

The Future of Biometric Technology for Policing and Law Enforcement

Informing UK Regulation

Sam Stockwell, Megan Hughes, Carolyn Ashurst and Nóra Ní Loideáin

March 2024



About CETaS.....	2
Acknowledgements	2
Executive Summary.....	3
Recommendations	6
Introduction	10
1. Definitions and Taxonomies.....	18
1.1 Defining biometrics: limits and issues	18
1.2. Understanding biometrics as a ‘spectrum’	20
2. Opportunities and Benefits for Public Safety.....	24
2.1. Current applications.....	24
2.2. Future trends and applications	27
3. System Risks and Challenges	30
3.1. Reliability: Performance, bias, and scientific validity.....	30
3.2. Concerns around data collection and sharing	32
3.3. Appropriate use and impacts to civil liberties	33
3.4. Trust and transparency.....	34
3.5. Challenges for evaluation.....	35
4. Legal Risks and Challenges.....	37
4.1. Overview and limitations of UK biometrics regulation	37
4.2. Overview and limitations of UK biometrics policy	42
5. Public Attitudes to Biometrics	45
5.1 Comfort and trust vary by application and organisation	45
5.2 High levels of concern shown for a wide range of risks.....	48
5.3 A strong desire for explicit regulation and bans on certain use cases	49
5.4 Most people perceive benefits will outweigh concerns	50
6. Alternative Policy and Regulatory Options	52
6.1. Insights from the EU AI Act	52
6.2. Improving biometric governance and oversight.....	53
About the Authors	55
Appendix 1. CETaS Public Opinion Survey	56

About CETaS

The Centre for Emerging Technology and Security (CETaS) is a research centre based at The Alan Turing Institute, the UK's national institute for data science and artificial intelligence. The Centre's mission is to inform UK security policy through evidence-based, interdisciplinary research on emerging technology issues. Connect with CETaS at cetas.turing.ac.uk.

This research was supported by The Alan Turing Institute's Defence and Security Programme. All views expressed in this report are those of the authors, and do not necessarily represent the views of The Alan Turing Institute or any other organisation.

Acknowledgements

The authors are grateful to all those who took part in a research interview or workshop for this project, without whom the research would not have been possible. The authors are very grateful to Fraser Sampson at Sheffield Hallam University for their Strategy Advisor role on the project, as well as to Marion Oswald, Lindsey Chiswick, Campbell Cowie, Matthew Boakes, Malak Sadek and Chris for their valuable feedback on an earlier version of this report. The authors are also thankful to Florence Enock and Eirini Koutsouroupa for their continuous assistance in the drafting and design of the project survey. Design for this report was led by Michelle Wronski.

This work is licensed under the terms of the Creative Commons Attribution License 4.0 which permits unrestricted use, provided the original authors and source are credited. The license is available at: <https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode>.

Cite this work as: Sam Stockwell, Megan Hughes, Carolyn Ashurst and Nóra Ní Loideáin, "The Future of Biometric Technology for Policing and Law Enforcement: Informing UK Regulation," *CETaS Research Reports* (March 2024).

Executive Summary

This CETaS Research Report explores the future of biometric technology for UK policing and law enforcement. It analyses technical trends and highlights where new regulatory measures may be required to facilitate responsible uses and restrictions of these systems for public safety purposes. Gathering insights from existing literature, research interviews with 35 experts and a workshop with policing, government and regulator officials, a diversity of views have informed the study findings. This study also incorporates the most up-to-date public survey on biometric systems, which considers future technological developments and their regulatory implications, involving a nationally representative sample of 662 members of the UK population.

There is ongoing disagreement over definitions of 'biometric technology'. Current discourse tends to define biometric technology as systems used for the purposes of uniquely identifying an individual or verifying their identity. However, this definition is outdated and does not account for the full range of biometrics-based systems now available. Therefore, this report argues for a broader conceptualisation of biometric technology, to account for the emergence of new inferential and classification biometrics-based systems – such as age estimation, emotion recognition, and demographic-based categorisation.

Biometric systems offer new benefits for tackling crime by uniquely identifying individuals with a high degree of confidence, which in certain circumstances – such as crowded public places – would be extremely challenging for human operators to achieve manually. In some cases, biometrics might protect against the errors of human judgement. There is also growing demand among consumers and industry for more secure ways to protect personal data, due to increasingly sophisticated cybersecurity threats and identity fraud techniques.

However, despite their many benefits, critics have argued that emerging biometric systems are prone to technical flaws, pose risks to human rights and in some cases lack scientific validity. This has led to calls for certain biometric systems to be heavily regulated or outright banned. For instance, the EU's forthcoming AI Act is likely to implement a general ban on live facial recognition technology with exemptions for specific policing and law enforcement use cases, as a means of attempting to balance benefits and risks. With discussions ongoing in the UK over how best to regulate AI technology, public attention will also turn to what future regulatory model the UK will pursue for emerging biometric systems.

Our study shows that, in the next 5-10 years, the type of biometric systems and data available are likely to broaden dramatically. Moving beyond prevailing purposes of uniquely identifying or verifying individuals, the same technology may be used for making inferences

about someone's behaviour, emotional state, or classifying them into demographic groups, despite significant concerns over the scientific validity and potential benefits of such use cases. New developments such as frictionless biometric formats that require little or no physical contact, and multimodal systems which combine multiple biometric data sources, could also improve the reliability of biometric systems and, in turn, enhance law enforcement capabilities.

This research reinforces existing evidence that the UK's legal framework for biometrics is inadequate and in need of reform. Current laws are failing to keep pace with changes to biometric technology, which risks undermining public confidence and trust in these systems. Most notably, the current legal framework does not adequately distinguish between tried and tested, scientifically valid biometric systems (such as fingerprint identification, DNA analysis and facial matching) and novel, often untested inferential or classificatory systems – such as age estimation, emotion recognition and gait analysis.

Nevertheless, the public survey conducted for this project has demonstrated support for police and law enforcement use of biometric identification and verification systems such as live facial recognition, but *not* for the use of inferential systems such as polygraph testing or emotion recognition. In general, the UK public is marginally optimistic about the benefits that biometrics could provide for crime reduction. However, many respondents expressed anxiety over the adequacy of safeguards to protect individuals from a range of risks, such as data misuse and discriminatory implications of certain emerging use cases.

1. 60% of respondents reported that they were 'comfortable' with policing and law enforcement applications involving identification biometric systems (e.g. facial recognition to identify criminal suspects in crowded areas). In contrast, only 29% were 'comfortable' with the use of inferential systems (e.g. polygraphs).
2. Respondents reported higher levels of trust in the use of biometric systems by public sector organisations such as police forces (79%) and the NHS (66%), as opposed to commercial entities, particularly employers (42%) and retailers (38%).
3. Most respondents (57%) were 'quite uncomfortable' or 'very uncomfortable' with biometric data sharing schemes between police forces and the private sector for public safety activities, such as tackling shoplifting.
4. Respondents suggested that most biometric use cases should be explicitly regulated rather than outright banned. In terms of outright bans, however, most respondents believed that the use of novel biometric systems in job interviews to assess performance (63%), and tracking student or employee engagement (60%) should both be banned.

5. Most respondents (53%) reported that the benefits of biometrics will outweigh the concerns (either greatly or marginally), whereas 24% thought that the concerns will outweigh the benefits (either greatly or marginally).

To reassure the general public, maximise the benefits of biometric technologies and protect individual rights, our recommendations emphasise the need to simplify the complex web of existing regulatory and policy measures; introduce new protections for emerging biometric systems; and standardise testing and evaluation procedures. This should be achieved through updating existing biometrics legislation and developing new codes of practice for certain data types and systems. Such measures should address the risks, harms and purpose of specific use cases, distinguishing between established technologies, and novel use cases that may involve classification or inferential systems. Any new regulation or codes must apply consistent cross-sector standards for any systems used for public safety purposes, and establish mandatory requirements for independent system auditing and testing.

Recommendations

New legal definitions

1. Future legislation should introduce a new legal definition of 'biometrics-based data', to take into account how different types of biometric data may be used for purposes other than uniquely identifying individuals, such as inference or classification.

New codes of practice and guidance

2. The UK Equality and Human Rights Commission should issue a new code of practice for compliance with the public sector equality duty when using identification, classification or inferential biometric systems. The code should highlight protections needed to prevent *group*-level discrimination and profiling risks, recognising the prevailing focus on individual-level protections within current equality and human rights law.

3. The College of Policing should develop new Authorised Professional Practice (APP) for *retrospective* facial recognition (RFR), to address the specific risks that may arise from its use, given existing APP only covers live facial recognition (LFR).

4. The Home Office should issue new guidance on the appropriate collection, retention, use and deletion of biometric facial images and voice samples by police and law enforcement agencies. This will provide greater legal clarity to existing data protection regulations that fall outside of DNA and fingerprint samples.

5. The Police Digital Service (PDS) should issue new guidance for standardising third-party biometric system procurements, with reference to pre-defined system requirements and evaluation processes, to ensure that future system transfers adhere to minimum standards of accountability, transparency and technical performance.

Policing transparency

6. The National Police Chiefs' Council (NPCC) should establish a nationwide, public biometrics deployment register for police procurement and use of biometric systems. The UK Government's Algorithmic Transparency Recording Standard could provide a basis for such a register.

7. The NPCC should consult with academics, civil society organisations and regulators to establish standardised procedures for public communications campaigns around the use of biometric systems. These should go beyond mechanisms that aim to inform and towards those that actively involve affected communities, such as physical engagements, surveys or focus groups, to improve public confidence in future policing deployments.

Regulator responsibilities

8. The Information Commissioner's Office (ICO) should ensure that any market outreach for upcoming 'regulatory sandboxes' to test biometric systems includes engagement with policing and law enforcement agencies, which will help to pre-empt and address system risks associated with promising innovations for public safety.

9. The ICO should also develop a new risk management framework to address the range of risks from biometric systems which fall outside of data protection legislation.

Future regulatory and policy measures

10. Alongside requirements in existing legislation and technical standards, any future regulatory or policy measures for biometric technologies must:

- a. Identify the purpose, risks and harms of different use cases to inform appropriate levels of oversight and regulation.
- b. Integrate a system-focused approach, including creating a list of specific use cases which could be amended based on new technical or legal developments. This should include banning scientifically untested use cases if the risks and potential harms to individuals are judged to be unacceptable.
- c. Outline a consistent set of mandatory standards and accountability measures which all organisations must adhere to when using biometric systems for public safety activities, particularly given current legal ambiguities with private sector deployments.
- d. Mandate auditing and evaluation procedures by an independent body, such as the National Physical Laboratory (NPL). These procedures could be based on existing ISO standards (e.g. ISO/IEC19795-2: 2007, ISO/IEC19795-6: 2012 and ISO/IEC 19795-1:2021) to ensure that any systems are certified to an appropriate standard before deployment.

11. Any changes to UK biometrics regulation should take into account the distinct legal frameworks of devolved administrations. This will help to apply a more consistent governance approach and reduce the risk that new measures conflict with separate biometric laws in Scotland or Northern Ireland.

Public deliberation

12. The CETaS survey data demonstrated significant variation in public attitudes, with particular concern over the harms that could arise from emerging biometric systems, mixed levels of trust in organisations and preferences for stronger regulation. Inclusive roundtable discussions should be organised by police forces or relevant government departments (e.g. the Home Office) on future biometric technologies to identify areas of positive feedback and concern.

Assessing proportionality

13. Organisations using biometric systems for policing or law enforcement should adopt clear frameworks for proportionality assessments, such as the CETaS framework for assessing proportionality of privacy intrusion of automated analytics.

14. Early-stage testing of biometric systems should seek to minimise potential negative impacts on the public, such as through using consenting volunteers, synthetic datasets and testing in controlled environments before moving to live testing with members of the public. The time period, purpose, impacts, and evaluation methodology of pilots should also be clearly articulated to regulators and the public.

Minimum system requirements

15. The NPL should work with the British Standards Institute (BSI)'s IST/44 biometrics committee to establish mandatory requirements that must be met in the design, deployment, and evaluation of biometric systems. These should include minimum error rates, demographic fairness requirements and human operator considerations across all environmental conditions.

16. The NPL should also test any early-stage biometric systems where there is a lack of a consensus on their scientific evidence base. If such assessments cannot establish appropriate assurance, the system in question should be prohibited for use by policing and law enforcement agencies.

Testing and evaluation standards

17. BSI's IST/44, in consultation with other relevant standards bodies, should explore updating existing standards for the testing and evaluation of biometric systems to incorporate further sociotechnical considerations. These should include:

- a. Potential consequences of system deployments beyond individual privacy, given the increased sensitivity and permanence of biometric data compared with other personal data types.
- b. The role of human error and how to mitigate against this, owing to how the effectiveness of biometric systems can be influenced by human factors such as sensor positioning and data handling.
- c. A requirement for testing and evaluation procedures to be conducted and periodically reviewed throughout the system lifecycle.

Introduction

What are biometrics?

The term 'biometrics' is derived from the Greek words '*bio* -' (meaning life), and '*metric* -' (meaning measurement). The literal meaning therefore refers to the measurement of an individual's life characteristics.¹ In practice, the term is most commonly associated with types of samples, data and systems which together link back to a specific individual based on certain characteristics. More recently, the term has also become associated with data and systems aiming to predict certain attributes (such as age) or states (such as alertness) of individuals.

Historically, systems which utilised biometric data worked by obtaining physical material from an individual (e.g. a fingerprint mark) that human experts analysed to extract the unique features – such as their specific fingerprint ridges. One method would then involve manually comparing these features against a pre-existing sample of a person to determine if they are who they say they are (verification). This process was relatively straightforward and resulted in few errors. Another method involved comparing these features against a database of multiple different samples, to determine if they match to a specific person on that database (identification).² Unlike verification, this latter process was more challenging given the number of comparisons, therefore risking higher error rates.³

Biometric systems convert the relevant features into a 'biometric template', which stores the necessary information in a convenient form for comparison – see Figure 1. The term 'biometric data' is often reserved to refer to these resultant features or templates rather than the initial sample, particularly in law. The process of converting a sample (which may be physical or digital) into templates is not necessarily immediate and may in itself be subject to errors and uncertainties.⁴

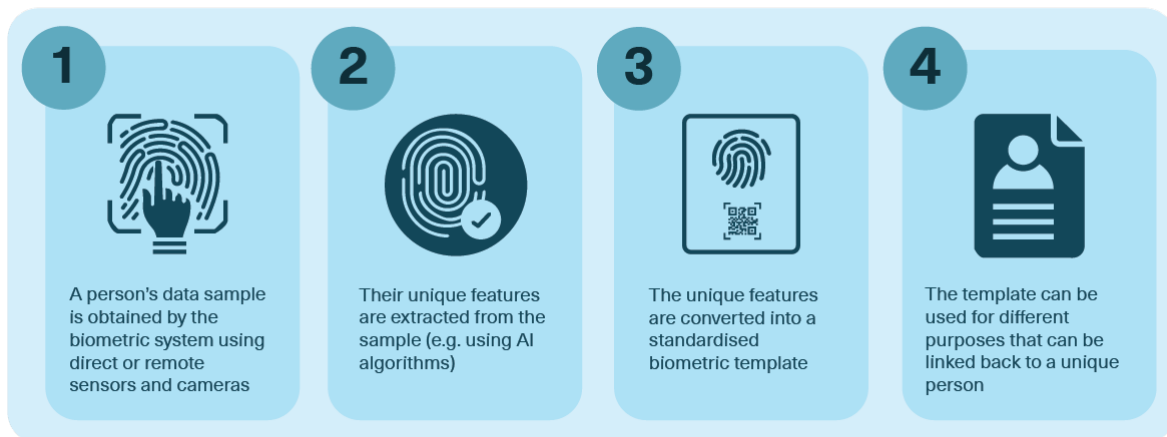
¹ "What are biometrics?," Scottish Biometrics Commissioner, <https://www.biometricscommissioner.scot/biometrics/what-are-biometrics>.

² "What is a biometric system, and how to secure it," Veridium, 19 July 2018, <https://veridiumid.com/biometric-system-secure/>.

³ Government Office for Science, *Biometrics: A Guide* (2018), 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf; Interview with industry representative, 21 November 2023.

⁴ Catherine Jasserand, "Experiments with Facial Recognition Technologies in Public Spaces: In Search of an EU Governance Framework," in *Handbook on the Politics and Governance of Big Data and Artificial Intelligence*, ed. Andrej Zwitter and Oskar J. Gstrein, (Cheltenham: Edward Elgar Publishing, 2023), 5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204452.

Figure 1: Stages of biometric data collection and processing



Digital technologies such as artificial intelligence (AI) have fundamentally changed biometric processing. AI can be understood as machines that perform tasks that would ordinarily require human brainpower to accomplish. Certain novel systems incorporating AI can now capture samples from individuals without needing the direct involvement of the subject, such as remote facial recognition (FR) systems which process images of individual faces. Algorithms can also extract and compare key features more quickly, accurately, securely and against a larger database of other templates than human analysts – speeding up potential matches and reducing error rates.⁵ For instance, a biometric system using soft computing methods was found to have an error rate of 0.18% in 2022.⁶

AI has also created new possibilities to use biometric data for purposes other than verification or identification. New systems have been developed that use statistical correlations between biometric characteristics and certain traits with the aim of classifying individuals into different demographic categories (e.g. age or ethnicity), or to infer emotions and psychological states. These systems have proved controversial due to concerns over their scientific validity and ethical implications. The applications of these systems could therefore, if embedded within society, lead to people being negatively impacted.⁷

⁵ Yash Rawat et al., "The Role of Artificial Intelligence in Biometrics," in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, (19-21 July 2023): 622-626, DOI: 10.1109/ICECAA58104.2023.10212224.

⁶ Vani Rajasekar et al., "Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm," in *Scientific Reports* 12, no. 662 (January 2022), DOI: 10.1038/s41598-021-04652-3.

⁷ Matthew Ryder QC, *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales* (Ada Lovelace Institute: June 2022), 3-7, <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf>.

