics: insight

Information Commissioner's Office

Contents

Introduction

Biometric technologies and the data they collect and generate are already a significant part of our lives. Yet, they are not static. New technologies continue to develop at pace; new ways of gathering data and analysing our lives will be commercially available in the next two to seven years.

Biometric technologies provide opportunities for innovation. They can:

- enhance and facilitate access to a wide variety of services and devices;
- provide additional security for complex data and transactions; and
- improve accuracy in education, healthcare and entertainment.

Yet, the ICO also recognises the scope for future potential harm. Anticipating future developments in the use of this technology will help us respond in a timely and proactive manner.

This report sets out the grounds of our research, core definitions and technical and legal contexts that are used to understand the potential challenges that may emerge. It is intended to provide a short introductory guide for those who wish to know more about the current state of biometric technologies from a regulatory perspective. We consider uses of data that are considered to be 'biometrics' by researchers and specialists.[1] However, they may not fall under the definitions of biometric data or special category biometric data under the UK GDPR. This includes novel applications in behavioural analysis and classification.

As well as presenting our views on current systems, this publication supports our Biometrics: Foresight report which explores plausible impacts of biometric technologies as they develop in the near horizon and includes a detailed analysis of both the challenges and opportunities our biometric future might bring.

This analysis has been commissioned to ensure the ICO is well placed to protect individuals, provide clarity for businesses and facilitate privacy-positive innovation. Following this report, the ICO will set out a call for views and produce targeted guidance on biometrics by Spring 2023. The guidance will set out core definitions and approaches, link to existing ICO guidance, identify emergent risks and highlight user based and sector specific case studies to set out good practice.

[1] The ICO has already considered on the legal and regulatory implications of the use of facial recognition technologies (FRT) in the law enforcement sector and within public spaces. See the Commissioner's opinion on the use of this technology in public spaces for further information.

Background

Why biometric data?

Processing biometric data poses a significant and specific risk to people's information rights in two ways:

- Its intrinsic nature; for example, you cannot change your vasal patterns, fingerprint, subconscious emotional responses or DNA. This means that if this biometric data was lost, stolen or inappropriately used, it could not simply be replaced or varied[2].
- Its potential for leading to inaccurate or inappropriate inferences, or both, being made about people; for example, about a person's ethnicity, age or gender. Also, when biometric data is processed in conjunction with algorithmic processing it may be impacted by an underlying systemic bias.

Biometric technologies can offer significant benefits and opportunities for people and organisations. They can:

- enhance and facilitate access to a wide variety of services and devices;
- provide additional security over complex data and transactions; and
- offer greater accuracy in education, healthcare and entertainment.

As well as these opportunities for innovation, we also recognise the scope for future potential harm.

Defining biometric data

This personal data gained through the use of biometric technologies (referred to here as 'biometrics') is categorised in two ways under the GDPR. Under article 4(14) the UK GDPR defines biometric data 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 [fingerprint] data'.

The above definition relates to personal data that allows or confirms the unique identification of an individual. Whereas biometric data that is explicitly used for the purpose of identifying a natural person is special category data under Article 9 (1):

[2] This also links to broader issues regarding freedom of expression and a right to privacy, as an individual cannot reasonably be expected to conceal their face or gait as they might with a password or pin number. See Microsoft Word - R (Bridges) -v- CC South Wales ors Judgment.docx (judiciary.uk) for further details.

> "processing of … biometric data for the purpose of uniquely identifying a natural person".

However, for the specific purposes of this report and the partner Biometrics: Foresight report, we have considered biometric technologies as:

> "Technologies that process biological or behavioural characteristics for the purpose of identification, verification, categorisation or profiling".

This broader definition allows us to also consider uses of data that are considered to be 'biometrics' by researchers and specialists but which may not necessarily fall within the definitions of biometric data as set out above and therefore fall outside the scope of UK data protection legislation. In practice, this includes (but is not limited to) techniques such as the use of:

- micro expression analysis, keystroke analysis and physiological data for classification and inferences; and
- techniques such as facial, gait, iris and vocal recognition for identification or verification (that are considered biometric data under the UK GDPR).

We have identified novel use cases with potential privacy concerns in sectors including employment, finance or insurance, transport, healthcare and education. We have used these to develop the scenarios presented in our Biometrics: Foresight report.