Figure 2: Examples of established biometric data types

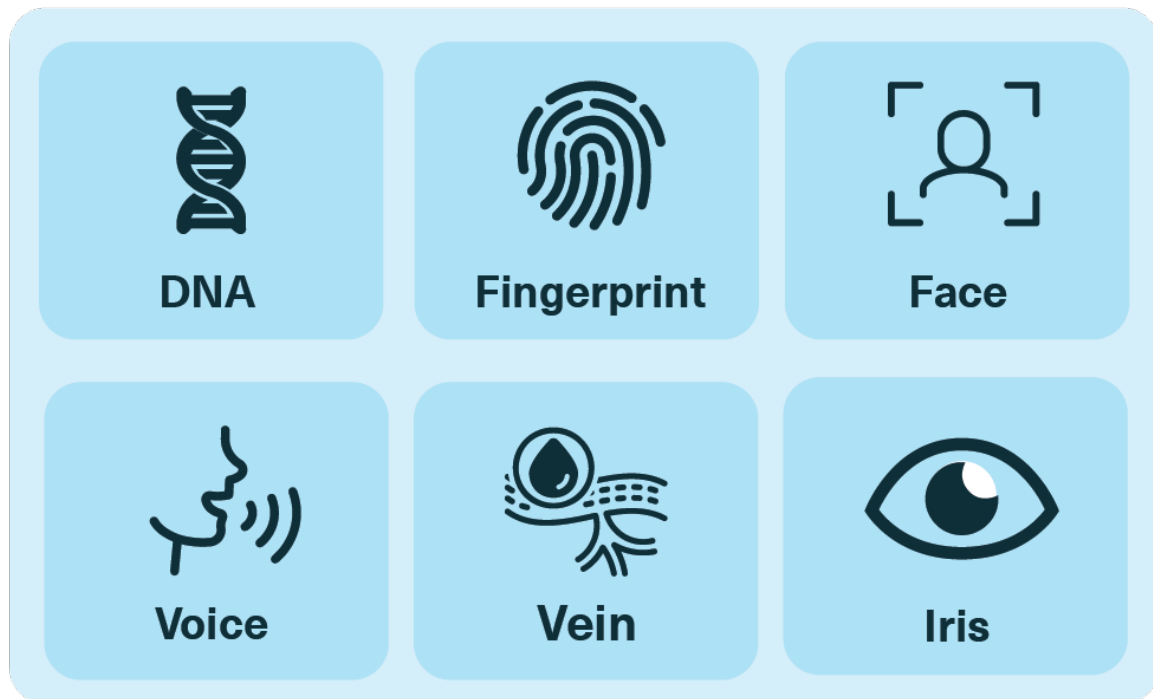
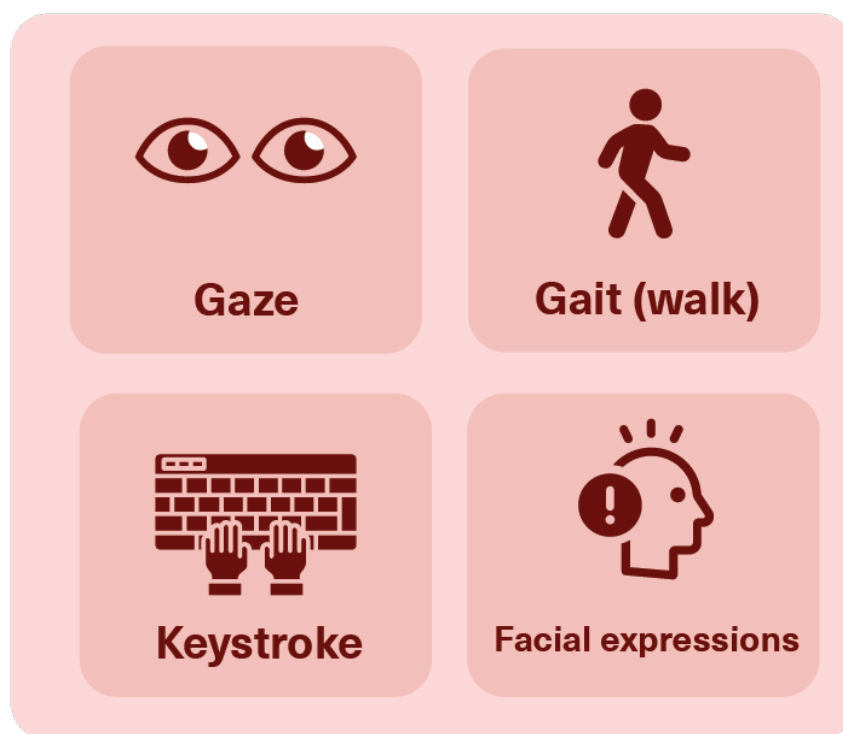


Figure 3: Examples of contested biometric data types



As discussed in the following sections, current discourse tends to define biometric technology as systems used for the purposes of uniquely identifying an individual or verifying their identity. However, this definition is outdated and does not account for the full range of biometrics-based systems now available. Therefore, this report argues for a broader conceptualisation, adopting the following definition of biometric technologies:

Computer-based systems which collect and process physiological data or behavioural data. This data can be used for numerous purposes, for instance to identify an individual, verify their identity, categorise them into different groups, or make inferences about their psychological or emotional states.

We recognise that this expanded categorisation goes beyond existing legal definitions of biometric data. However, as it will be shown, this broader conceptualisation is essential to cover the full range of new risks and regulatory considerations arising from new and emerging biometrics-based systems.

Why are biometrics important?

The collection, analysis and sharing of our biometric data has now become an everyday occurrence – from enabling individuals' identity to be verified at borders, to providing convenient access to personal devices such as mobile phones. For police and law enforcement agencies, biometric data is used routinely to identify suspects present at crime scenes through DNA or fingerprint analysis, and increasingly in crowded public spaces using live facial recognition.

New generative AI tools that produce highly realistic artificial content have already demonstrated the vulnerability of traditional cybersecurity techniques. Across 2023, there was a 704% increase in face swaps, a type of deepfake (or fake content designed to look real) that can be used to trick biometric systems for fraudulent activities.⁸ Given recent evidence showing poor human detection rates against these system attacks, new security risks may therefore arise by opting *not* to use biometric measures.⁹ There are also potential consequences of human error when biometric samples are involved in legal cases. The so-called 'Prosecutor's Fallacy' is where the claimed probability of a sample (e.g. DNA) being matched to an accused person in court is taken to be absolute, while neglecting how

⁸ "New Threat Intelligence Report Exposes the Impact of Generative AI on Remote Identity Verification," iProov, Press Release, 7 February 2024, <https://www.iproov.com/press/new-threat-intelligence-report-exposes-impact-generative-ai-remote-identity-verification>.

⁹ Matthew Groh et al., "Deepfake detection by human crowds, machines, and machine-informed crowds," *Proceedings of the National Academy of Sciences* 119, no. 1 (2022), <https://doi.org/10.1073/pnas.2110013119>.

contextual factors – such as margins of error and sample size – can mean that there is still a likelihood of false association.¹⁰

Nevertheless, biometric systems themselves also present numerous risks. Some of these relate to reliability concerns. Biometrics typically involve comparative analysis of one sample against another (or many others). They also exploit statistical correlations between biometric traits and characteristics. Due to the probabilistic nature of statistical analysis, there is a risk of false positives and false negatives – whether as a result of poor quality data or human error.¹¹ Equally, behavioural inferences (such as detecting emotions) are likely to be highly unreliable due to a lack of scientific validity in the research of inferential systems.

Other risks relate to human rights and proportionality, owing to the unique properties of biometric data compared to other forms of data used to identify individuals. This type of personal data can reveal other sensitive information – such as ancestry, health, or demographics. Given this, there are important considerations over the intrusiveness into an individual's privacy when biometric data is collected. This includes scenarios where police forces are capturing facial images of civilians walking past a system within a crowded public area as part of an operation, who may be unaware of this processing taking place. Possession of biometric data can also enable more effective physical surveillance due to the fact that the information processed is *inseparable* from a person (e.g. their facial features or fingerprints). In doing so, a sense of pervasive monitoring in public could erode individuals' rights of free assembly or expression due to fears over the potential consequences.¹²

Alongside these problems, the UK's existing biometrics legal framework – which consists of a complex web of overlapping equality, human rights, data protection and police powers legislation – has also been criticised as insufficient and unclear.¹³ As far back as 2016, the then-UK Biometrics Commissioner who was responsible for overseeing the use and retention of biometric data raised similar concerns in his annual report, stressing the lack of clarity over 'future governance arrangements'.¹⁴ The publication of the Ryder Review in 2022

¹⁰ David Spiegelhalter and Anthony Masters, "Covid, false positives and conditional probabilities...", *The Guardian*, 25 April 2021, <https://www.theguardian.com/theobserver/commentisfree/2021/apr/25/covid-false-positives-and-conditional-probabilities>.

¹¹ Government Office for Science (2018), 4-5.

¹² Jasserand, 2023, 21.

¹³ Brian Plastow, "Is Scotland 'sleepwalking' towards its place within a UK surveillance state in 2024?," 8 January 2024, <https://www.biometricscommissioner.scot/media/uhbowbhn/sbc-opinion-piece-january-2024.pdf>; Interview with government representative, 10 October 2023.

¹⁴ Paul Wiles, *Annual Report 2016* (Commissioner for the Retention and Use of Biometric Material: March 2017), https://assets.publishing.service.gov.uk/media/5a74eb86ed915d3c7d528fb5/CCS207_CCS0917991760-1_Biometrics_Commissioner_ARA_Accessible.pdf.

further articulated the need for new legal measures to be considered.¹⁵ Despite these mounting concerns, there has been a lack of corresponding progress in changes to regulation and policy, as the law falls further behind innovation.

Methodology and structure

Within this context, CETaS conducted a research project on the future of biometric technology for UK policing and law enforcement. This study aims to move beyond the current debates that specifically concentrate on FR technology, instead considering the full range of biometric technologies currently available and on the near-term horizon.

Research questions

- **RQ1:** What is the ‘state of the art’ in relation to emerging biometric technologies with potential security implications?
- **RQ2:** Where are the current gaps in existing biometric policy and regulation? Is a regime of safeguards for the retention of specific biometric data still fit for purpose, as opposed to a system that primarily regulates the *use* of biometric technologies?
- **RQ3:** What regulatory and policy actions are needed to ensure that emerging developments in this area are adequately covered for policing and law enforcement usage?
- **RQ4:** What distinctions should be drawn between the use of biometrics by public and private sector organisations when considering the potential for intrusion and the safeguards required?

Methods

1. **Literature review:** the research team analysed relevant biometric regulatory and policy measures in the UK, policing and law enforcement trends, use cases and risks from future developments in biometric technology.
2. **Interviews:** semi-structured, anonymised interviews between August and November 2023 with 35 participants across academia, civil society organisations, UK government, policing and industry. Participants were identified through a purposive sampling strategy to ensure informed responses.

¹⁵ Matthew Ryder QC (2022), 3-7.

3. **Workshop:** an invitation-only workshop held in January 2024 entitled, “Stress-Testing Future Biometrics Policy Options for Policing and Law Enforcement”. This session gathered 12 experts from law enforcement, regulators and other relevant areas of government, to review different potential regulatory approaches for biometrics.
4. **Survey:** to investigate public perceptions towards biometric technologies, CETaS conducted a survey with a representative sample of 662 UK-based respondents. Key themes from the survey can be found in Section 5, while more detail on the methodology and results can be found in Appendix 1.
5. **Freedom of Information (FOI) requests:** CETaS submitted a series of FOI requests to the Home Office in November 2023. These were based on emergent findings from the literature. The results can be found in Sections 2 and 3.

Limitations

1. This study is focused on the use of biometric systems within a policing and law enforcement context. That is, when the technology is used by public bodies – or private sector organisations acting on behalf of the state – for activities designed to protect the public.
2. This study does not explore the regulation of *covert* uses of biometric systems by policing and law enforcement, which fall under different legislative frameworks. As such, the study is solely concerned with *overt* deployments of this technology.
3. The focus of this report is on data-driven biometric technology. Therefore the report does not explore non-digital biometric samples taken and retained by police and law enforcement agencies.
4. While the report does cover technical trends in the development of biometric systems, particularly those that have implications for policy and legislation, detailed analysis of state-of-the-art adversarial attacks on biometric systems are out of scope.

Structure

This report is structured as follows. **Section 1** explores the definition and scope of the term ‘biometric data’ and ‘biometric systems’, summarising disagreements between experts in the field. **Section 2** provides an overview of the opportunities and benefits of biometric systems, exploring both current applications and future trends. **Section 3** discusses the risks and challenges posed by biometric systems, such as demographic bias and human

rights considerations. **Section 4** provides an overview of existing legal and policy frameworks for biometric technologies and their limitations. **Section 5** details the key findings from the public survey, while **Section 6** concludes with a discussion of alternative regulatory and policy measures which the UK could adopt to improve governance and oversight.

1. Definitions and Taxonomies

This section introduces our understanding of ‘biometrics’, where disagreement lies between stakeholders on what should be included under this concept, and the need to move towards understanding biometrics as a ‘spectrum’ rather than a discrete category of technologies.

1.1 Defining biometrics: limits and issues

Within the existing literature, many taxonomies are used to categorise different types of biometrics. The most common distinctions include the following (although specific definitions often vary).








- **Soft vs hard biometric data.** *Hard biometrics* are integral characteristics of a person which can be used for uniquely identifying them to a high degree of confidence, such as fingerprints and DNA. Conversely, *soft biometrics* relate to learned characteristics (e.g. gait /walking patterns) and non-unique integral characteristics (e.g. eye colour). While learned characteristics are weaker identifiers for matching back to a specific person, non-unique integral characteristics could be used in addition to other biometric samples for increasing the *accuracy* of identifying a specific person.¹⁶
- **Physiological vs behavioural biometric data.** The former rely on physical characteristics, including someone’s face or fingerprints, while the latter relate to patterns in behavioural characteristics of the human body, such as keyboard stroke or gait.¹⁷
- **Direct vs remote biometric systems.** *Direct* biometric systems rely on physical contact with the subject. These include traditional biometric data types, like requiring someone to present their fingerprint. *Remote* systems, however, can capture the necessary information from remote sensors and processes. For instance, face and gait recognition do not need the active engagement of an individual.¹⁸

¹⁶ Government Office for Science (2018), 3.

¹⁷ Christiane Wenderhorst & Yannic Duller, *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* (European Parliament’s Policy Department for Individuals’ Rights and Constitutional Affairs: August 2021), 67-68, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf).

¹⁸ “Remote biometric identification: a technical & legal guide,” EDRI, 23 January 2023, <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>.

Table 1: Common distinctions of biometric data types

Biometric data	Hard or soft	Physiological or behavioural	Direct or remote
DNA 	Hard	Physiological	Direct
Fingerprint 	Hard	Physiological	Direct
Face 	Hard	Physiological	Remote
Voice 	Soft	Behavioural	Remote
Gait 	Soft	Behavioural	Remote
Facial expressions 	Soft	Behavioural	Remote
Keystroke 	Soft	Behavioural	Remote

Experts continue to disagree over these definitions, and what should be interpreted as falling under the term ‘biometrics’.¹⁹ This includes whether emergent applications should be included (e.g. those using physiological and behavioural data to classify individuals into categories rather than identify them).²⁰ Existing legal frameworks in the UK and EU define biometric data in a narrow sense, where it is only considered as such when it involves the unique identification of a person.²¹

However, several interviewees and legal experts have criticised this current framing on the basis that when originally drafted, these regulations did not account for how the integration of AI has led to the rise of new functions for biometrics (such as classification and inferential uses) that fall outside existing frameworks and may pose a risk to human rights.²² Some therefore advocate for expanding the definition of biometrics, to ensure that such additional applications are scrutinised and explicitly regulated.

In contrast, some interviewees believed that expanding the legal concept of biometric data or systems would have more negative implications than retaining the existing one. Widening the definition to include some technologies that are widely believed to lack scientific validity may damage the reputation of more reliable systems and vendors.²³ For instance, controversial emotion recognition systems could then be permitted for integration into applications, on the basis of being legally defined as a form of biometrics. Yet any negative impacts on individuals resulting from such integration could lead to an erosion in trust with other biometric systems (e.g. verification models) which offer security benefits.²⁴

1.2. Understanding biometrics as a ‘spectrum’

Ongoing disagreements over fundamental definitions of biometric technologies have undermined the ability to revise existing regulatory frameworks, ensuring they remain up to

¹⁹ Interview with academic representative, 25 September 2023; Interview with academic representative 28 September 2023; Interview with academic representative, 10 October 2023; Interview with industry representatives, 12 October 2023.

²⁰ For an example in the literature of a more expansive concept of biometrics, see: <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf>, 16-20.

²¹ “What is special category data?,” ICO, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd4>.

²² Interview with academic representative, 25 September 2023; Interview with academic representative, 28 September 2023; Interview with academic representative, 10 October 2023; Matthew Ryder QC (2022), 3-7; ICO, *Biometrics: Foresight* (October 2022), 8-11, <https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf>.

²³ Interview with industry representatives, 12 October 2023.





²⁴ Gloria Fuster and Michalina Peeters, *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence* (Panel for the Future of Science and Technology: December 2021), 20-21, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU\(2021\)697191_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf).

date and address new issues that arise.²⁵ A large portion of interviewees therefore believed that it was better to understand biometric technologies as a 'spectrum'.²⁶

A spectrum of biometric systems

There is a need clarify the different types of biometric systems that have emerged in recent years, to facilitate more precise discussion about the implications and risks associated with distinct uses. The taxonomy outlined in Table 2 was developed from these insights.

Table 2: Taxonomy of biometric systems

Biometric system	Purpose	Relative degree of public acceptability ²⁷
Verification 	Uses a 1:1 match to determine if an individual is who they say they are	High Typically requires active user involvement and match is only compared against a single data source, so may have lower margins of error
Identification 	Uses a 1:N (one-to-many) match to determine if an individual corresponds to a member of a pre-existing database of multiple biometric samples	Medium Typically does not require user's direct involvement and data comparisons against a larger database may increase the margin of error
Classification 	Used to classify individuals into different groups	Low Includes some systems that lack scientific validity, as well as some that raise significant ethical concerns (e.g. racial profiling)
Inferential 	Used to make inferences about someone's psychological or emotional state	Very low Includes some systems that lack scientific validity, as well as some with potentially malicious uses (e.g. coercive manipulation)

²⁵ Interview with academic representative, 25 September 2023.

²⁶ Interview with government representative, 27 October 2023; Interview with government representative, 31 October 2023; Interview with government representative, 2 November 2023; Interview with academic representative, 2 November 2023.

²⁷ Based on the results of the CETaS public survey (see Section 5) and interview analysis.

The spectrum of biometric data

As with the subtleties between biometric systems, similar analysis is applicable to biometric data. Biometric modalities are sometimes assumed to involve one key feature that is extracted (e.g. geometric measurements from a person's face to verify their identity). In reality, these modalities can contain a diversity of data types. From a person's face, other data features such as wrinkles or eye shape could be extracted for classification purposes such as estimating that person's age.

Current legislation typically covers some of these processes, in that only data which is used for identification or verification purposes is considered "biometric". While other "special category" data as defined in UK GDPR could protect against certain use cases (such as when the information could reveal one's ethnic origins), this may not address inferences made about one's behaviour or emotions, which could still create significant risks to human rights. This is because they operate a 'fuzzy' zone within the realm of personal data, where although it may not always be linked back to a specific person, individuals cannot easily change learned or inner traits compared to other forms of personal data.²⁸

A key finding from the survey was the level of concern over emotion recognition systems, due to the belief that emotions were highly sensitive information to an individual. As such, more nuances may be needed to ensure that stricter protections are in place, such as by defining a new legal term for 'biometric-based data'.²⁹ Table 3 shows how this could work in practice, with a hypothetical example of a police officer analysing a voice recording to assist in catching a suspect who fled a crime scene.

Table 3: Biometric data vs. biometric-based data

Data category	Summary
Biometric data	A police officer uses an AI system to capture a voiceprint of a fleeing suspect from a voice recording which is unique to that individual.
Biometric-based data	A police officer uses an AI system to assess the likely demographic profile of a fleeing suspect (e.g. age group, gender and native vs. non-native English speaker) from certain elements of their voice recording, such as pitch and tone.

²⁸ Wendehorst & Duller (2021), 68.

²⁹ Ibid. 69.

Taken together, the range of biometric systems and data types described above may lead to new applications in different sectors (see below). Although certain use cases could be beneficial, others may pose risks to individuals (e.g. job screening based on perceived emotions discriminating against neurodivergent candidates).

Table 4: Current and future applications of biometric systems and data

Use case	Biometric system	Modality and feature
Age verification for alcohol purchases at supermarket self-checkouts ³⁰	Classification	Face (geometry and features)
Targeted demographic-based advertising (e.g. age and gender-specific)	Classification	Face (geometry and features)
Pain monitoring for non-verbal patients ³¹	Inferential	Eyes (pupil dilation); heart (pulse); respiratory system (breathing rate)
Online job interview candidate screening based on perceived emotions ³²	Inferential	Face (facial expression); eyes (eye movement)

³⁰ “Asda to trial digital ID at self-checkouts,” Asda, 31 January 2022, <https://corporate.asda.com/newsroom/2022/01/31/asda-to-trial-digital-id-at-self-checkouts>.