Biometric technologies – the context

It's helpful to be aware of the broader developments that have led to emerging biometric technologies, including the current commercial and legal contexts. As an aid to the analysis below, see definitions of specific technologies in Annex A.

First generation biometrics can be considered to have begun with the use of fingerprinting in law enforcement as far back as the 19th century. More recently it is also considered to include verification and authentication methods, such as facial recognition, and for some researchers, iris scanning.[3] What further defines these approaches as first generation is the high level of friction needed to gather the data via highly specialised technology.

Second generation biometrics includes gait recognition, voice recognition, vasal analysis and keystroke logging. These second generation technologies remain focussed on processes of verification and authentication, albeit often combined when assessing an individual, in order to reduce the risks posed by lower rates of accurate association. Also, they enable reduced friction, meaning that these technologies can be deployed without direct physical contact or significant

[3] https://www.researchgate.net/publication/328404365_Second_Generation_Biometrics_and_the_Future_of_Geosurveillance_A_Minority_Report_on_FAST

pauses required to gather data. This increases efficiency and potential biometric sampling events (BSEs), while also raising issues of transparency, consent and appropriate notification to affected people.

Certain technologies may also be considered 'generation 2.5' for the purposes of this report. This includes the deployment of multiple verification or authentication technologies through purpose agnostic devices, such as a smartphone. This builds on the need to use multi-modal approaches to compensate for lower accuracy rates common to many second generation technologies. Second and even first generation technologies can be deployed in new, low, or even non-friction means. For example, it is possible to use high resolution cameras to capture fingerprints remotely.

Generation 2.5 and now emerging generation 3 tech are increasingly used for classification as well as verification and authentication. Examples of generation 3 technologies include behavioural biometrics, a broad term that encompasses gaze tracking, keystroke logging, natural language processing (NLP), gait recognition (when used for classificatory purposes) and emotional AI.[4]

There are further common divisions of biometrics; the term hard biometrics refer to modalities that are physiological in nature such as fingerprints, ear patterns, facial patterns and vasal analysis that do not change with age, barring significant injury or disability. By contrast, soft biometrics relate to physiological and psychological aspects of a person that can shift depending on time or circumstance, or both. This includes behaviours and emotions, as well as modalities such as gait and facial analysis, where age, injury or illness may alter the data provided.

Setting out clear definitions of authentication, verification, identification and classification is essential to understanding when data is biometric data:

- **Verification** – a one-to-one comparison of data to stored information to confirm access to a service or device.
- **Authentication** – matching a person to a specific stored identifier. Stakeholders have highlighted that this differs from verification which focusses on confirming the identity of an individual.
- **Classification** – categorising aspects of a person, whether physical or behavioural, often via inferences. This may or may not be personal data depending on how (and if) it is linked to a known person and raises significant questions about how we approach this use of biometrics.
- **Identification** – a one-to-many comparison of data to stored information to identify a person (or people) within a larger data set. This is likely to be the mode of processing for mass public and private processing.

[4] For further details on these technologies see Annex A.

Current and emerging methods of deployment of biometric technologies impact processing. The advent of multi-modality is therefore key and can refer to both the use of:

- a single biometric modality, such as gait recognition, to extract or infer multiple points of personal data. For example, gait recognition may provide a means of individualisation, identification, behavioural or emotional inferences or even healthcare data depending on what tools are used to capture it and what processing it is subjected to; and
- several biometrics at a single point of data collection. For example, the use of gaze tracking alongside LFR to provide additional security to a verification process. This may be done to counter criminal access, in this case through the use of an image or mask to spoof the camera, or multiple methods may be used to compensate for lower accuracy rates. By combining multiple lower-cost, lower-accuracy biometric modalities, a similar level of accuracy can be achieved as with a higher cost, potentially higher friction approach.

Why biometrics technologies?

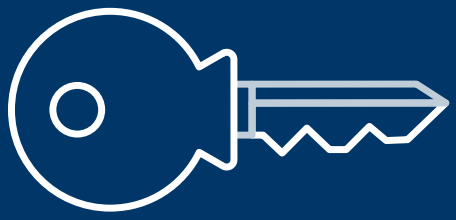
In our everyday lives

From fingerprint scanners and facial recognition in our phones, to use in law enforcement and even learning about our health, biometric technologies are everywhere.

The benefits

These technologies can offer:

- security
- accessibility
- convenience
- a wealth of information about our daily lives



The risks

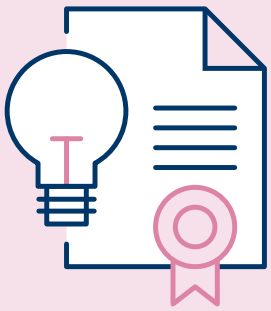
Your biometrics are intrinsic to you as an individual. Unlike passwords, if your biometrics data is lost or stolen, you cannot easily change your fingerprint, face or retina.

What next?

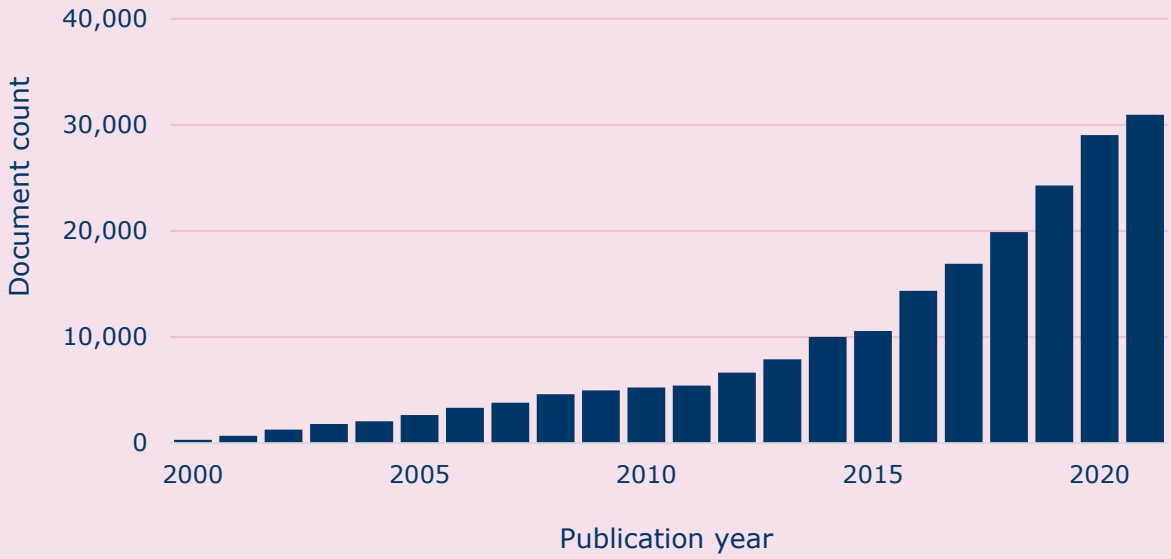
The ICO is exploring biometric technologies to understand which new technologies are likely to become part of everyday life. We want to assess what impact this may have on data protection.

Biometric technologies: patent analysis

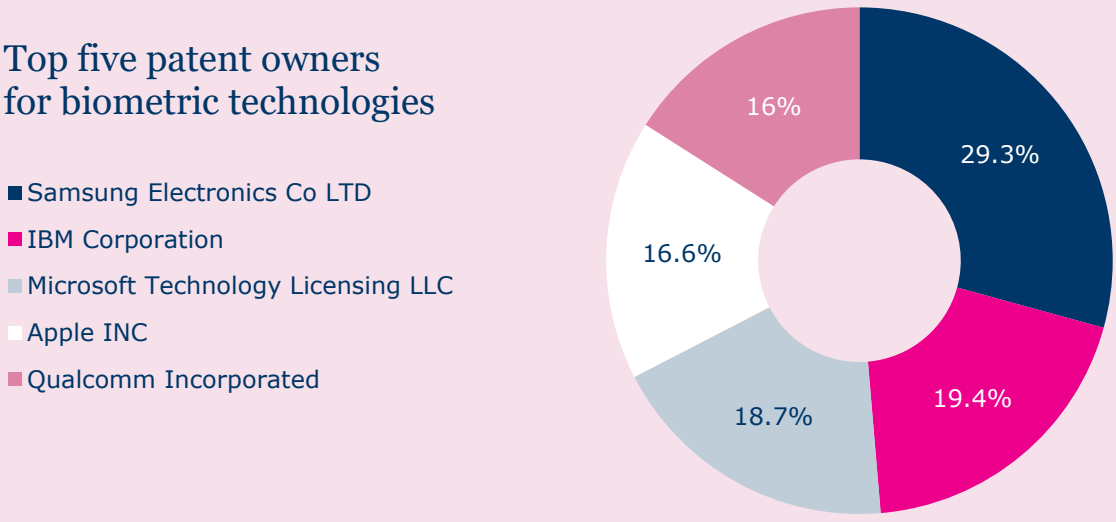
A patent is an official right to protect inventions for a specified time. Having a patent makes it illegal for people other than the patent holder (or those with permission from the patent holder) to make, use or sell the invention in the territory where the patent has been granted.