³¹ “PMD-200,” Medasense, <https://medasense.com/pmd-200/>.

³² Will Knight, “Job Screening Service Halts Facial Analysis of Applicants,” *WIRED*, 1 December 2021, <https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/>; Katina Michael et al., “Biometrics and AI Bias,” *IEEE Transactions on Technology and Society* 3, no. 1 (March 2022): 1-8, DOI: 10.1109/TTS.2022.3156405.

2. Opportunities and Benefits for Public Safety

This section provides an overview of current and potential future applications of biometric systems for policing and law enforcement. Broader technological and societal trends relating to the development of biometric technologies are also discussed.

2.1. Current applications

It is important to note that, particularly within a UK context, the roles of police and law enforcement are distinct. The former relate to the 45 territorial and 3 special police forces which are responsible for a broad range of policing duties in specific regions. The latter relate to agencies with non-regional duties and specific areas of remit, such as the National Crime Agency (NCA) and UK Border Force. While both types of organisations may deploy similar biometric systems, they are often used for different purposes. FOI requests obtained by CETaS and further analysis highlight some of the existing biometric data types used by police and law enforcement, as well as the scale of data samples available for tackling crime:

- As of October 2023, there were **16,572,608 custody facial images held on the Police National Database (PND)**.³³ It is highly likely that images of individuals who were never charged or were cleared of all charges remain stored on the PND indefinitely.³⁴
- As of 31st March 2022, there were **870,705 subject profile records** and **685,063 crime scene DNA profile records held on the National DNA Database (NDNAD)**.³⁵
- As of 31st March 2022, there were **27,168,685 fingerprint forms relating to 8,562,878 individuals and 2,009,989 unidentified crime scene marks held on the National Fingerprint Database and National Automated Fingerprint Identification System (now known collectively as IDENT 1)**.³⁶

³³ Freedom of information request submitted to the Home Office by CETaS on 24 November 2023.

³⁴ Cahal Milmo and Mark Wilding, "Hundreds of thousands of innocent people on police databases as forces expand use of facial recognition tech", *iNews*, 29 September 2023, <https://inews.co.uk/news/police-secretive-facial-recognition-database-millions-innocent-people-2635445>.

³⁵ Ben Snuggs, *Forensic Information Databases Strategy Board Annual Report: April 2021 - March 2022* (Home Office and National Police Chiefs' Council: May 2023), 9, https://assets.publishing.service.gov.uk/media/646c7fe6a726f60013cebc09/Forensic_Information_Databases_Strategy_Board_Annual_Report_2021-22_Web_Accessible__002_.pdf.

³⁶ Ibid.

The main examples of how law enforcement currently use biometrics include:

- **Border security and immigration:** UK Border Force collects fingerprints and facial images to support the UK immigration system, such as when verifying the identity of an individual seeking to enter the UK who cannot produce a document establishing identity, nationality or citizenship.³⁷
- **Domestic security:** fingerprint scanners are currently being rolled out by the Home Office to replace the use of ankle tags to monitor individuals facing deportation.³⁸
- **Air and rail travel:** FR technology is also used in 'ePassport' gates available at some British air and rail ports, while trials of passport-free e-gates using FR systems are due to begin in 2024.³⁹

By contrast, UK policing currently uses biometrics in two ways:

- DNA and fingerprints can be used for the purpose of **evidential forensics**, such as informing evidence during a court trial as to whether someone was present at a crime scene.
- Other biometrics can be used for **intelligence and crime prevention purposes**. Suspects or wanted individuals may have their images compared against CCTV or police watchlists to help determine who the person is and assist in narrowing down potential geographical areas where they may be present based on recent footage.⁴⁰ DNA and fingerprints can also be collected from arrested persons (and crime scenes) to confirm an individual's identity for investigations.⁴¹ The use of the polygraph is discussed further below.

Some of the most prominent biometric technologies in use by policing and law enforcement agencies include mobile fingerprint scanners and FR systems. Pronto mobile devices, first deployed by West Yorkshire Police in 2018, enable officers to check fingerprints from the

³⁷ HM Government, *Biometric enrolment: policy guidance* (Home Office: February 2024), 4, <https://assets.publishing.service.gov.uk/media/653a41a9e6c9680014aa9b62/Biometric+information+-+enrolment.pdf>.

³⁸ Nicola Kelly, "UK plans GPS tracking of potential deportees by fingerprint scanners," *The Guardian*, 13 January 2023, <https://www.theguardian.com/uk-news/2023/jan/13/potential-deportees-fingerprint-scanners-gps-tracking-home-office-plans>.

³⁹ Ben Clatworthy, "No passports needed under Border Force e-gate plan," *The Times*, 1 January 2024, <https://www.thetimes.co.uk/article/uk-flights-passports-border-force-queues-szdd39c5x>.

⁴⁰ HM Government, *Biometrics Strategy: Better public services, maintaining public trust* (Home Office: June 2018), 12, https://assets.publishing.service.gov.uk/media/5b34f69c40f0b60b107a4a80/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.

⁴¹ Ibid.

field against national database records in real-time.⁴² These increase the efficiency of verification and identification processes, which previously would have necessitated arresting and holding an individual in custody while conducting hours of enquiries.⁴³

There are three types of FR used by UK police forces.⁴⁴

- **Operator Initiated Facial Recognition (OIFR):** use of a mobile application to check a person of interest's identity against the police national database without having to take them into custody.
- **Retrospective Facial Recognition (RFR):** use of images supplied after an event or incident for comparison against national custody images of individuals on the PND.
- **Live Facial Recognition (LFR):** use of live video capture to identify a person of interest in real time.

Currently, police use of LFR has been limited – and restricted to a small number of forces including the Metropolitan Police Service (MPS), South Wales Police (SWP) and Essex Police. However, any new regulatory changes or operational requirements could lead to greater uptake across forces. Indeed, the MPS is already working with a group of large retailers on the 'Pegasus' initiative, where the police are analysing CCTV images and using RFR technology to identify prolific shoplifters.⁴⁵

Police forces do not currently use novel classification and inferential biometrics, but polygraph technology (also known as the 'lie detector') is used by the Probation Service to monitor people convicted of sexual, domestic abuse and terrorism-related offences – ensuring they comply with harm prevention orders.⁴⁶ Nevertheless, recent analysis has found that individuals arrested on suspicion of sex offences have also been subjected to the polygraph, despite not having a conviction, which represents a potential misuse of policing powers.⁴⁷

⁴² Motorola Solutions, "Pronto Biometrics – Fingerprint Identification," Motorola Solutions, 2018, https://www.motorolasolutions.com/content/dam/msi/docs/en-xu/public-safety/pronto_biometric_app.pdf.

⁴³ Home Office (2018), 6-8.

⁴⁴ Home Office, "Police use of Facial Recognition: Factsheet," Home Office in the media blog, 29 October 2023, <https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/>.

⁴⁵ Divya Talwar and Eleanor Layhe, "Small shops call for aid to tackle 'brazen' shoplifters," *BBC News*, 16 September 2023, <https://www.bbc.co.uk/news/uk-66819837>

⁴⁶ Cahal Milmo and Mark Wilding, "Police forces may be exceeding powers in the use of lie detectors," *iNews*, 1 January 2024, <https://inews.co.uk/news/uk-police-forces-expanding-lie-detector-tests-2822226>.

⁴⁷ Ibid.

2.2. Future trends and applications

Technological trends

Advances in biometric technologies are likely to proliferate out to 2030 and beyond due to innovation driven by a range of factors from consumer demand to increasingly sophisticated adversarial attacks on systems. Some of these advances will relate to new *forms* of biometric processing.

Table 5: Future biometric formats

Format trend	Summary
Cancellable biometrics	Biometric templates are transformed in such a way that, if they are compromised, the original feature cannot be determined. A new version would then need to be reissued (akin to resetting a password). ⁴⁸
Multi-modal biometrics	These systems collect data from several biometric modalities (such as keystroke analysis alongside fingerprint recognition) or use a single modality to extract multiple forms of data (e.g. extracting gaze estimation and pupil diameter data from a single eye image). ⁴⁹ This trend may help mitigate some of the existing problems associated with individual systems, such as sensor accuracy. ⁵⁰
Frictionless biometrics	Where little (or no) physical contact or pausing is required to gather biometric data. ⁵¹ This will offer enhanced efficiency and convenience, but the ability to use these systems at a distance without requiring someone’s awareness is likely to prompt questions surrounding consent for data processing. ⁵²

Alongside these new formats, there will be changes related to both the wider *design* and *performance capabilities* of biometrics systems. Further advancements in deep learning

⁴⁸ Interview with industry representative, 29 September 2023.

⁴⁹ ICO, *Biometrics: insight* (ICO: October 2022), 6, <https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf>.

⁵⁰ Interview with academic representative, 22 September 2023.

⁵¹ ICO, *Biometrics: insight* (ICO: October 2022), 5, <https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf>.

⁵² ICO, *Biometrics: foresight* (ICO: October 2022), 5, <https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf>.

could enable improved FR in challenging conditions, such as reduced visibility and low-resolution cameras,⁵³ as well as with masked faces.⁵⁴ This could allow for more flexible deployment of the technology, without compromising accuracy.⁵⁵ Biometric systems could also become more accessible in the next decade as hardware miniaturisation allows for heightened portability, while software will increasingly be integrated into mobile phones and drones.⁵⁶

As the private sector provides increased access to personal surveillance systems through the consumer market, the volume of potential biometric data could increase exponentially. This phenomenon is already underway; one in five British households uses doorbell cameras⁵⁷ and a quarter of British drivers use dashcams.⁵⁸ One interviewee believed that the abundance of images and videos shared online will contribute to this trend, and that biometric information can no longer be considered confidential.⁵⁹ With advances in AI lowering the barrier to entry for forging identities, veracity (the accuracy and reliability of biometric information used for verification) will play a key role in the future.⁶⁰

Future applications

The development of existing and emergent technologies could enable a range of new applications relevant to policing and law enforcement in the UK. The below applications were posited as potentially useful and worthy of further consideration by research participants.

Three-dimensional (3D) FR or accurate iris recognition under imperfect conditions could be useful for identifying or verifying a known individual.⁶¹ Contactless fingerprint verification could be valuable for border control applications, as well as for the identification of missing

⁵³ Katina Michel et al., (2022).

⁵⁴ Marta Gomez-Barrero et al., "Biometrics in the Era of COVID-19: Challenges and Opportunities," *IEEE Transactions on Technology and Society* 3, no. 4 (December 2022): 307-322, DOI: 10.1109/TTS.2022.3203571.

⁵⁵ Interview with government representative, 24 October 2023.

⁵⁶ Interview with industry representatives, 31 October 2023; Interview with academic representative, 22 September 2023; Cahal Milmo and Mark Wilding, "Police across UK equipped with live facial recognition bodycams," *iNews*, 25 November 2023, <https://inews.co.uk/news/police-uk-live-facial-recognition-bodycams-2775720>.

⁵⁷ Dominic Penna, "More households install alarms and doorbell cameras over crime fears," *The Telegraph*, 1 May 2023, <https://www.telegraph.co.uk/news/2023/05/01/people-turn-to-diy-security-amid-crime-fears/>.

⁵⁸ RAC, "New app could soon turn every car into a speed camera – and report traffic offences at the touch of a button," RAC Drive News, 20 March 2023, <https://www.rac.co.uk/drive/news/driving-tech/new-app-could-soon-turn-every-car-into-a-speed-camera/>.

⁵⁹ Interview with industry representative, 21 November 2023.

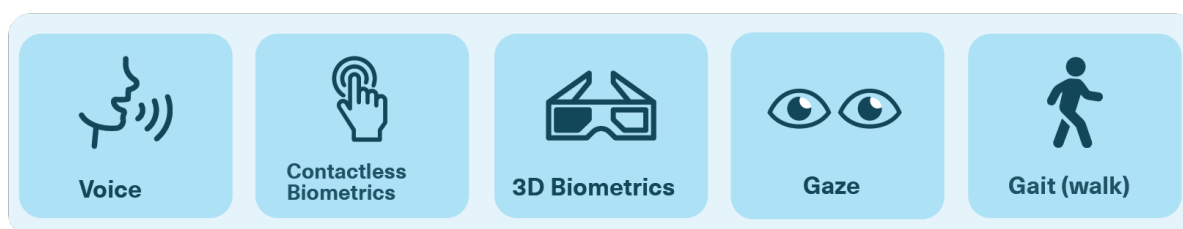
⁶⁰ Interview with policing representative, 6 October 2023.

⁶¹ Interview with industry representative, 12 October 2023.

persons.⁶² Emergent systems such as gait analysis and gaze estimation (which predicts where a person is looking) are likely to see greater multi-sectoral use.⁶³ For instance, future gait analysis systems could indicate whether someone is concealing a weapon,⁶⁴ while gaze estimation could be used to monitor individual behaviour considered to be suspicious – for instance to detect whether they are conducting hostile reconnaissance.⁶⁵

One interviewee suggested it may actually be unethical *not* to use new biometric systems – especially if they are shown to better protect vulnerable individuals compared to existing tools and humans.⁶⁶ Voice recognition technology in particular was mentioned as being currently underutilised for public safety purposes.⁶⁷ The large volume of available audio samples on video and social media platforms is an enabling factor behind the fast-paced development of voice recognition systems.⁶⁸ INTERPOL's global voice database (SiiP) is their third-largest biometric database, demonstrating the utility of this particular modality.⁶⁹

Figure 4: Potential future biometric trends for policing and law enforcement



⁶² Interview with policing representative, 6 October 2023.

⁶³ Interview with industry representative, 12 October 2023.

⁶⁴ Interview with industry representative, 31 October 2023.

⁶⁵ Virginio Cantoni et al., "Gaze-based biometrics: An introduction to forensic applications," *Pattern Recognition Letters* 113, (October 2018): 54-57, <https://doi.org/10.1016/j.patrec.2016.12.006>.

⁶⁶ Interview with industry representative 2, 12 October 2023.

⁶⁷ Interview with policing representative, 6 October 2023.

⁶⁸ Fieke Jansen, Javier Sánchez-Monedero, and Lina Dencik, "Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP." *Big Data & Society* 8, no. 2 (2021), DOI: 20539517211063604.

⁶⁹ Ibid.

3. System Risks and Challenges

This section presents risks and challenges associated with the use of biometric systems for policing and law enforcement.

3.1. Reliability: Performance, bias, and scientific validity

The impact of environmental factors on performance

Environmental factors, such as lighting conditions or image quality, can significantly impact the performance of biometrics systems. These include factors related to *how data subjects interact with the system* (e.g. finger placement for fingerprint systems),⁷⁰ *how practitioners operate the system* (e.g. the placement of cameras),⁷¹ and *other external factors* (e.g. lighting conditions).⁷² These environmental factors have implications for the real-world reliability of systems under different conditions. At worst, such errors in a law enforcement context could result in wrongful arrests (from false positives) or allow perpetrators to avoid apprehension (false negatives).⁷³ It is also important to recognise how human operators themselves can be affected by environmental factors. Fatigue, distractions, multi-tasking commitments and time pressures could all undermine the optimal performance of biometric systems or exacerbate existing technical deficiencies.⁷⁴

Demographic bias

Of particular concern is the risk of differences in system performance for different demographic groups.⁷⁵ One participant described how fingerprints can be less reliable for the elderly, Asian females, or those undergoing chemotherapy, due to less well-defined

⁷⁰ Interview with academic representative, 22 September 2023.

⁷¹ Science, Innovation and Technology Committee, "Governance of artificial intelligence (AI) - Oral evidence," 24 May 2023, 28, <https://committees.parliament.uk/oralevidence/13201/pdf/>; Interview with government representative, 24 October 2023.

⁷² Interview with academic representative, 6 October 2023.

⁷³ Madeleine Chang, *Countermeasures: the need for new legislation to govern biometric technologies in the UK* (Ada Lovelace Institute: June 2022), <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf>.

⁷⁴ Interview with industry representative, 21 November 2023.

⁷⁵ Pawel Drozdowski et al., "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Transactions on Technology and Society* 1, no. 2 (2020): 89-103; Chang (2022); Interview with industry representative, 12 October 2023; Interview with industry representative 2, 12 October 2023; Interview with industry representative 2, 20 October 2023.

fingerprint ridges.⁷⁶ Increased awareness of demographic bias has resulted in efforts to collect more diverse training datasets, and more concerted efforts to measure performance for certain groups. However, these are typically restricted to a narrow range of dimensions (e.g. race or gender, while ignoring factors such as disability) and categories (e.g. comparing male versus female, while ignoring identities such as non-binary).

Mitigating demographic bias is particularly critical in law enforcement (e.g. entry and freedom of movement), given the potential impact on individuals' human rights. Close attention should therefore be paid to how bias may enter in biometric systems, including within datasets or system outputs.⁷⁷ Bias can also be introduced by humans-in-the-loop (operators using the system) which can be more difficult to test and detect.⁷⁸ This should be taken into account during testing and evaluation processes to avoid potential discriminatory implications arising from the wider deployment setup.

Questions over scientific validity

While the debate over identification systems has often focused on skewed datasets and environmental factors, critics of certain *inferential* systems have pointed to more fundamental limitations. Emotion detection – which aims to infer emotional states from facial images, speech and other characteristics – has been widely criticised as ‘pseudoscience’.⁷⁹ Critics suggest there is a lack of evidence that external expressions can infer emotional states, and that how emotions are displayed depends on social and cultural contexts. Some particular *classification* systems have also been labelled as ‘pseudoscience’, such as those that predict age based on bone structures, or sexuality based on facial features.⁸⁰ Subsequently, police and law enforcement should be particularly cautious of the hype and overselling of these new and often unproven technologies and, in

⁷⁶ Interview with industry representative 2, 12 October 2023; “Data protection requirements when using biometric data,” ICO, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/guidance-on-biometric-data/data-protection-requirements-when-using-biometric-data/>.

⁷⁷ Malak Sadek, Sam Stockwell and Marion Oswald, *Evaluating the use of facial recognition in UK policing*, (The Alan Turing Institute: December 2023); Interview with industry representative 2, 12 October 2023; Interview with industry representative, 12 October 2023.

⁷⁸ Ibid; Interview with industry representative, 21 November 2023.

⁷⁹ Meredith Whittaker et al., *AI Now report 2018* (AI Now Institute: December 2018), <https://ainowinstitute.org/publication/ai-now-2018-report-2>; Amba Kak and Sarah Myers West, *2023 Landscape: Confronting Tech Power* (AI Now Institute: April 2023), <https://ainowinstitute.org/2023-landscape>; Lisa Feldman Barrett et al., “Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements,” *Psychological science in the public interest* 20, no. 1 (2019): 1-68; Interview with industry representative, 26 September 2023; Interview with academic representative, 2 October 2023.

⁸⁰ Interview with academic representative, 28 September 2023.

cases where the scientific evidence base is uncertain, prohibit the use of such systems due to the risks that may arise.⁸¹

Adversarial attacks

Although not a focus of this report, the increasing advancement of adversarial attacks is an ongoing risk. These attacks aim to trick biometric systems – for example to achieve false matches for verification (spoofing), or to avoid detection from identification systems (masking), such as through obscuring sensors.⁸² Progress in generative AI techniques, along with the increased availability of publicly available biometric data (e.g. facial images) has enabled increased performance in some attacks.⁸³ Threats to system security are particularly important in a law enforcement context, for example actors attempting to spoof verification systems to gain unauthorised access to a system, device or premises.