The number of new biometric technology patents therefore offers a helpful insight into how the industry is evolving. The graph below shows the growth in patents globally for biometric technologies since 2000*.



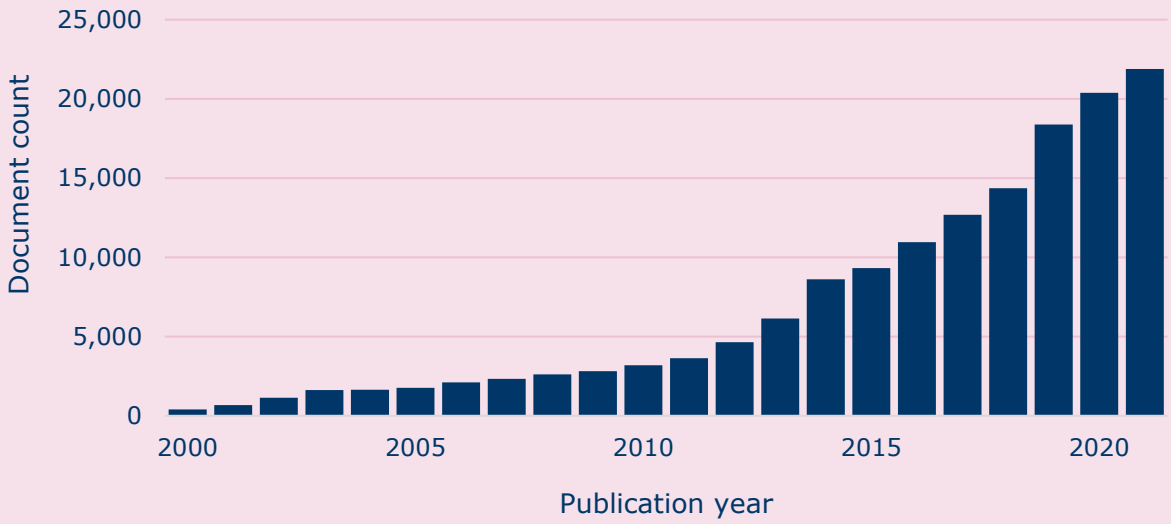
Top five patent owners for biometric technologies