3.2. Concerns around data collection and sharing

AI-based systems often require very large training datasets. This has resulted in several controversies whereby biometric images or videos are scraped from the Internet without the explicit knowledge or consent of data subjects, who may not have expected their data to be used for such purposes.⁸⁴ In 2022, Clearview AI was fined for breaching data protection laws by the ICO, who accused the company of unlawfully collecting Internet data on individuals from the UK and globally to create a FR database that was accessible for police departments.⁸⁵ Leakage or theft of biometric data can be particularly harmful to affected individuals and organisations based on its sensitive nature. For example, everyone can change compromised passwords. However, since biometric information is encoded in an individual's body or behaviour, such information may be impossible to replace if compromised without additional protections. Genetic data can also contain information about relatives, posing a privacy threat beyond the individual in question.⁸⁶

⁸¹ Interview with academic representative, 25 September 2023.

⁸² Interview with academic representative, 22 September 2023; Interview with academic representative, 6 October 2023; Interview with industry representative 2, 12 October 2023; Interview with academic representative, 22 September 2023.

⁸³ Interview with industry representative, 21 November 2023.

⁸⁴ Nicolas Kayser-Bril, "Face recognition data set of trans people still available online years after it was supposedly taken down," *Algorithm Watch*, 15 September 2022, <https://algorithmwatch.org/en/dataset-face-recognition>.

⁸⁵ "ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted," ICO News and Blogs, 23 May 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>.

⁸⁶ Interview with academic representative, 2 November 2023.

3.3. Appropriate use and impacts to civil liberties

Many applications of biometrics technologies have been criticised on ethical grounds, rather than performance. These relate to the use of systems in ways that can negatively impact human rights, such as during protests, or by oppressive regimes to identify minority groups, track journalists and for other authoritarian purposes.⁸⁷ While many inferential systems (such as emotion detection) have been described as pseudoscientific, highly subjective and context-dependent – *accurate* inferential systems would also raise serious concerns. These systems could intrusively reveal intimate states, such information could be misused (e.g. for manipulation), and individuals may have little control over the signals used to acquire such predictions.⁸⁸ Several classification systems that aim to predict demographic characteristics such as race and gender may also be problematic, given that these can be contextual, fluid, and political, with many individuals viewing themselves through a multicultural lens.⁸⁹

Human rights considerations

Concerns have been raised that biometric systems can disproportionately interfere with human rights, including the right to respect for private life (Article 8 of the European Convention on Human Rights, ECHR), freedom of expression (Article 10 ECHR), and freedom of assembly and association (Article 11 ECHR). LFR in particular has been a topic of heated debate regarding its impact for civil liberties, especially given its increasing use in public spaces.⁹⁰ Beyond these immediate impacts, some have highlighted ambiguity over how biometric systems could also lead to unpredictable impacts and harm in future. Even if systems are introduced in constrained settings under tight controls for a specific purpose, there is a risk of ‘mission’ or ‘function creep’ and the expansion of use over time.⁹¹ Indeed, one interviewee was concerned that discussions on FR had moved from static one-off uses

⁸⁷ Richard Van Noorden, “The ethical questions that haunt facial-recognition research,” *Nature* 587, no. 7834 (2020): 354-359; Conor Healy and Donald Maye, “Punishing Journalists PRC Province’s Latest Mass Surveillance Project, Won by Neusoft Powered by Huawei,” IPVM, 29 November 2021, <https://ipvm.com/reports/henan-neusoft>.

⁸⁸ Wendehorst & Duller (2021).

⁸⁹ Nenad Tomasev et al., “Fairness for unobserved characteristics: Insights from technological impacts on queer communities,” in *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (New York: Association for Computing Machinery, 2021), 254–265; Ruha Benjamin, “Race after technology,” in *Social Theory Re-Wired: New Connections to Classical and Contemporary Perspectives*, ed. Wesley Longhofer and Daniel Winchester (Routledge, 2023), 405-415.

⁹⁰ Chang (2022).

⁹¹ Zara Rahman, Paola Verhaert, and Carly Nyst, *Biometrics in the humanitarian sector* (Oxfam: 2018), <https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620454/rr-biometrics-humanitarian-sector-050418-en.pdf?sequence=1>.

towards their use in conjunction with body-worn cameras,⁹² which could contribute to a problematic normalisation of increased surveillance.⁹³

Proportionality and consent

Since the use of biometric technologies can impact human rights, whether such rights should be infringed upon for policing or law enforcement requires a legal framework that meets the standards for the rule of law and the linked requirements of necessity and proportionality.⁹⁴ Participants at a recent workshop hosted by The Alan Turing Institute and Metropolitan Police highlighted that proportionality assessments could not be limited to either technical or legal evaluations – instead requiring consideration of policies, procedures and evaluation mechanisms.⁹⁵ The CETaS *Structured Framework for Assessing Proportionality of Privacy Intrusion of Automated Analytics* provides one such framework for bringing these elements together, which aims to cover the entire lifecycle of analytic systems.⁹⁶

To improve proportionality during system trials, UK policing should also ensure that all procedures include a range of testing options from highly controlled environments towards operational conditions, moving along as the testing (and subsequent necessary improvements) provides assurance of the system's reliability. This was reflected in France's approach, where it deployed FR technology with consenting volunteers who were compared against a watchlist containing a combination of their own and AI-generated faces.⁹⁷

3.4. Trust and transparency

The risks and sensitivities around biometrics point to the importance of public understanding and trust. However, building and maintaining this trust first necessitates adequate transparency. A recurring challenge mentioned by policing interviewees was how officers should communicate strategies to the public, particularly given that the 'black-box' nature of many AI systems can make it difficult to understanding how outputs are reached.⁹⁸

⁹² Interview with civil society representative, 6 November 2023.

⁹³ Sadek et al., (2023).

⁹⁴ "Human Rights Act 1998," Legislation.gov.uk, <https://www.legislation.gov.uk/ukpga/1998/42/contents>; Sadek et al., (2023).

⁹⁵ Sadek et al., (2023).

⁹⁶ Ardi Janjeva, Muffy Calder and Marion Oswald, "Privacy Intrusion and National Security in the Age of AI: Assessing proportionality of automated analytics," *CETaS Research Reports* (May 2023).

⁹⁷ Jasserand (2023), 12-19.

⁹⁸ Interview with policing representative, 6 October 2023; Interview with policing representative, 26 October 2023.

In their view, failure to clearly explain the benefits and oversight of these systems with local communities can pose challenges in enabling wider deployment for public safety activities.

Police representatives emphasised that engagement with the public should address the following areas: who is in control of the system, who is defining the boundaries of use and what benefits do these systems provide?⁹⁹ However, it is important to note that these methods primarily focus on *informing* the public and other stakeholders. More is needed to ensure meaningful engagement and accountability, such as collaboration with communities through surveys or focus groups to build buy-in.¹⁰⁰

3.5. Challenges for evaluation

Understanding system performance, for example through accuracy or error rates, is vital to identifying the potential impacts of deployment.¹⁰¹ However, testing strategies employed by developers often differ, making interpretation and comparisons difficult.¹⁰² Testing is also often done in idealised settings, meaning that real-world performance is likely to be worse in practice.¹⁰³ Understanding how performance may vary for different demographic groups is also essential. Efforts to improve evaluation in this respect have improved following work by scholars, advocacy groups and journalists to surface such risks, though many believe more needs to be done. For instance, NIST conducted one specific test which demonstrated how all of the algorithms assessed exhibited 'different levels of biased performances based on gender, race, and age groups'.¹⁰⁴

To understand whether a particular system is appropriate for use, evaluation needs to go beyond system performance measures. One interviewee suggested the need for four stages of evaluation: *technology evaluation*, *scenario evaluation*, *operational evaluation* and *continuous evaluation*, with particular emphasis on the last stage which is not referenced strongly in existing technical standards on biometric system evaluation.¹⁰⁵ Assurance is not only needed that the model in isolation performs as intended, but that the wider outcomes

⁹⁹ Interview with policing representative, 6 October 2023; Interview with policing representative, 26 October 2023.

¹⁰⁰ Ada Lovelace Institute, *Participatory Data Stewardship* (Ada Lovelace Institute: 2021), <https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/>.

¹⁰¹ Interview with industry representative 2, 12 October 2023.

¹⁰² Hitoshi et al., "The future of biometrics technology: from face recognition to related applications," *APSIPA Transactions on Signal and Information Processing* 10, (2021): e9.

¹⁰³ Jansen et al., (2021).

¹⁰⁴ Anil K. Jain, Debayan Deb, and Joshua J. Engelsma, "Biometrics: Trust, but verify," *IEEE Transactions on Biometrics, Behavior, and Identity Science* 4, no. 3 (2021): 303-323.

¹⁰⁵ Interview with industry representative, 29 September 2023.

of the system deployed in context are understood.¹⁰⁶ This includes accounting for how the system is used in practice, how operators act on its outputs and broader societal impacts, such as surveillance risks.

¹⁰⁶ Rosamund Powell and Marion Oswald, "Assurance of Third-Party AI Systems for UK National Security," *CETaS Research Reports* (January 2024), <https://cetas.turing.ac.uk/publications/assurance-third-party-ai-systems-uk-national-security>.

4. Legal Risks and Challenges

This section presents a summary of the current UK regulatory and policy framework governing police and law enforcement use of biometrics, as well as criticisms over gaps or risks that have emerged in recent years.

4.1. Overview and limitations of UK biometrics regulation

Overview of UK biometrics regulation

The UK's current biometrics regulatory framework constitutes several pieces of legislation which stretch back decades. Instead of applying blanket coverage to biometric data or systems, different legal areas seek to govern biometrics in specific ways (see Figure 5). Yet as this section highlights, these various laws have been subject to criticisms over gaps and shortcomings.

Figure 5: Legal areas covering biometrics oversight in the UK



Limitations of UK biometric regulation: common law reliance

There have been several instances in the UK where different organisations unlawfully collected, retained, used or shared biometric data – or failed to apply biometric techniques correctly.¹⁰⁷ These have had serious consequences, including miscarriages of justice (see Table 6). Recent announcements from the UK's senior policing minister on allowing police access to passport photos, alongside running FR searches against 50 million driving licenses, raise questions about the adequacy of measures in place for preventing future data misuse.¹⁰⁸

Failure to keep pace with innovation has been exacerbated by confusion over where the legal boundaries lie with new biometric systems or data types. Despite the sheer amount of existing relevant legislation, many statutes were not enacted at a time when the capture, automated processing, and analysis of biometrics in real time from public spaces was feasible. As a result, legal rulings and other *ad-hoc* developments are being heavily relied upon to inform procedures and provide safeguards.¹⁰⁹

While these developments have since improved practices, there are concerns over whether they can be extended to establish a clear nationwide basis for the long-term use of biometric systems.¹¹⁰ Although UK police forces have a core duty under common law to 'protect the public by detecting and preventing crime', these are broad powers and can sometimes be vague in terms of applying limits.¹¹¹ The *Bridges* judgement (2020) in particular reflected how relying on common law powers did not give a specific legal basis authorising police use of FR systems.¹¹²

¹⁰⁷ It is important to also note a recent non-UK legal ruling (*Glukhin v. Russia*), whereby the European Court of Human Rights ruled that the detaining of a protestor using FR systems following a demonstration violated the protestor's right to freedom of expression.

¹⁰⁸ Tom Singleton, "Police access to passport photos 'risks public trust'," *BBC News*, 4 October 2023, <https://www.bbc.co.uk/news/technology-67004576>; Joel R. McConvey, "UK bill would let police run facial recognition against all driver's licenses," *Biometric Update*, 21 December 2023, <https://www.biometricupdate.com/202312/uk-bill-would-let-police-run-facial-recognition-against-all-drivers-licenses>.

¹⁰⁹ Nóra Ní Loideáin, "Lawfulness and Police Use of Facial Recognition in the UK: Article 8 ECHR and *Bridges v South Wales Police*," in *Facial Recognition in the Modern State*, ed. Rita Matulionyte and Monika Zalnieriute (Cambridge: Cambridge University Press, 2024), 19, <https://ssrn.com/abstract=4413996>.

¹¹⁰ Baroness Hamwee, "House of Lords Justice and Home Affairs Committee letter to the UK Home Secretary," 26 January 2024, <https://committees.parliament.uk/publications/43080/documents/214371/default/>.

¹¹¹ Jennifer Brown, "Police powers: an introduction," House of Commons Library, 21 October 2021, <https://commonslibrary.parliament.uk/research-briefings/cbp-8637/>.

¹¹² Ní Loideáin (2024), 17.

Table 6: Overview of major biometric legal incidents in the UK since the 1990s

Legal incident	Examples	Summary
Miscarriages of justice	<ul style="list-style-type: none"> Stefan Kiszko's incorrect conviction (1992) Andrew Malkinson's incorrect conviction (2004) 	Both individuals were wrongfully imprisoned on the basis of incorrect biometric forensic samples used by the police, with advancements in techniques later acquitting them of committing any crimes. ¹¹³
Court rulings	<ul style="list-style-type: none"> <i>S & Marper v United Kingdom</i> (Grand Chamber) (2008) <i>RMC & FJ v Commissioner of the MPS and Secretary of State for the Home Department</i> (2012) <i>Ed Bridges v South Wales Police</i> (2020) <i>Gaughran v the United Kingdom</i> (2020) 	The UK Courts ruled, in several different legal cases, that the UK Government and policing officials had violated the law in relation to biometrics. This includes infringing on data protection law, as well as human rights law, with the deployment of LFR systems that breached privacy rights. ¹¹⁴
Database violations	<ul style="list-style-type: none"> Suprema (2019) HM Revenue and Customs (2019) Clearview AI (2022) 	Organisations had illegally collected, retained or used the biometric data of UK individuals. ¹¹⁵

¹¹³ Evidence Based Justice Lab; Lauren Hirst and Tom Mullen, "Andrew Malkinson's rape conviction quashed after 20-year fight," *BBC News*, 26 July 2023, <https://www.bbc.co.uk/news/uk-england-manchester-66310919>.

¹¹⁴ "S and Marper v United Kingdom," Equality and Human Rights Commission, 8 June 2016, <https://archive.equalityhumanrights.com/en/legal-casework/s-and-marper-v-united-kingdom>; Rachit Buch, "Police retention of photographs unlawful, High Court rules," UK Human Rights Blog, 27 June 2012, <https://ukhumanrightsblog.com/2012/06/27/police-retention-of-photographs-unlawful-high-court-rules/>; Jenny Rees, "Facial recognition use by South Wales Police ruled unlawful," *BBC News*, 11 August 2020, <https://www.bbc.co.uk/news/uk-wales-53734716>.

¹¹⁵ Josh Taylor, "Major breach found in biometrics system used by banks, UK police and defence firms," *The Guardian*, 14 August 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>; Emily Cox, "UK ICO challenges Clearview AI ruling," Pinsent Masons News, 21 November 2023, <https://www.pinsentmasons.com/en-gb/out-law/news/uk-ico-challenges-clearview-ai-ruling>.

Concern over risk and regulator coverage

Historically, the primary focus of biometrics regulation has been on protecting an individual's personal data and their right to privacy, given the ability to uniquely identify an individual with a high degree of confidence using such data.¹¹⁶ However there are other serious concerns over biometric systems among the public which fall outside of these considerations, such as the consequences for individuals if a system output is incorrect (e.g. wrongful arrest).¹¹⁷

Identification and classification techniques also raise *group*-level risks that may affect multiple individuals. The sensors on technology such as FR can capture data from their surroundings, outside of just the individual who is in primary view, which could therefore include unaware individuals walking past in the background. Moreover, existing equality and human rights laws are primarily focused on protecting the rights of the individual.¹¹⁸ As such, there may be ambiguity over how such legislation might apply for group-based classification systems – for instance a biometric system which categorises individuals into different demographic groups, without necessarily identifying them.

The forthcoming Data Protection and Digital Information Bill is designed to simplify the UK's data protection rules, and includes amendments to the position of the Biometrics and Surveillance Camera Commissioner (BSCC), the only regulator with an explicit remit for biometrics in England and Wales.¹¹⁹ In abolishing the surveillance component of this role, oversight of biometrics is expected to be passed on to the ICO, which has remit over data protection.¹²⁰ However, there are concerns over whether the ICO has sufficient resources and scope to cover the range of potential risks outlined above.¹²¹ The creation of a risk management framework could therefore help to alleviate these anxieties. The regulator does appear to be taking a forward-looking approach to the technology, through planning to use regulatory sandboxes to test innovations.¹²² Such experiments should include a focus on systems that may be used within law enforcement, which could help to pre-empt system risks with innovations that could be promising for public safety activities.

¹¹⁶ Matthew Ryder QC (2022), 21.

¹¹⁷ See survey data in Section 5.

¹¹⁸ CETaS workshop, 22 January 2024.

¹¹⁹ Fussey & Webster (2023), 6-7.

¹²⁰ Biometrics and Surveillance Camera Commissioner (2023).

¹²¹ Fussey & Webster (2023), 50-54.

¹²² "Our current areas of focus for the Regulatory Sandbox," ICO, <https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/our-current-areas-of-focus-for-the-regulatory-sandbox/>.

Ambiguous private sector oversight

Private sector use of biometric systems is growing.¹²³ This trend has heightened concern that biometrics regulation predominantly applies to the public sector. Laws such as the Police and Criminal Evidence Act 1984 (PACE) and the Terrorism Act 2000 only regulate police or border security uses of biometric data. Yet even those broader in scope, like the Equality Act 2010, are only applicable to private organisations in limited circumstances (e.g. those performing public functions).¹²⁴ Risks from this patchy oversight could materialise as some companies explore using biometric systems for tackling crime (e.g. identifying shoplifters).¹²⁵ Given the low confidence in private companies using biometric systems,¹²⁶ much is needed to increase public confidence over safeguards in place.

¹²³ Jawahitha Sarabdeen, “Protection of the rights of the individual when using facial recognition technology,” *Heliyon* 8, no. 3 (March 2022): 1-2, <https://doi.org/10.1016/j.heliyon.2022.e09086>.

¹²⁴ ICO, “Data sharing: a code of practice,” <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/>.

¹²⁵ Josie Hannett and William McLennan, “Shoplifting: The small businesses using facial recognition cameras,” *BBC News*, 11 October 2023, <https://www.bbc.co.uk/news/uk-england-surrey-66982326>. <https://www.bbc.co.uk/news/uk-england-surrey-66982326>

¹²⁶ See survey data in Section 5.

4.2. Overview and limitations of UK biometrics policy

Overview of UK biometrics policy

Policy acts as an additional layer to legislation in providing guidance for decision-making. Figure 6 provides an overview of relevant policy areas, while the rest of this section highlights corresponding gaps and limitations.

Figure 6: Policy areas covering biometrics in the UK



Limitations of UK biometrics policy: patchy codes of practice

The most prominent component of biometrics policy relates to codes of practice. These act as a set of either voluntary or legally enforceable guidelines that set minimum standards and promote compliance with the law. Codes can cover everything from the appropriate deployment of biometric systems to the correct processing and handling of biometric data. However, there are concerns that current codes are both outdated and insufficient. Existing codes focus almost exclusively on legal compliance when handling certain data types, like DNA and fingerprints.¹²⁷

Policing and law enforcement are increasingly using FR technology that captures and stores facial images, while voice recognition is considered an area of future interest.¹²⁸ The lack of

¹²⁷ Surveillance Camera Commissioner's Office, "What we talk about when we talk about biometrics...", Surveillance Camera Commissioner's Office Blog, 12 October 2021, <https://videosurveillance.blog.gov.uk/2021/10/12/what-we-talk-about-when-we-talk-about-biometrics/>; Pete Fussey and William Webster, *Independent report on changes to the functions of the Biometrics and Surveillance Camera Commissioner arising from the Data Protection and Digital Information (No. 2) Bill* (CRISP: October 2023), 9,

https://assets.publishing.service.gov.uk/media/653f7128e6c968000daa9cae/Changes_to_the_functions_of_the_BSCC.pdf.