*Data Source: The Lens (lens.org/lens) – search term: Biometric Technology

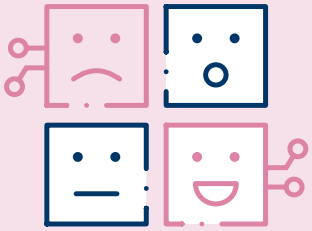
Facial recognition

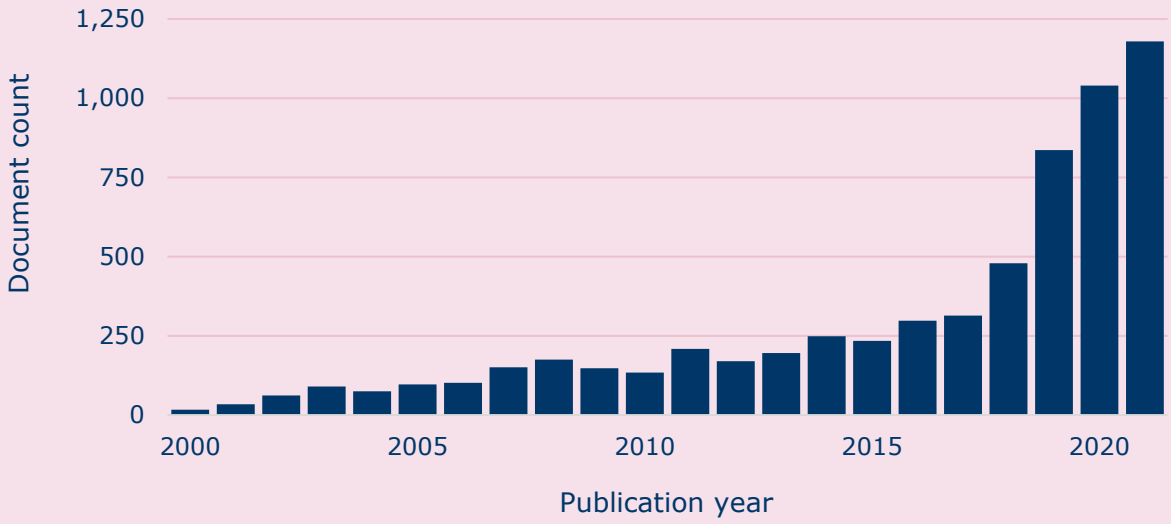
Some areas of biometric technology have already become a part of daily life. We can see the global patent document count steadily growing, for example in the graph below for facial recognition technology*.



Emotional analysis

Other novel biometric technologies that are not yet widely available on the market have seen a rapid growth in the last few years. For example, emotional analysis, that uses biometric technologies to collect data about human emotion, moods and affective states.**



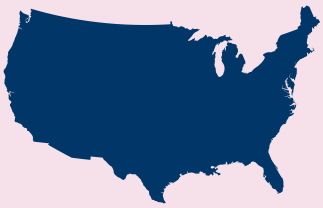


*Data Source: The Lens (lens.org/lens) – search term: Facial Recognition
**Data Source: The Lens (lens.org/lens) – search term: Emotional AI'

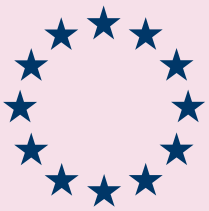
Leading jurisdictions

The patent document count for biometric technology is highest across:

WIPO
(UN Agency)



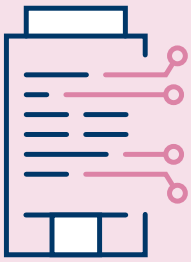
United States of America



European Union

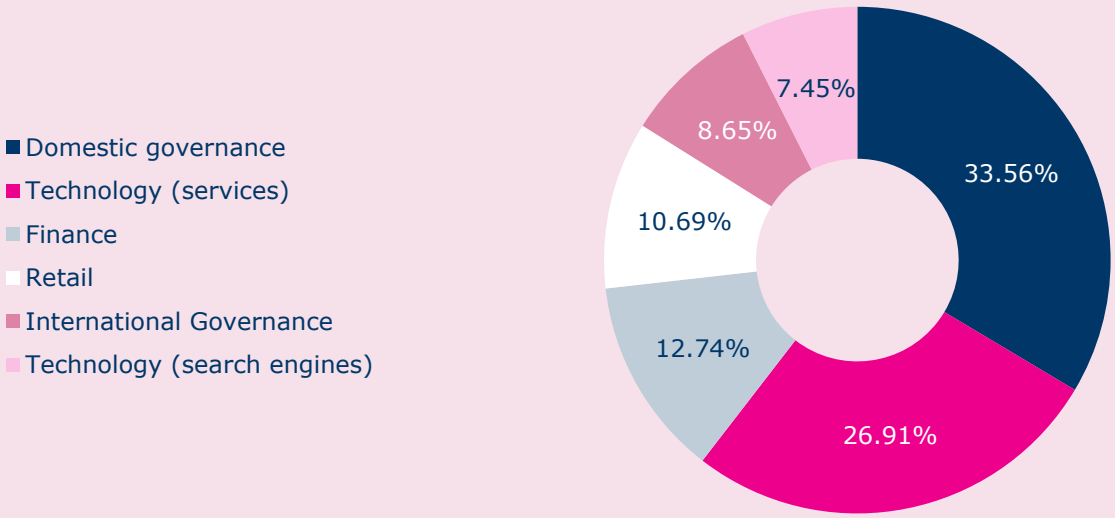
Biometric technologies: further insights

The ever-growing relevance of biometric technologies is indicated elsewhere as well.



Biometric technologies are used across sectors, indicating that there are a variety of applications (tracked as events below) to serve different purposes. We anticipate this becoming increasingly the case as novel biometric technologies come to market.

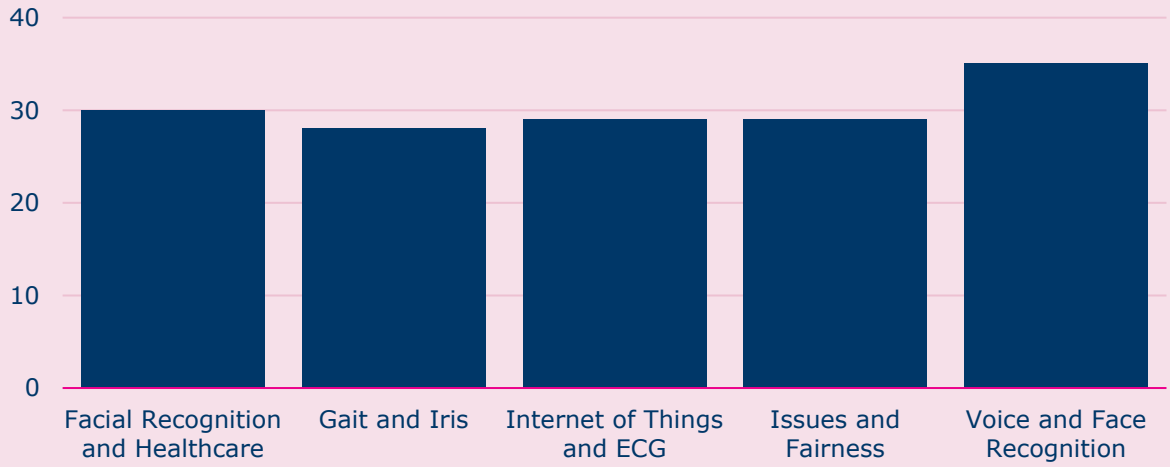
Events are defined here as a set of unique documents published within a short time frame (typically one to three days) containing similar wording and entities. In the media, events are typically reported on by a number of publications in quick succession, enabling this detection.*



*Data Source: Primer Analyse (primer.ai) - search term: Biometric Technology
Top 25 entities sample taken and biometric technology developers whose products serve multiple sectors were removed. The remaining 14 entites are captured in this visual.

Biometric technologies are also featuring heavily in academia

The graph below indicates the most frequently discussed topics about biometric technologies in academic papers from the previous year (June 2021 – June 2022). Looking at academic publications can provide valuable insights into what topics and approaches are emerging in cutting-edge thinking.



What does this mean for the ICO?

These visuals show that there is a sustained and growing interest globally in biometric technologies across a number of sectors and jurisdictions. Some of these, such as facial recognition, are already relatively well-established in the market. The use of more novel technologies is projected to grow significantly within the next five years.

Different types of biometric data can be gathered through different means and for different purposes. The application of biometric technology is therefore far wider than law enforcement or user verification. The processing of biometric data is likely to become increasingly prevalent. As the regulator for information rights, the ICO is thinking ahead about what this could mean for data protection.

Whilst the above is useful for giving an oversight of how the industry is evolving, it can be difficult to imagine how and what this will look like in our day to day lives and what emerging data protection challenges may be. To better understand this, we can turn to other, foresight based approaches set out in our Biometrics: Foresight report.

Data Source: Primer Science (science2.primer.ai) - Search Term: Biometric AND Technology.

Legal context

Understanding the broader legal context relevant to biometric data is also important. Beyond the GDPR, a variety of legislative approaches have been taken to regulate biometric technologies and their use of personal data. Historically, the EU's Article 29 Data Protection Working Party (which was replaced by the European Data Protection Board) was one of the first data protection advisory bodies to note the increasing importance of 'soft biometrics', This recognised the diversity of data collection and the development of what would become behavioural and sentiment analysis, alongside approaches such as gait and facial analysis.[5] However this distinction between soft and hard biometrics and any risk-based implications were not reflected within the GDPR. Instead it presented tightly delineated definitions of biometric data and special category biometric data under Articles 4(14) and 9(1).