¹²⁸ Interview with academic representative, 25 September 2023; Interview with government representative, 24 October 2023.

tailored safeguards over these materials risks legal ambiguity which could be exploited.¹²⁹ While some recent codes have been important in filling gaps in primary legislation, such as the College of Policing's APP on LFR use by UK police forces, they are equally limited in that they do not address other forms of FR (e.g. retrospective use). A new APP on retrospective FR would therefore be beneficial for legal clarity.¹³⁰

Sociotechnical considerations in system evaluation standards

A number of international standards bodies publish best practices on biometric system specifications and quality management. This includes ISO/IEC JTC 1/SC 27 and 37, BSI's IST/44 and CEN-CENELEC's CEN/TC 224. Topics covered by these groups include standards on evaluation (e.g. ISO/IEC 19795-1:2021) which provide useful information on error rates, throughput rates and reducing bias.¹³¹ Nevertheless, there is lack of wider sociotechnical considerations in existing standards, which are important for biometric systems given the degree of sensitive data involved.¹³² As such, relevant working groups within standards bodies, such as BSI's IST/44, should explore updating current standards on testing and evaluation. This could incorporate potential consequences of system deployments on surveillance concerns and 'chilling' effects in public spaces, alongside the role of human error in potentially undermining the reliability of outputs (e.g. through the poor placement of sensors).

Public-private partnerships

Participants raised several concerns regarding current legal frameworks for public sector acquisition and use of commercial biometric systems.¹³³ In comparison to the stringent accountability mechanisms placed on UK police and law enforcement agencies, the lack of comparative checks in the private sector means that there can be less transparency on system data and testing when sourced through industry.¹³⁴

In response to an FOI request submitted for this study, the Home Office stated that 'the decision to purchase a biometric system on a trial basis is for each police force to take

¹²⁹ Matthew Ryder QC (2022), 52.

¹³⁰ College of Policing, *Authorised Professional Practice: Live facial recognition* (College of Policing: March 2021), 6, <https://assets.college.police.uk/s3fs-public/2021-05/live-facial-recognition-app.pdf>.

¹³¹ "ISO/IEC 19795-1:2021," ISO, May 2021, <https://www.iso.org/standard/73515.html>.

¹³² Interview with academic representative, 28 September 2023; Interview with industry representative, 29 September 2023.

¹³³ Interview with policing representative, 6 October 2023; Interview with academic representative, 6 October 2023; Interview with policing representative, 11 October 2023.

¹³⁴ Interview with policing representative, 6 October 2023.

locally'.¹³⁵ While such local decision-making enables regional context to be taken into account, insufficient national oversight can lead to duplication of effort and a patchwork of safeguards and oversight mechanisms. With Essex Police recently announcing trials of LFR with equipment supplied by SWP, there remain questions over where accountability lies for the use of the system.¹³⁶ One option is the creation of a nationwide registry of new biometric systems in policing, which would help to keep track of deployments and improve public transparency. Another option is the development of policing guidance that would streamline requirements applied during any transfers of technology between forces, as well as with procurements from the private sector.

¹³⁵ Freedom of information request submitted to the Home Office by CETaS on 24 November 2023.

¹³⁶ "Live facial recognition," Essex Police, <https://www.essex.police.uk/police-forces/essex-police/areas/essex-police/au/about-us/live-facial-recognition/>.

5. Public Attitudes to Biometrics

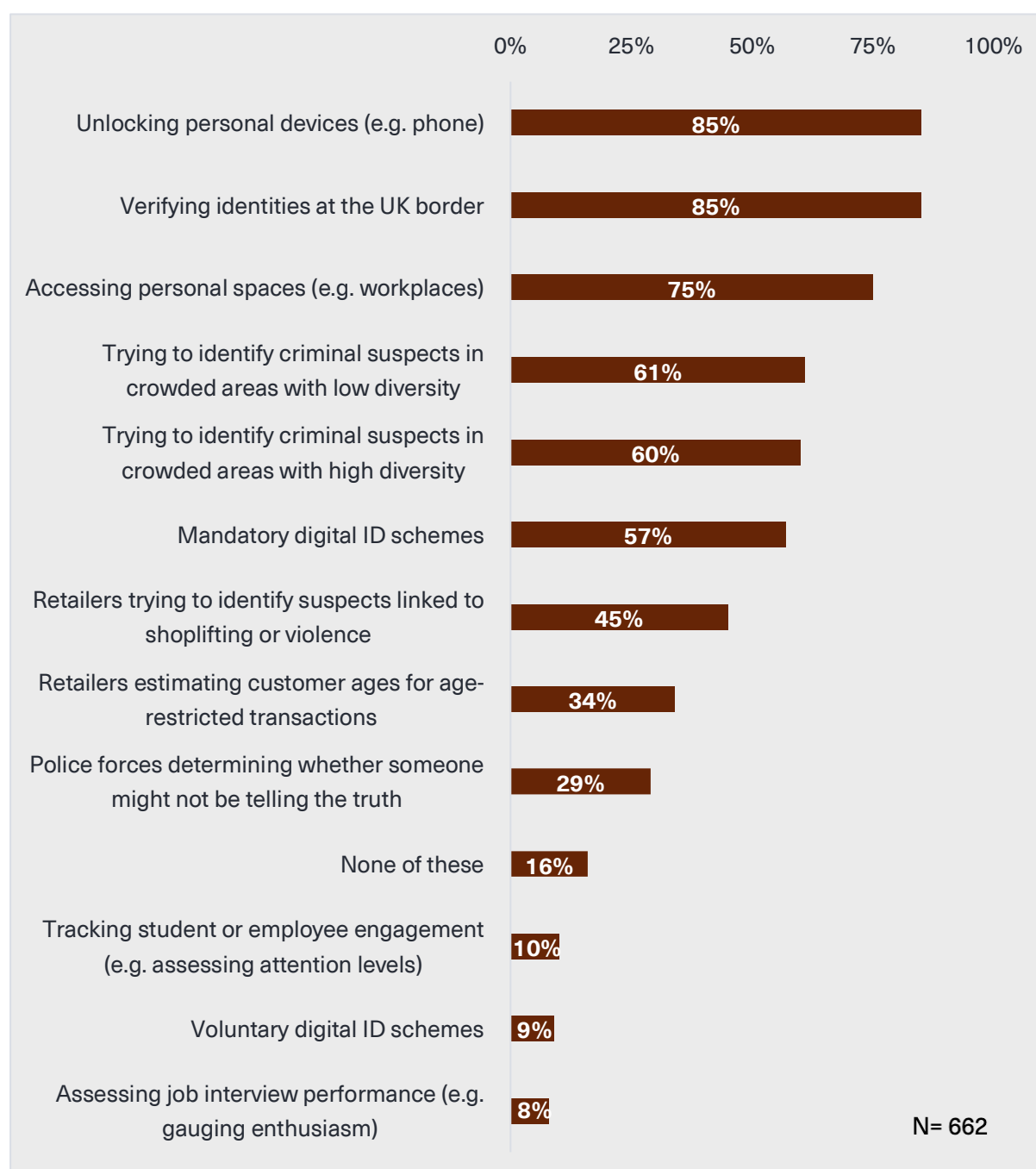
This section presents the findings of the CETaS survey, which involved a nationally-representative sample of 662 UK-based respondents. As a nationally-representative sample, we acknowledge that the sample is skewed towards demographic majority groups and may not therefore account for the specific concerns held by minority demographics. ‘Not sure’ or ‘prefer not to say’ responses have been excluded from the data visualisations in this section given the focus on key findings, which means that some of the total percentage counts do not add up to 100%. Additional information on methodology and the full survey results can be found in Appendix 1.

5.1 Comfort and trust vary by application and organisation

Respondents demonstrated a nuanced view of biometric technologies, with expressed levels of comfort varying significantly depending on the application (see Figure 7). For most policing and law enforcement applications, the majority of respondents feel comfortable with such use; namely using biometrics to verify identities at the UK border (85%) or trying to identify criminal suspects in crowded areas with low or high diversity (61% and 60% respectively) (see Figure 7). The exception was the use of biometric data to determine whether someone might not be telling the truth, for which only 29% selected that they felt comfortable. This finding correlates with a similar survey conducted by the Ada Lovelace Institute, which found FR technology applications that were used by the police for criminal investigations received much stronger support than other use cases.¹³⁷

¹³⁷ Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology* (Ada Lovelace Institute: September 2019), 8, https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf.

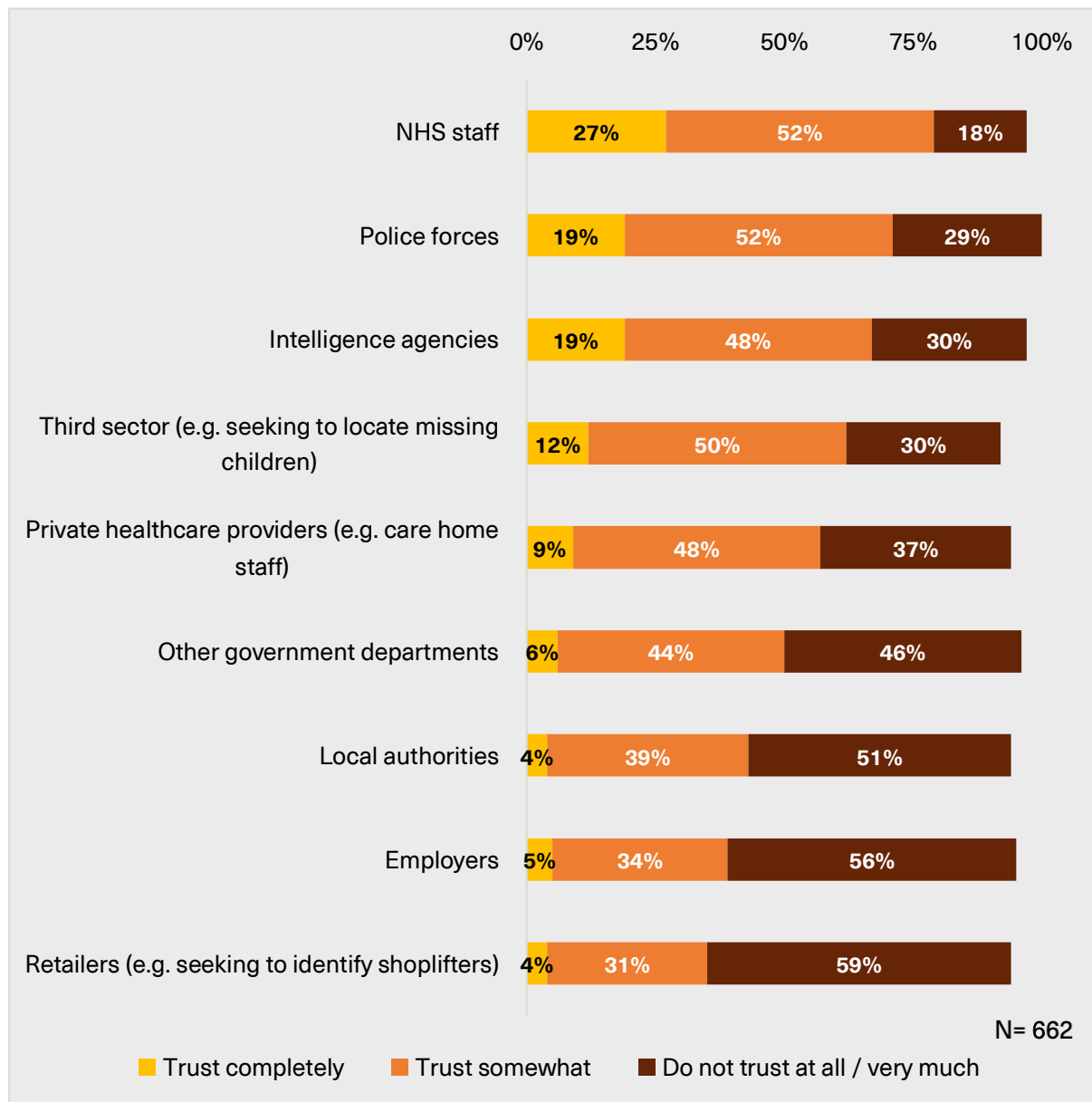
Figure 7: Percentage of participants who selected that they feel 'comfortable' with the given application



When it came to trust in organisations, respondents reported higher levels for public sector organisations such as police forces (79%) and the NHS (66%), but much lower for commercial entities – particularly employers (42%) and retailers (38%). This graph combines the average percentages from two separate survey questions on trust.¹³⁸

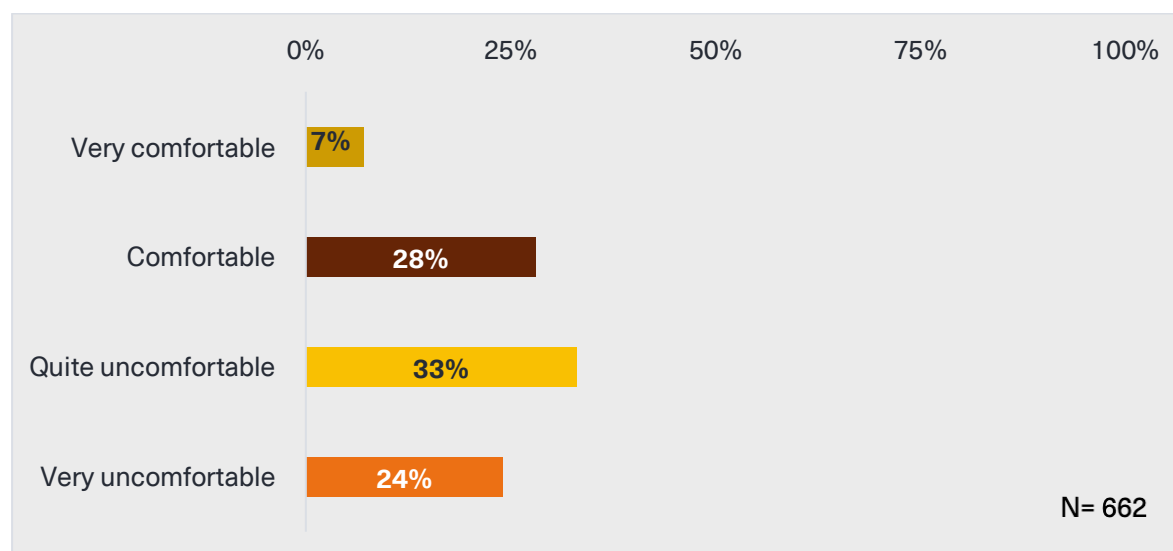
¹³⁸ For detailed survey results, please see Appendix 1.

Figure 8: Percentage of participants who selected whether they 'trust completely', 'trust somewhat' or 'do not trust at all / very much' different organisations to use biometric systems responsibly



When asked whether participants were comfortable with biometric data sharing schemes between police forces and the private sector for public safety activities, **the majority of respondents were 'quite' or 'very' uncomfortable with this type of data sharing process (57%).**

Figure 9: Percentage of participants who selected whether they were 'very comfortable', 'comfortable', 'quite uncomfortable' or 'very uncomfortable' in biometric data sharing between the police and private entities

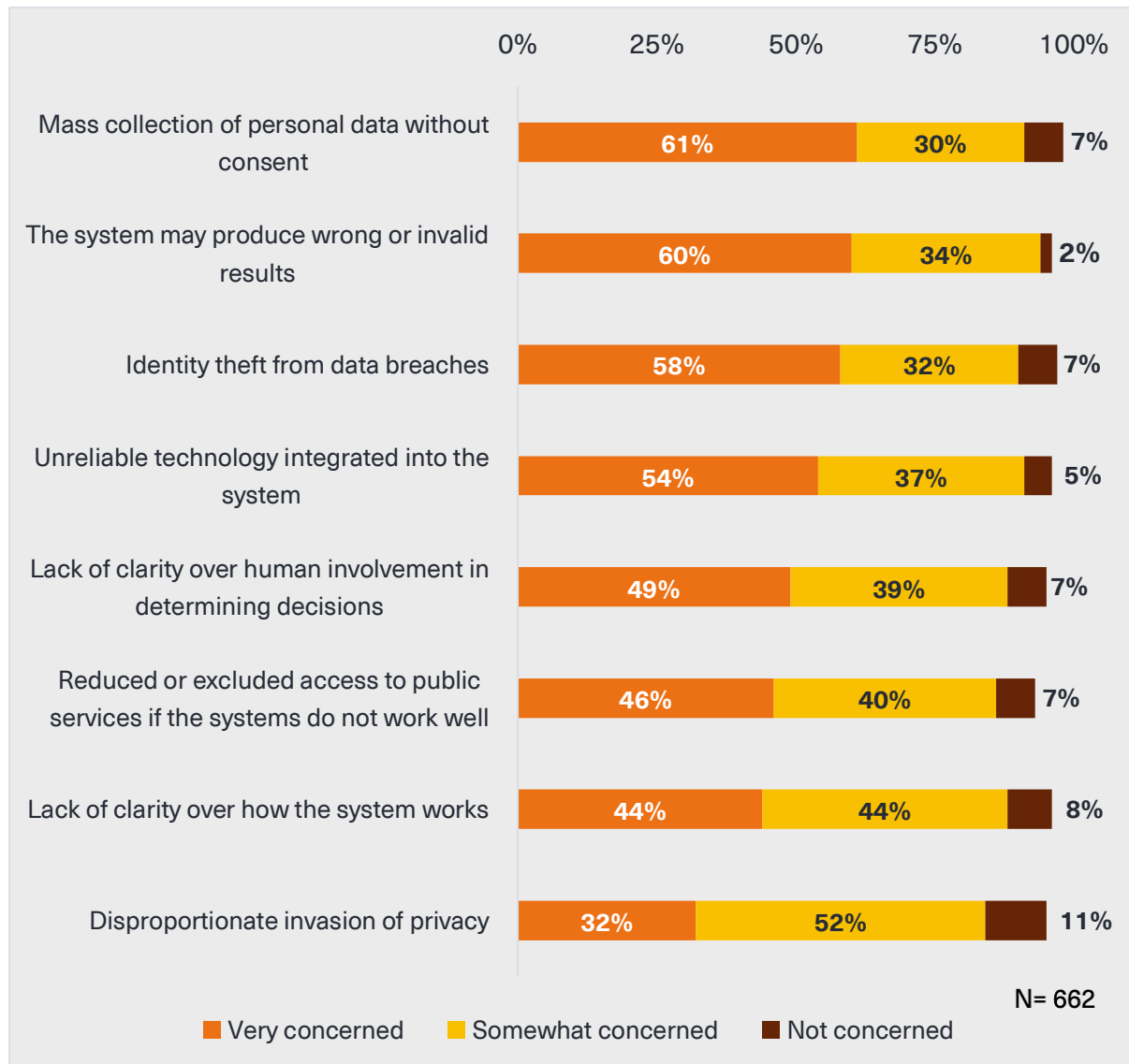


Responses to this question **differed by region**, with respondents from **Scotland (28% “comfortable” or “very comfortable”)** and **Northern Ireland (11%) being less comfortable** with data being shared between the police and the private sector **than those in England (36%) and Wales (48%)**. While this may be due to a number of contextual factors affecting trust in police more generally, these findings highlight that public attitudes to biometrics vary between the nations, which should not be overlooked when designing new policies.