Building on these definitions, the CNIL's model regulation on biometrics in the workplace seeks to provide greater clarity on the use of biometric data in specific circumstances.[6] Under GDPR Article 9(4), France has introduced member state specific legislation that gives a prescriptive list of the types of personal data that may be collected and further processed for workplace purposes. It defines the data retention periods and specifies technical and organisational measures that must be implemented to ensure the security of the personal data. The Model regulation also requires data controllers who process employee biometric data to carry out a Data protection impact assessment (DPIA) and regularly update it, at least every three years.

In contrast to European approaches, Article 29 of China's PIPL legislation considers all biometric data to be sensitive data, including that used for classificatory purposes. This broad-spectrum approach is combined with a definition of biometric data as "information that, once leaked, or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security".[7] The focus on harms provides a flexible, risk-based approach. Brazil's LGPD legislation at Art 5 (II) defines all biometric data as sensitive, yet does not define biometric data itself. Such an approach allows for significant regulatory coverage of a wide variety of processing.

While the impact of Brazil's recent legislation on biometric innovation is yet to become fully clear, legislation in the USA[8] such as Illinois' Biometric Information Privacy Act (BIPA) has, at times, generated a significant level of litigation.[9] It

[5] Draft outline for WP29 opinion on "consent" (europa.eu)
[6] CNIL Publishes Binding Rules on Processing Biometric Data as Workplace Access Control | Privacy & Information Security Law Blog (huntonprivacyblog.com) and Délibération n°2019-001 du 10 janvier 2019 portant sur le règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'acès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail (cnil.fr)
[7] Analysing China's PIPL and how it compares to the EU's GDPR (iapp.org)
[8] When is a Biometric No Longer a Biometric? - Future of Privacy Forum (fpf.org)
[9] McDonald v. Symphony Bronzeville Park, LLC :: 2022 :: Supreme Court of Illinois Decisions :: Illinois Case Law

requires that businesses obtain consent prior to collecting biometric information (eg fingerprints, facial geometry information and iris scans as the definition focusses on hard biometric modalities), issue a publicly available data retention policy, and refrain from certain data sales and disclosures. Recent cases such as *McDonald v. Symphony Bronzeville Park*[10] have demonstrated that the risk of class actions may potentially influence future deployments of biometric technologies across a variety of sectors including employment and potentially finance as the potential financial penalties for organisations increase. California's Consumer Privacy Act (CPA) may have a similar impact on the use of biometrics, although its definition of "biometric information" is closer to that set out in the GDPR, covering both hard and soft biometrics for the purpose of identification.[11]

Looking forward to emerging legislation, the EU's proposed AI Act currently ports across the GDPR's definition of biometric data.[12] The AI Act identifies all algorithmic-based processing of biometric data as 'high risk' and requiring further legal and governance-based mechanisms in order to process.[13] New legislation (such as the AI Act) about the use of biometric technologies within the EU is likely to have a global impact as controllers and processors align to seek continued participation in European markets.

What's next?

If you are interested in understanding some of the key issues relevant to the intersection of biometric technologies and data protection in the future, we encourage you to read the Biometrics: Foresight report. This partner publication builds upon the work set out here and applies foresight methodologies to construct and analyse plausible future scenarios. Both of these publications provide a foundation on which we are developing further biometric specific guidance.

In support of the ICO's ongoing work on biometrics, including the development of targeted guidance, we are issuing a further call for views. We want to hear from stakeholders who are working in this sector; whether it's in developing biometric technologies, deploying them or thinking about them in a policy based or regulatory context. We'd very much like to hear from you as we continue to develop our knowledge and thinking in this area. We can be reached at:

biometrics@ico.org.uk

[10] McDonald v. Symphony Bronzeville Park, LLC :: 2022 :: Supreme Court of Illinois Decisions :: Illinois Case Law :: Illinois Law :: US Law :: Justia
[11] Codes Display Text (ca.gov)
[12] The Artificial Intelligence Act |
[13] Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces (europa.eu)

Annex A – Glossary

Terminology/ technology (modalities)	Definition	Key data protection risks	Potential sectors of use
Facial recognition	Aspects of the face are used to construct a mathematical model for comparison to an image.	Systemic bias via underlying algorithms leading to unfair and discriminatory outcomes.	Law enforcement, commercial purposes, payment verification, device security.
Gaze tracking	Tracking the movement of the eye to understand where and what a person is looking at.	Potential discrimination against disabled people if this is the only means of data collection.	Entertainment, advertising, workplace surveillance.
Pupillometry	Measuring the size and response of a person's pupil to stimuli.	May reveal sub-conscious responses and highly sensitive personal data without the person's choice.	Health and medical care, used within emotional AI in employment, entertainment, advertising and assistive technology.
Gait analysis	Stride length, width, measurement of the bones and joints in the leg can be used to create a means of identifying a person.	Data collection may be obscured by bags, other people and gait may alter due to age, injury or medical conditions raising the risk of	Workplace surveillance, security, public surveillance.

Terminology/ technology (modalities)	Definition	Key data protection risks	Potential sectors of use
		inaccurate data.	
Vasal analysis	The unique structure of veins in the hand and palms are used to identify a person.	Potential discrimination against disabled people if this is the only means of data collection.	Workplace surveillance, security, finance.
Iris/ scleral vein analysis	Mathematical analysis of the eye identifies unique patterns in the iris or the veins in the whites of the eye.	Potential discrimination against disables individuals if this is the only means of data collection.	Workplace surveillance, security.
Ear analysis	Mathematical analysis of the ear can identify unique patterns.	Authentication or multi-modal verification approaches will reduce the risk of exclusion.	Workplace surveillance, security.
Heartrate tracking (ECG analysis)	Heartbeats are unique and an identifying electronic signature can be derived from the sound, size and shape of the organ.	Continuous authentication may raise the risk of revealing additional health related data alongside the expected data.	Workplace surveillance, security.

Terminology/ technology (modalities)	Definition	Key data protection risks	Potential sectors of use
Brain analysis (EEG analysis)	The electrical impulses of the brain can be recorded and measured, creating a unique pattern for a person.	May reveal sub-conscious responses and highly sensitive personal data without the person's choice.	Health and medical care, used within emotional AI in employment, entertainment, advertising.
Sweat tracking (GSR analysis)	Tracking of moisture on the skin in response to stimuli.	May reveal sub-conscious responses and highly sensitive personal data without the person's choice.	Health and medical care, used within emotional AI in employment, entertainment, advertising.
Hand or finger geometry	The physical structure of the hand (joints, digit length and surface identifiers) or the finger (length, width, thickness and surface texture) are used to build a unique pattern about a person.	Potential discrimination against disabled people, if this is the only means of data collection.	Workplace surveillance, security, finance.
Fingerprint	The unique papillary ridges on each person's fingers can be used to identify them.	Remote (low friction) fingerprint detection may increase the risk of a lack of transparency in processing.	Workplace surveillance, security, finance.

Terminology/ technology (modalities)	Definition	Key data protection risks	Potential sectors of use
Voice analysis	The waves created by a person's voice can be measured and analysed to identify unique patterns. This differs from speech recognition that focusses upon the words said.	May reveal sub-conscious responses and highly sensitive personal data without the person's choice. May be unclear when this is being deployed.	Workplace surveillance, security- , finance.
Odour	While odour has been recognised as a unique identifier for some time, it has become increasingly possible to separate and analyse particular components.	Currently a research technique rather than a deployed technique, a key risk remains the lack of transparency when this data is collected.	Health sector, law enforcement.
Keystroke logging	A person's typing patterns can be logged and analysed to identify unique strokes and rhythms.	Transparency of collecting and processing of data.	Workplace tracking, online security.
Behavioural analysis	Behavioural analysis draws together many of the above technologies, such as keystroke logging, gait	May reveal sub-conscious responses and highly sensitive personal data without the person's choice. May be	Workplace tracking, entertainment, education, public surveillance.

Terminology/ technology (modalities)	Definition	Key data protection risks	Potential sectors of use
	analysis, voice analysis and others to identify patterns that form a unique set of unconscious actions linked to a person.	unclear when this is being deployed so again potential issues with transparency.	
Emotional AI	Building upon behavioural analysis, emotional AI interprets data captured by means such as gaze tracking, gait analysis heartbeats, facial expressions and skin moisture to estimate and classify someone's emotional state.	Underlying science of emotion detection is highly contested, systemic bias and potential 'training' of people towards desired behaviours. Transparency and fair notice of processing are also likely to be risks.	Health sector, entertainment, education, public surveillance.