5.2 High levels of concern shown for a wide range of risks

Participants were asked how concerned they were about eight wide-ranging risks from biometric systems, such as privacy intrusion or unreliable systems. For all risks, at least 84% of participants selected that they were 'somewhat concerned' or 'very concerned' (see Figure 10). Those with the highest rates for 'very concerned' were as follows: risks around **mass collection of personal data without consent (61%)**, potential **mistakes or invalid results being made by biometric systems (60%)** and **identity theft from data breaches (58%)**.

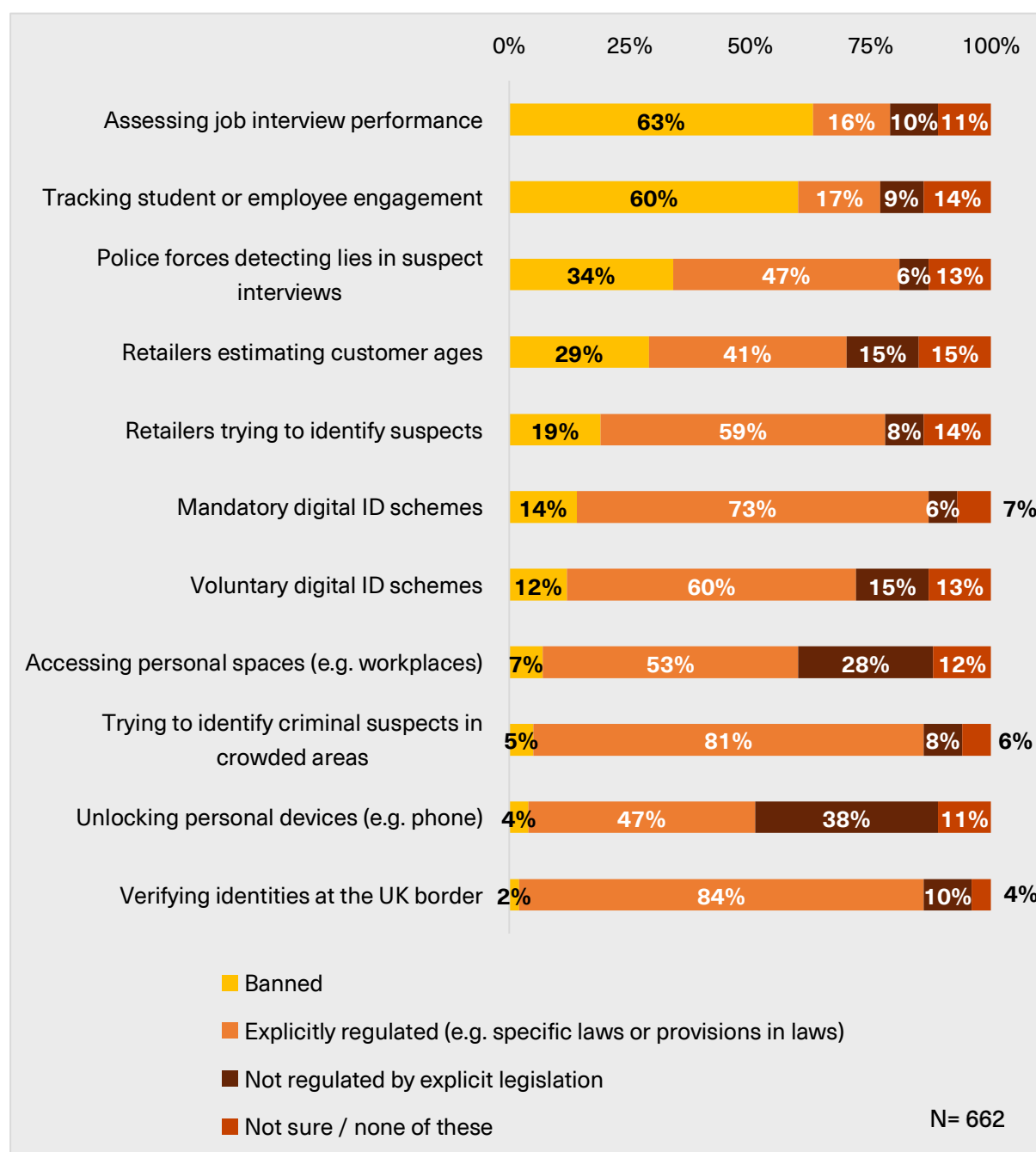
Figure 10: Percentage of participants who selected whether they were 'very concerned', 'somewhat concerned' or 'not concerned' with different risks from biometric systems



5.3 A strong desire for explicit regulation and bans on certain use cases

Respondents were asked whether certain biometric applications should be unregulated, explicitly regulated, or banned. For every application, the majority responded that the use case should be explicitly regulated or banned. In terms of outright bans, the majority of respondents reported that the use of **novel biometric systems** in job interviews to assess performance (63%) and tracking student or employee engagement (60%) **should be banned**.

Figure 11: Percentage of participants who selected whether they wanted different biometric use cases to be 'banned', 'explicitly regulated (e.g. specific laws or provisions in laws)' or 'not regulated by explicit legislation'

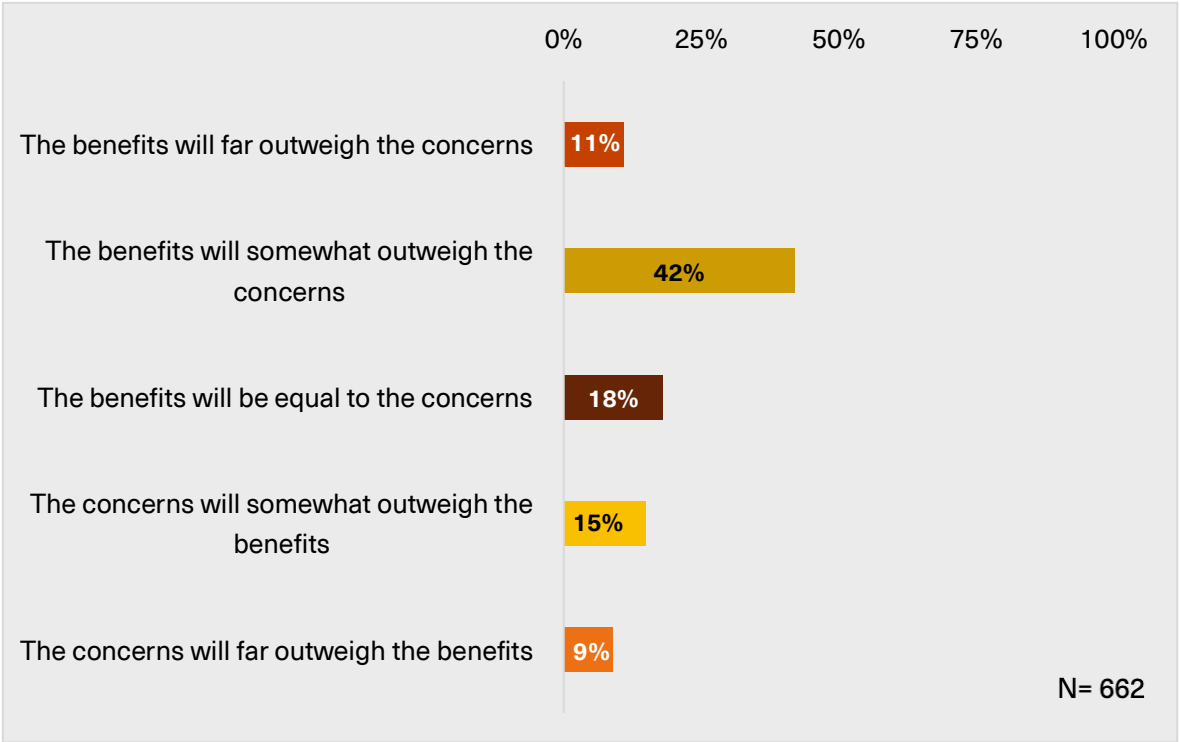


5.4 Most people perceive benefits will outweigh concerns

Finally, when considering how biometric systems will impact society in the future, a **slight majority of respondents (53%)** reported that the **benefits of biometrics will outweigh the**

concerns (either greatly or marginally), whereas **24% thought that the concerns outweighed the benefits** (either greatly or marginally).

Figure 12: Percentage of participants who selected whether the benefits of biometric systems either 'far outweigh', 'somewhat outweigh' or will be 'equal to' the concerns, or if the concerns 'far outweigh' or 'somewhat outweigh' the benefits



6. Alternative Policy and Regulatory Options

As demonstrated in Section 2, there will be ample opportunity to integrate emerging biometrics in policing and law enforcement. Section 5 also showed that the general public are comfortable with certain public safety applications of biometric systems when adequately regulated. This section now explores the most recent piece of non-UK legislation on biometrics drafted by the EU, as well as drawing on insights from relevant experts, to identify future options which could improve biometric governance and oversight in the UK.

6.1. Insights from the EU AI Act

In contrast to the UK and other countries which aim to regulate biometrics through broad data protection principles, the EU has taken a different route with its draft AI Act legislation – targeting the use of the *technology* through a risk-based approach.¹³⁹ Although the definition of ‘biometric data’ remains consistent, the AI Act seeks to address concerns previously outlined over restricting biometrics to uses involving unique identification. It does this by outlining a series of system types which are constrained to certain applications and organisations – or banned outright – based on the level of risk they pose to human rights. Table 7 highlights the main biometric systems which fall under the risk categories, which include novel categorisation (e.g. classification) and emotion recognition (e.g. inferential) models.¹⁴⁰

A benefit of the EU’s approach is that it incorporates a mechanism in the draft legislation (Annex III) where the list of use cases placed in different risk categories can be amended. This adds flexibility to the law, enabling it to keep pace with new technical developments which could pose a risk of harm to human rights.¹⁴¹ Moving forward, any future UK legislation should ensure that a similar mechanism is included, which will help to prevent legal frameworks from becoming overtaken by innovation.

¹³⁹ At the time of writing, the text of the EU AI Act was still in draft phase and as such, some of this analysis may not reflect the final legislation.

¹⁴⁰ AI-Regulation.com, “Tools for Navigating the EU AI Act: (1) Final Text with Interactive Table of Contents,” *AI-Regulation Papers* (February 2024), 92-94 and 229-232, <https://ai-regulation.com/wp-content/uploads/2024/02/AI-Act-ToC.pdf>.

¹⁴¹ Katerina Demetrou, “Introduction to the Conformity Assessment under the draft EU AI Act, and how it compares to DPIAs,” Future of Privacy Forum Blog, 12 August 2022, <https://fpf.org/blog/introduction-to-the-conformity-assessment-under-the-draft-eu-ai-act-and-how-it-compares-to-dpias>.

Table 7: EU AI Act proposed regulation of different biometric systems and use cases

Risk category	Biometric systems / use cases
Unacceptable risk	<ul style="list-style-type: none">• Categorisation based on biometric data to infer personal characteristics (e.g. race or sexual orientation)• Untargeted scraping of the Internet or CCTV for facial images to build up or expand databases• Emotion recognition systems in the workplace and education institutions• Real-time remote biometric identification in public spaces (subject to the below exceptions)
High-risk	<ul style="list-style-type: none">• Remote biometric identification in public spaces by law enforcement for specific purposes (e.g. prevention of a terrorist threat)• Polygraphs and emotion recognition systems with a law enforcement application• Labelling or filtering acquired biometric datasets, such as images, based on biometric data or categorising of biometric data for law enforcement purposes

6.2. Improving biometric governance and oversight

This sub-section summarises potential new regulatory measures for biometrics governance, drawing on interview data and findings from a ‘stress-testing’ policy workshop with 12 senior officials from police forces, law enforcement agencies and regulators.

Research participants were divided on whether new primary legislation should be introduced. Some argued that the various risks emanating from existing laws in place, and the current reliance on codes of practice, demonstrate that new legislation would likely still be inadequate moving forward.¹⁴² There was also recognition that codes of practice can potentially be introduced or updated far quicker than new legislation or legislative

¹⁴² CETaS workshop, 22 January 2024.

amendments. As such, while views varied among participants, **the research has concluded that future regulatory measures should include both updating existing biometrics legislation, and developing new codes of practice for specific policing and law enforcement use cases.** Such measures should address the **risks, harms and purpose** of specific biometric use cases to inform the appropriate level of regulation and avoid undermining the potential benefits that the technology could provide.

A systems-based focus is also needed to distinguish between applications involving existing, established biometric systems (e.g. for verification), and emerging and potentially untested use cases involving classification and inferential systems. Any new regulation or codes must also **apply consistent standards between different sector use cases for public safety**, given the legal ambiguity over commercial entities deploying biometric systems for tackling crime. There was also consensus that **mandatory system auditing and testing requirements** should be explicitly established in future regulation by an **independent body**, which could improve public confidence in the robustness of biometric systems.

Finally, the research identified several priorities for follow-on research, including:

- 1) A large-scale representative survey of minority groups in the UK to understand the specific attitudes of these groups towards biometric systems for policing and law enforcement;
- 2) Legal analysis of the use of the polygraph in the UK criminal justice system, as well as technical standards and scientific testing requirements;
- 3) Exploring specific risks and opportunities arising from the use of emerging biometric technologies within the UK intelligence community;
- 4) Insights from the wider UK law enforcement community (e.g. the UK Border Force and the National Crime Agency) on emerging biometric technologies;
- 5) Technical research on mitigating spoofing attacks against biometric systems and improving veracity (e.g. 'liveness') checks to confirm the presence of human users.

About the Authors

Samuel Stockwell is a Research Associate at the Centre for Emerging Technology and Security (CETaS). His research interests focus on the intersection between national security and the online domain, particularly in relation to countering radicalisation and violent extremism through both policy and technical solutions. Prior to joining the Turing, Sam worked on a wide portfolio of defence and security research at RAND – spanning military workforce issues, human security concerns, UK defence strategy and emerging technologies. He also led several projects using futures and foresight methodologies, such as horizon scanning for new S&T developments that may impact the UK Ministry of Defence, as well as scenario analysis of novel hybrid threats for the UK's Defence Science and Technology Laboratory (Dstl).

Megan Hughes is a Research Associate at CETaS. Prior to joining the Turing, Megan worked as an Analyst within the Defence and Security research group at RAND Europe. She led projects on a wide range of topics from assessing the impact of emerging technologies on the information environment to identifying the implications of disinformation and conspiracy theories in Europe. Her research has informed strategy and policy at the UK Home Office, UK Ministry of Defence, the European Commission, and the United Nations Development Programme.

Carolyn Ashurst is a Senior Research Associate in Safe and Ethical AI at the Alan Turing Institute. Her work is motivated by the question: How do we ensure AI and other digital technologies are researched, developed and used responsibly? Her research into algorithmic fairness seeks to understand the fairness implications of data-driven systems from theoretical, practical and domain-specific lenses. As well as mitigating the impacts from deployed systems, her work in responsible research seeks to understand the role of the machine learning (ML) research community in navigating the broader impacts of ML research.

Dr Nóra Ní Loideáin is Assistant Professor in Law and Director of the Information Law & Policy Centre at the University of London's Institute of Advanced Legal Studies. Her research focuses on EU law, European human rights law, and emerging technologies, particularly within the contexts of privacy and data protection, criminal justice, and national security. In 2019, she was appointed to the UK Home Office Biometrics and Forensics Ethics Group (BFEG) which provides independent advice ensuring the robustness of evidence underpinning biometrics and forensics policy development for public security within the Home Office.

Appendix 1. CETaS Public Opinion Survey

This Appendix details the rationale, methodology and results of the public survey component of the project.

A.1. Survey methodology

Rationale

The project team identified a gap in existing survey data around public understanding of biometrics, and attitudes towards different types of biometric systems and use cases. While some organisations have conducted important public perceptions work looking more specifically at facial recognition (FR) systems, they are both somewhat outdated and there remains a lack of data on the wider technology ecosystem as new systems and applications emerge.¹⁴³

Sample

Within this context, CETaS launched a public survey with a nationally-representative sample of 662 UK respondents aged 18 or over. The sample was recruited by Prolific, an online research platform that provides recruitment and management of survey participants.¹⁴⁴ 36,699 out of a total of 144,469 Prolific participants were eligible to take part in the survey. Prior to going live, a pilot was also conducted with 12 members of the public drawn from Prolific to inform survey timings – though their responses were not included in the final survey results. All 662 respondents completed their survey online, via a computer, mobile or tablet device. Since a nationally-representative sample was used, the data was left unweighted. Table 8 below provides an overview of the demographic data, which comprised categories including ethnicity and gender options based on Office for National Statistics labels.¹⁴⁵

¹⁴³ For examples, see: Ada Lovelace Institute (2019); London Policing Ethics Panel, *Final report on Live Facial Recognition*, May 2019,

http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf.

¹⁴⁴ "About us," Prolific, <https://www.prolific.com/about>.

¹⁴⁵ "Ethnic group, national identity and religion," Office for National Statistics, <https://www.ons.gov.uk/methodology/classificationsandstandards/measuringequality/ethnicgroupnationalidentityandreligion>; "Gender identity, England and Wales: Census 2021," Office for National Statistics, <https://www.ons.gov.uk/peoplepopulationandcommunity/culturalidentity/genderidentity/bulletins/genderidentityenglandandwales/census2021>.

Table 8: Survey demographic data

Demographic category		Total number	Percentage of sample
Age group	18-25 years	84	13%
	26-30 years	69	10%
	31-40 years	123	19%
	41-50 years	107	16%
	50+ years	277	42%
	Prefer not to say	2	0.3%
Gender	Female	331	50%
	Male	320	48%
	Non-binary	6	0.9%
	Trans man	1	0.2%
	Trans woman	1	0.2%
	Prefer to self-describe	1	0.2%
	Prefer not to say	2	0.3%
	England	567	86%

Country of residence	Northern Ireland	18	3%
	Scotland	50	8%
	Wales	25	4%
	Prefer not to say	2	0.3%
Ethnicity	Asian or Asian British	49	7%
	Black, African, Caribbean, or Black British	18	3%
	White	574	87%
	Mixed or multiple ethnic group	12	2%
	Other ethnic group	3	0.5%
	Prefer not to say	6	0.9%

Survey questionnaire

The survey was created on the Qualtrics survey platform, in consultation with subject matter experts within The Alan Turing Institute. Respondents were informed that the survey questions would focus on gathering data around public awareness of, and attitudes towards, biometric systems. The following definition of biometric systems was provided, based on early study findings:

'Biometric systems collect and process physiological data (measurements of physical characteristics, such as fingerprints or facial measurements) or behavioural data (how a person moves or acts, such as facial expressions or voice measurements). This data can be used to identify an individual, verify their identity, categorise them into different groups, or make inferences about their psychological or emotional states.'

The survey was divided into five sections, consisting of 24 questions. The project team deliberately avoided providing content or analysis to survey respondents, such as existing biometric regulations, legal gaps or the technical threat landscape, prior to the survey being completed. This was due to the primary aim of the survey being to understand *pre-existing* awareness and attitudes towards these technologies. The first section explored general awareness of biometrics and the type of data that biometric systems collect. Respondents were then asked about their knowledge of different biometric systems, before being invited to report their comfort levels with different potential biometric use cases and the risks related to these applications that they felt were most concerning. The penultimate section covered levels of trust towards different organisations using biometric systems, while the final section involved questions about future governance options, regulatory preferences for the use cases previously listed and optimism about the benefits of biometric systems in society.

To ensure that the duration of the survey was constrained to an average range of 15-20 minutes, close-ended questions were primarily used (13 in total), where respondents were asked to choose from a list of predetermined answers that best reflected their views. However, optional free text comments were permitted for 11 questions to collect insights on justifications behind answers. Survey analysis was conducted using Microsoft Excel via data collected in Qualtrics.

A.2. Quantitative survey results

The following tables and graphs present quantitative results from the multiple-choice survey questions.

Awareness of biometrics

Q1. Before today, please indicate how familiar you were with the concept of ‘biometric systems’ described at the start of this survey using the scale points shown below.

Very familiar	13%
Somewhat familiar	63%
Not very familiar	18%

Not familiar at all	6%
Not sure	0.3%

N = 662

Q2. Before today, were you aware of the existence of biometric systems that collect physiological data (e.g. measurements of physical characteristics, such as fingerprints or facial measurements)?

Yes	91%
No	3%
Not sure	6%

N = 662

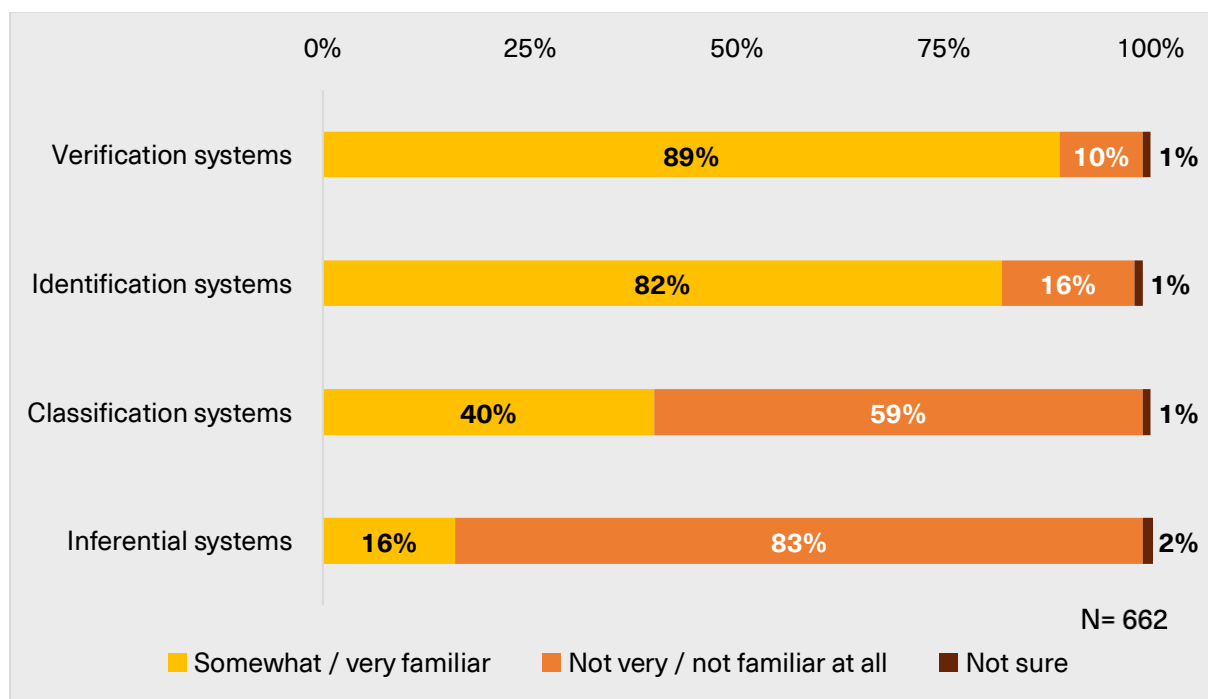
Q3. Before today, were you aware of the existence of biometric systems that collect behavioural data (e.g. how a person moves or acts, such as facial expressions or voice measurements)?

Yes	49%
No	35%
Not sure	16%

N = 662

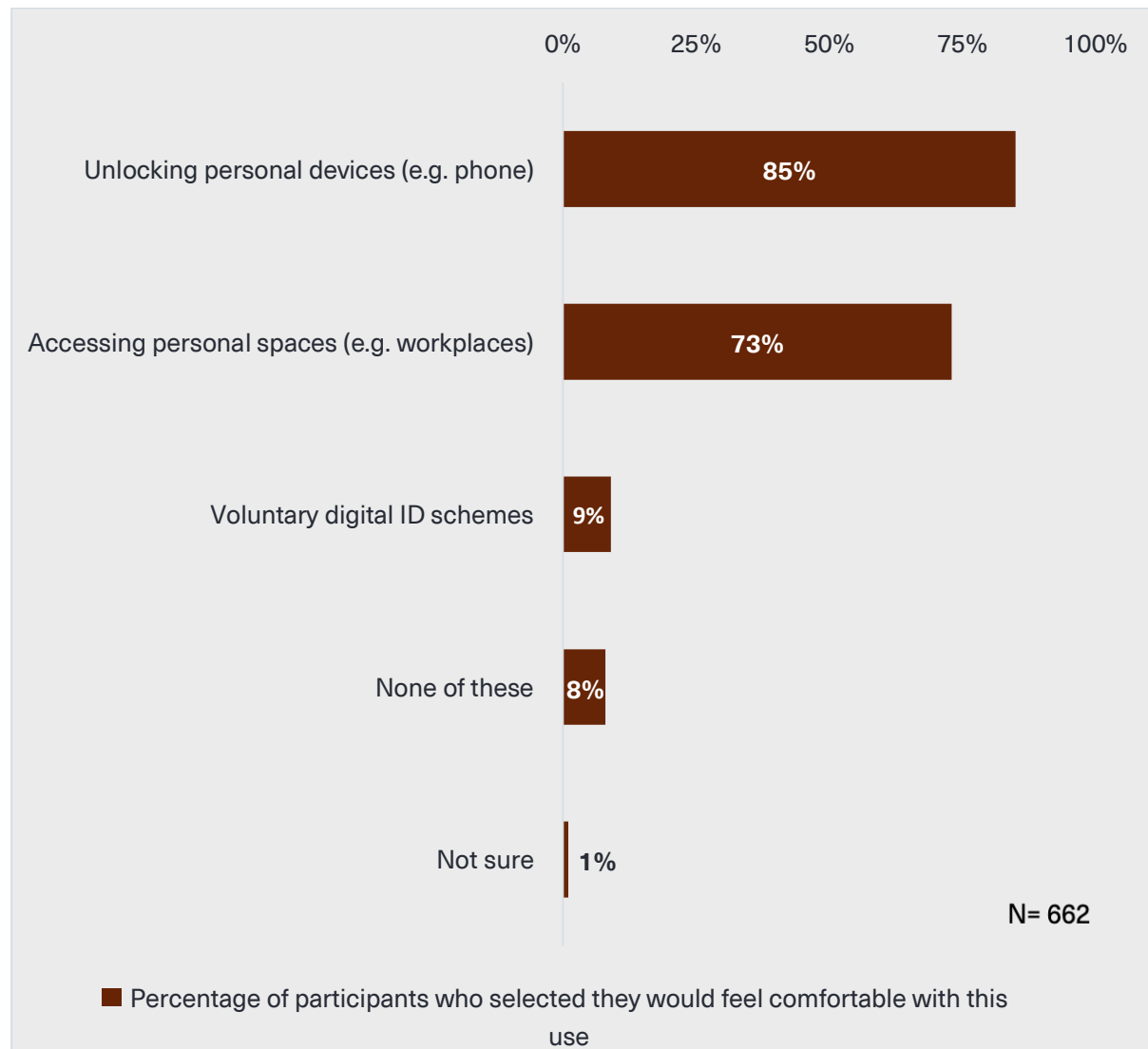
Q4. Before today, how familiar were you with the following different types of biometrics systems:

1. **Identification systems:** seek to recognise an individual by comparing someone's biometric data against all existing profiles on a database. For example, identifying an individual in video footage from a database containing images of known people.
2. **Verification systems:** seek to confirm the identity of an individual presenting themselves as a specific person. These systems check the individual's biometric data against one existing profile on a database. For example, verifying that an individual's face matches the one on the passport database when they present it at an airport.
3. **Classification systems:** seek to classify an individual against a specific category based on biometric data collected from them and compared with features on large databases. For example, estimating someone's age group, gender, ethnicity or race based on their facial scan which is compared against a large number of people whose age group, gender, ethnicity or race is known.
4. **Inferential systems:** seek to infer an individual's emotions or behaviour based on biometric data. For example, predicting whether an individual is alert or tired based on their facial movements compared against a database of facial movements of people whose emotions or behaviour are known.

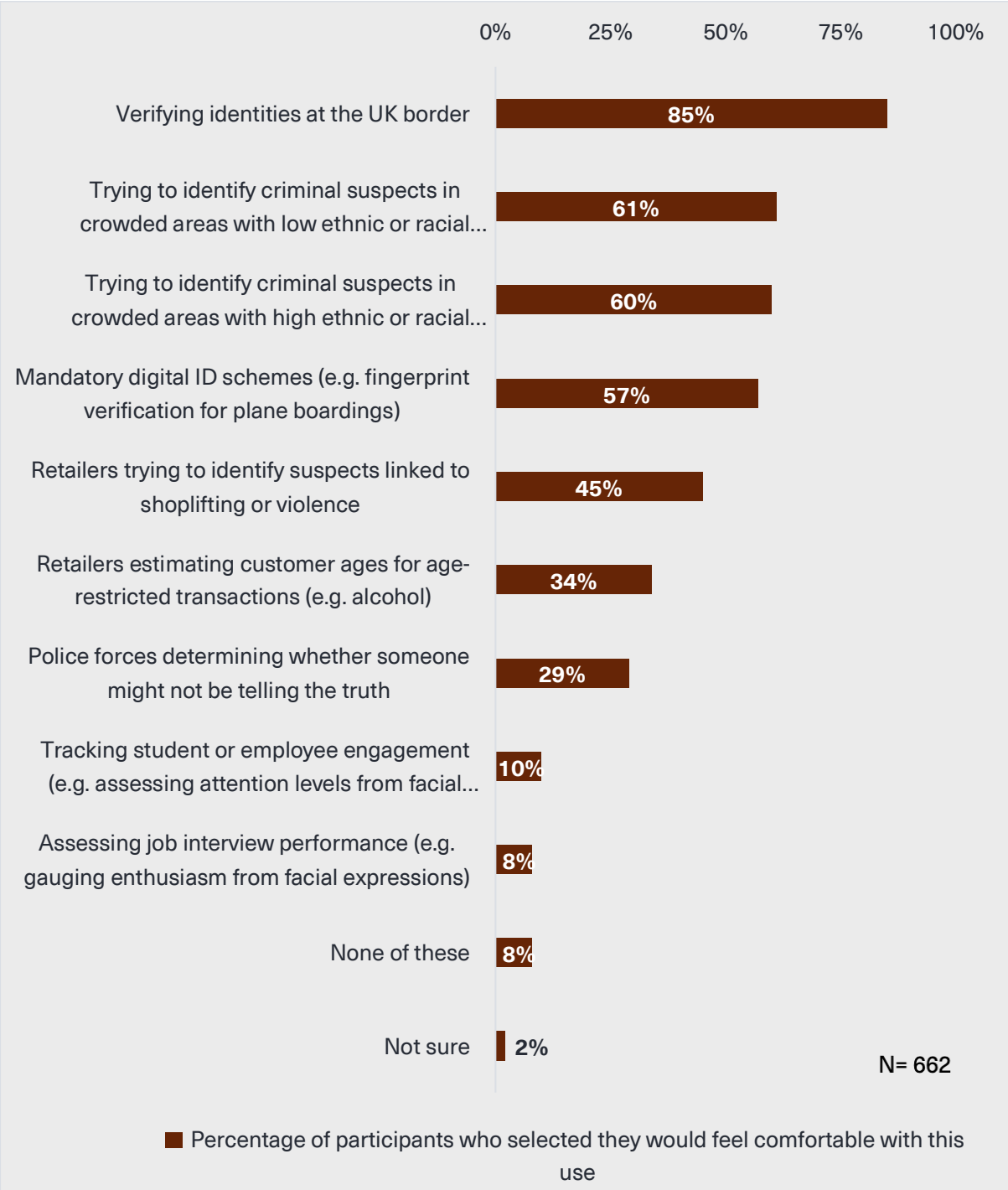


Attitudes towards different biometric applications and risks

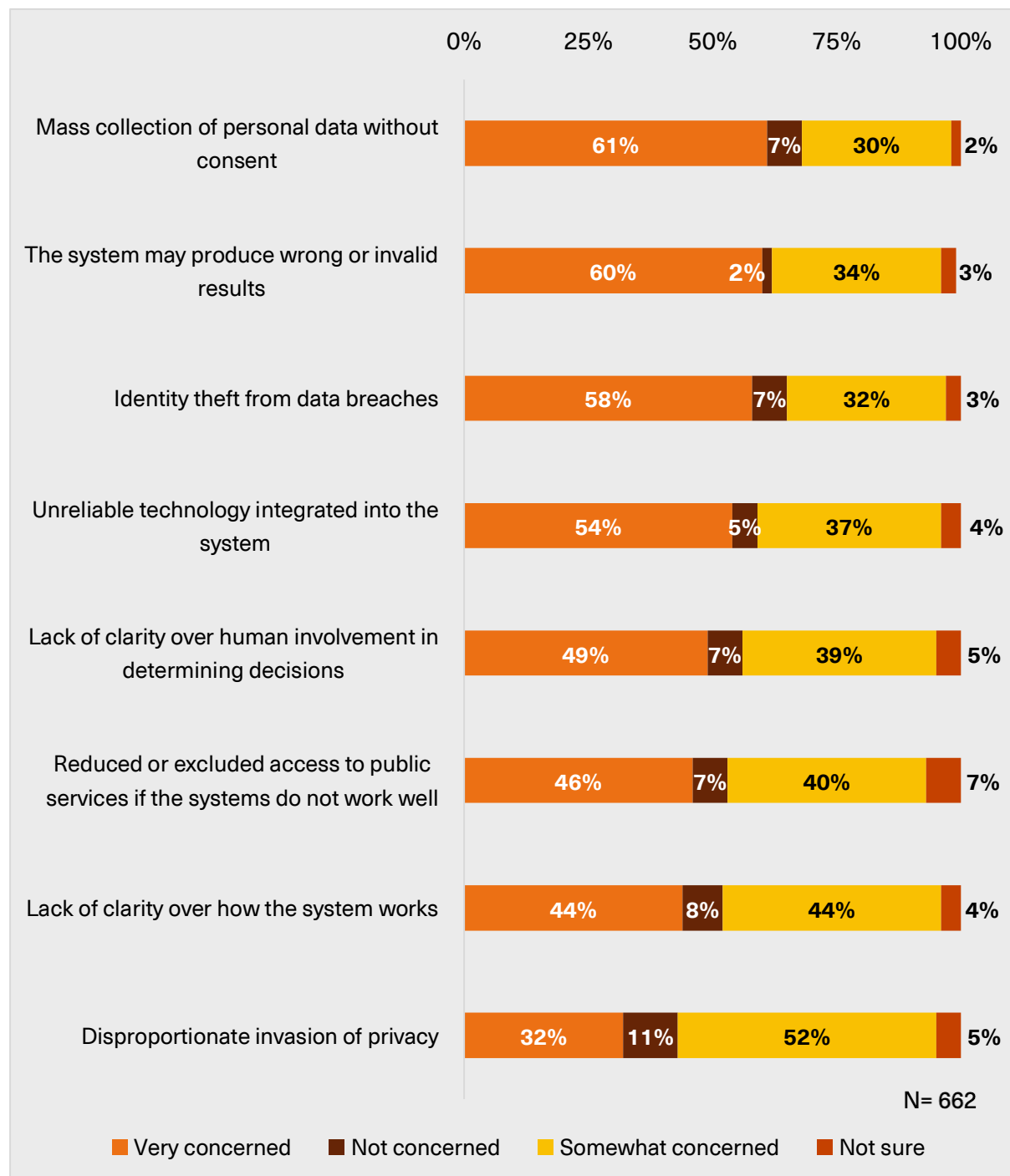
Q5. Please select all (if any) of the following applications where you would feel comfortable with the use of biometric systems. These are examples where the biometric system requires someone's active involvement and awareness.



Q6. Please select all (if any) of the following applications where you would feel comfortable with the use of biometric systems. These are examples where someone is having the biometric system applied to them without necessarily requiring their active involvement or awareness.

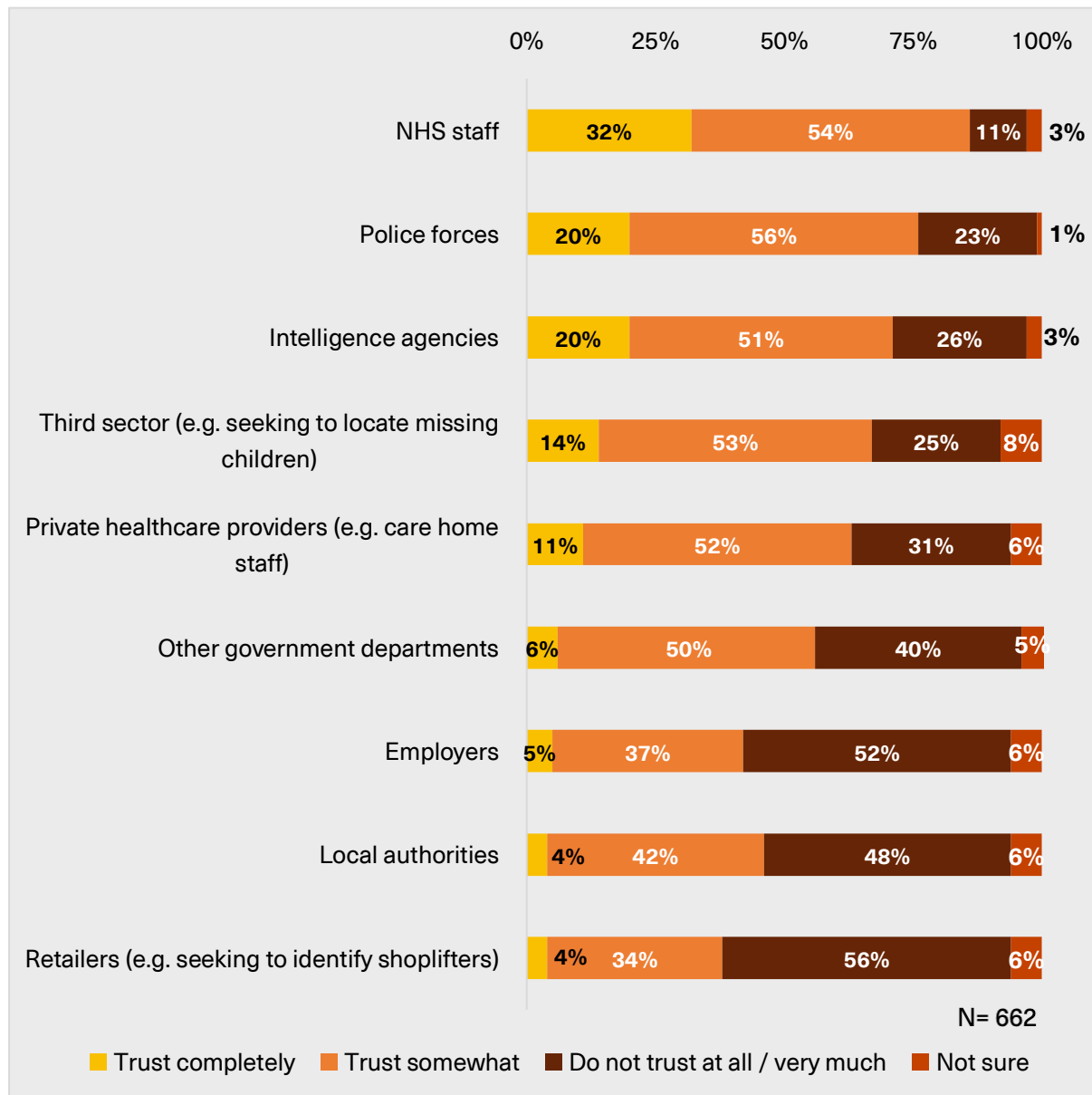


Q7. Please select how concerned you feel about the following list of potential risks from the use of biometric systems in different everyday activities.

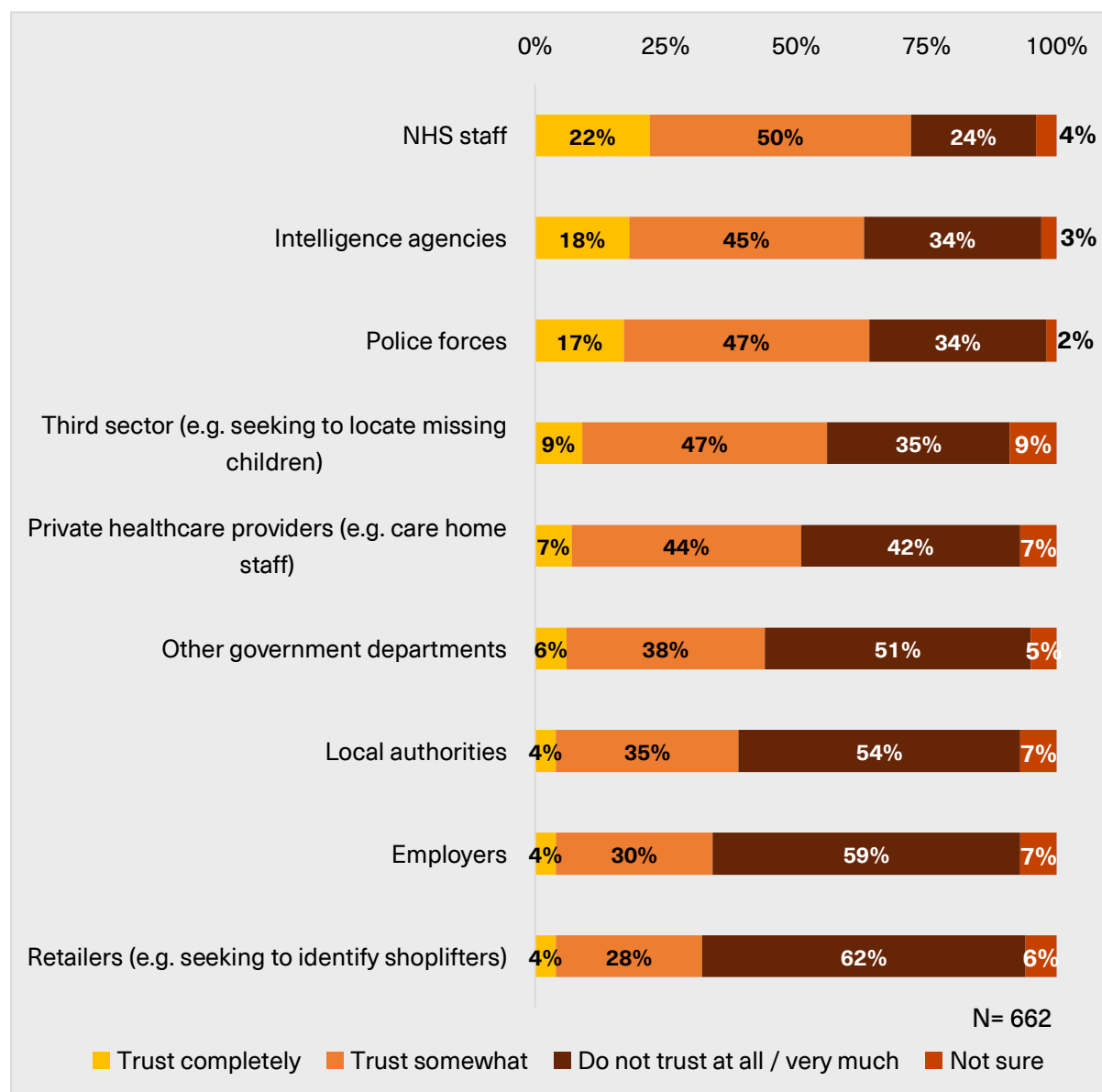


Trust in different actors using biometric systems

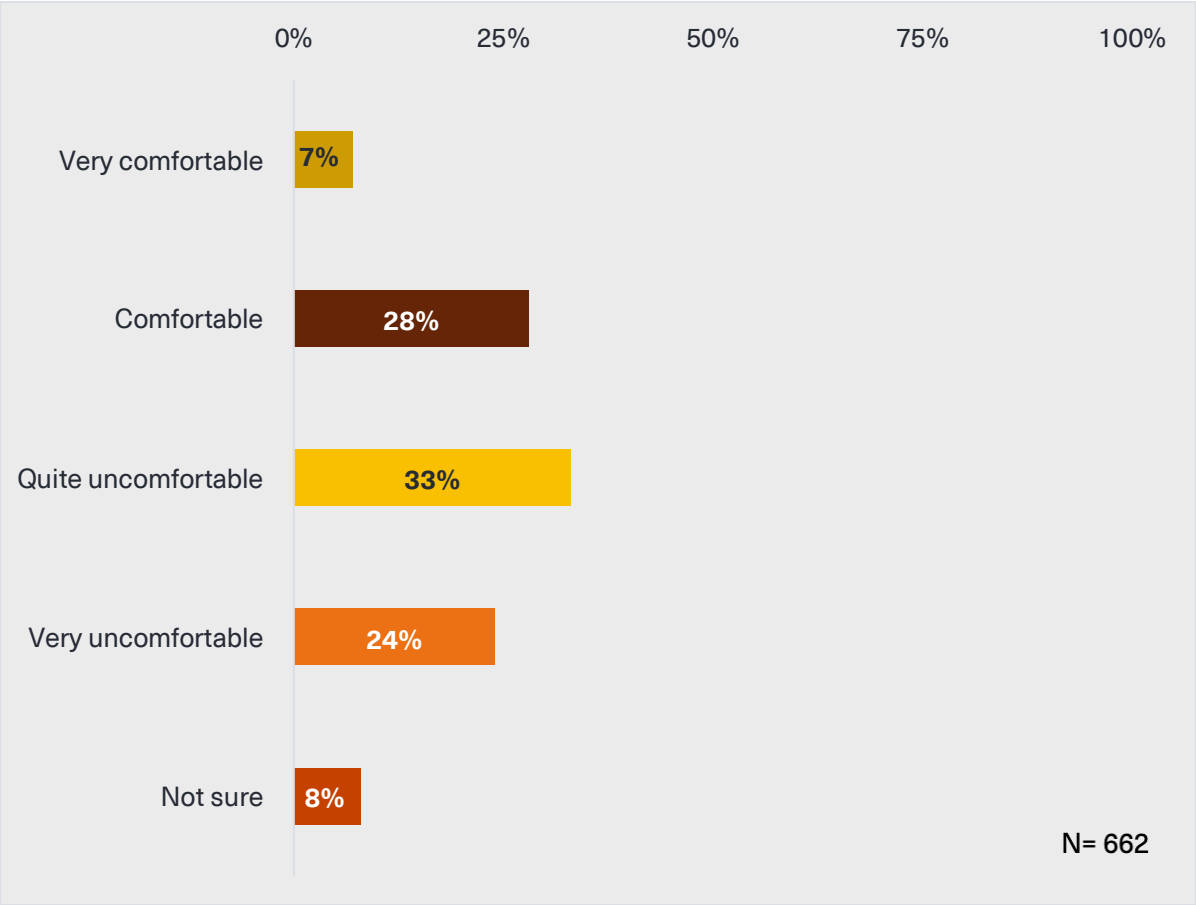
Q8. Please indicate how much you trust each of the following groups to responsibly use conventional biometric systems (e.g. processing DNA or fingerprint matching) which require someone's direct involvement in the activity.



Q9. Please indicate how much you trust each of the following groups to responsibly use remote biometric systems (e.g. facial or voice recognition) which do not require someone's direct involvement in the activity or awareness they are being subject to these systems.

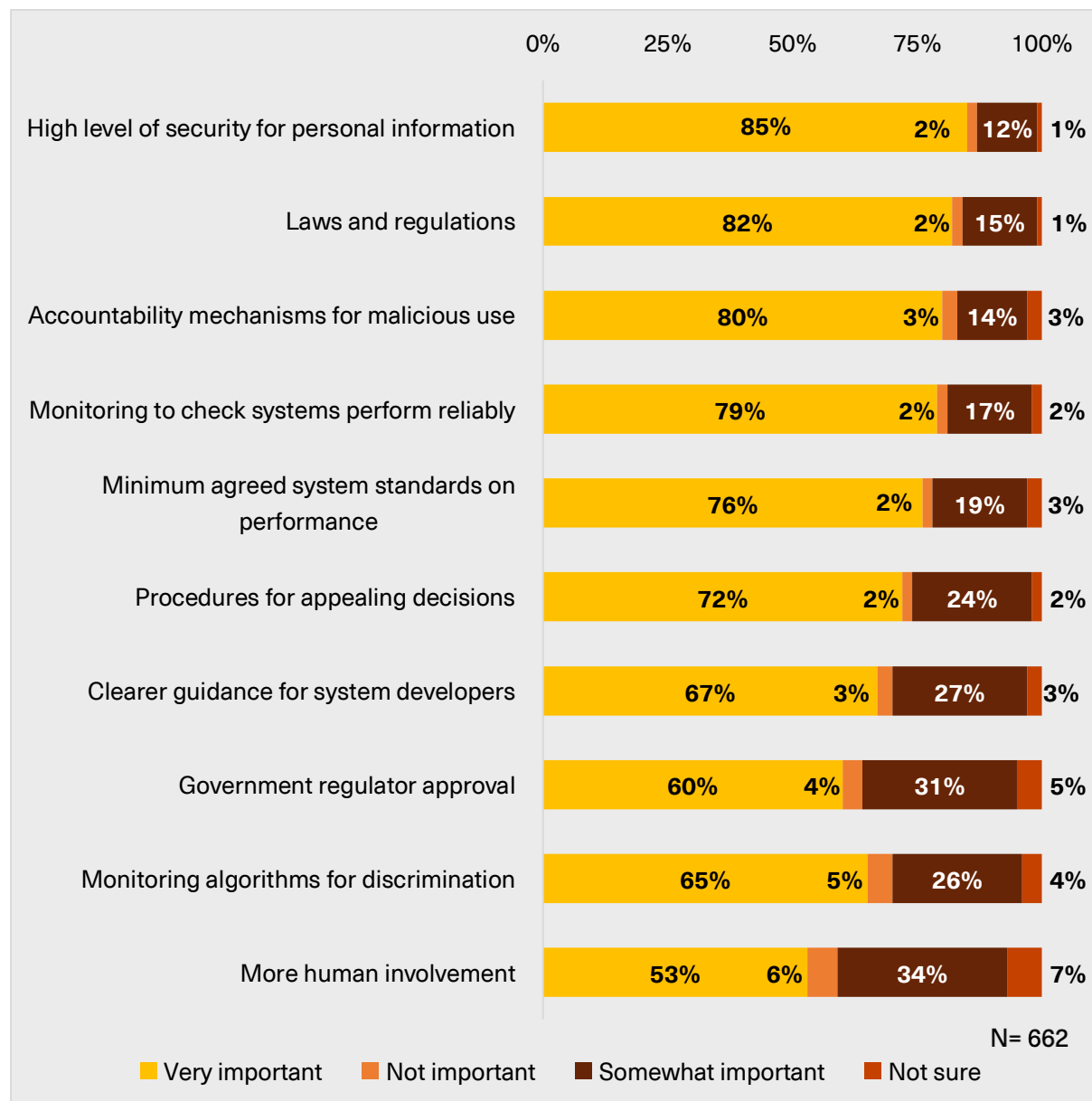


Q10. How comfortable are you with personal data collected through biometric systems being shared between police forces and private companies? For instance, a database of biometric samples collected in a supermarket being accessed by police officers to help identify criminal suspects.

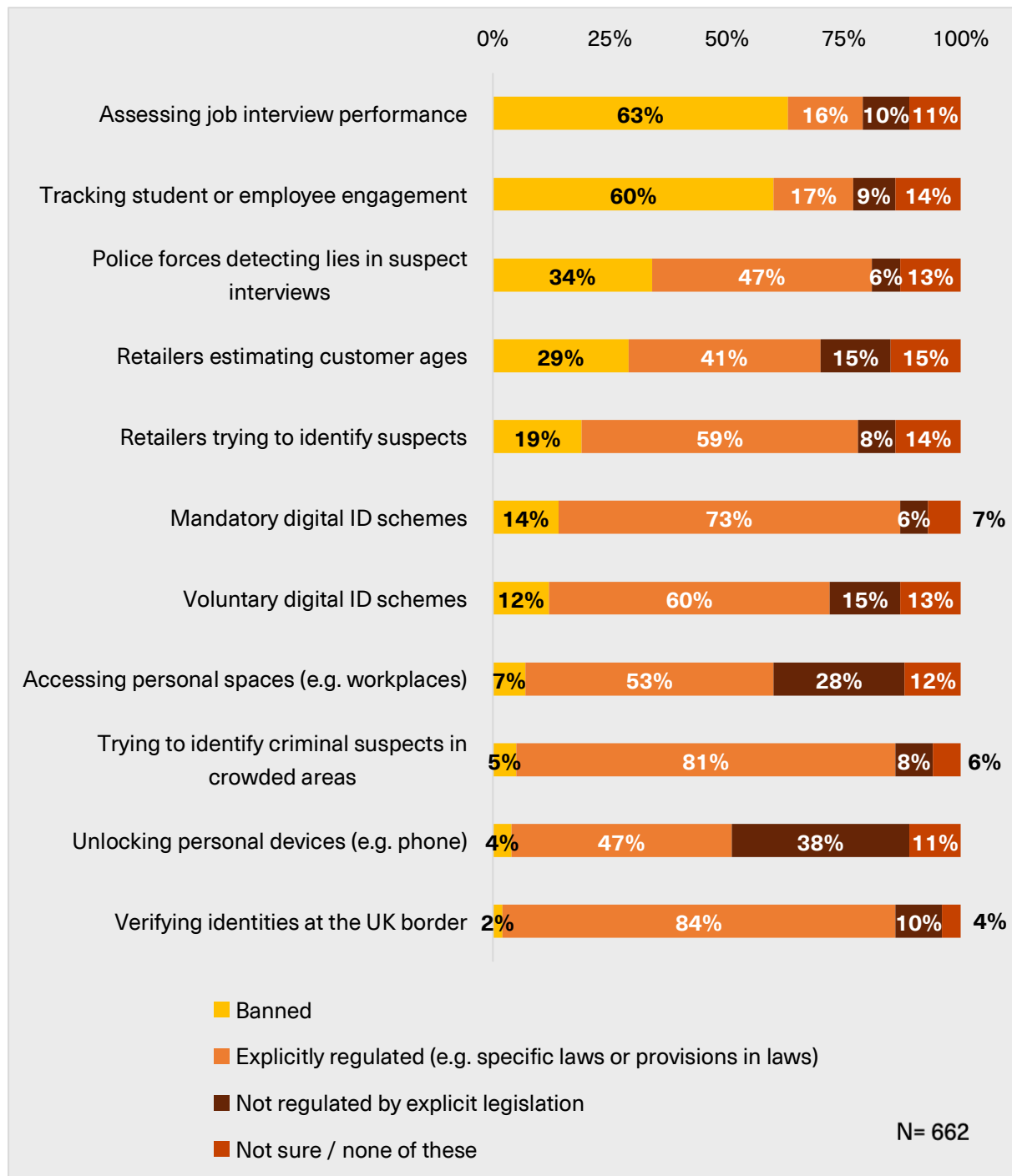


Biometric governance and regulation preference

Q11. In your view, how important are the following governance and oversight measures in making you feel more comfortable with biometric systems being deployed or used in society?

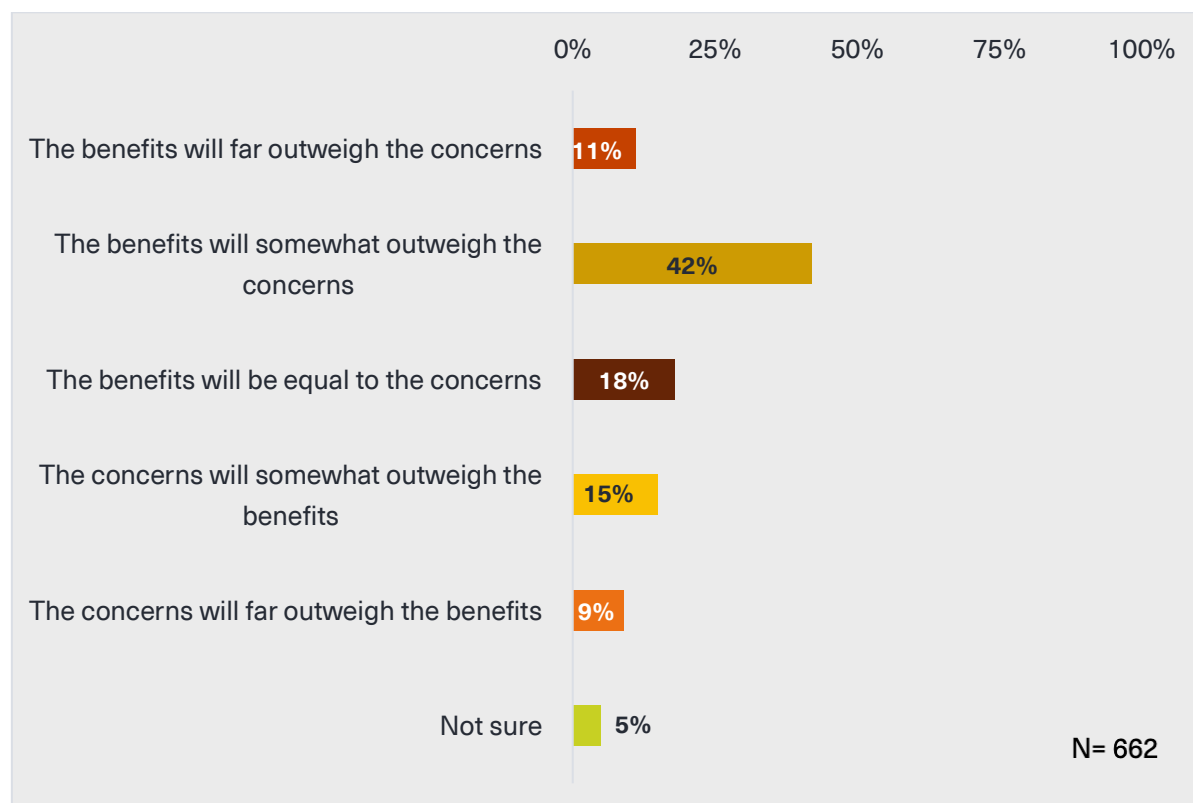


Q12. Please select all (if any) of the following applications where you feel that biometric systems should be either: unregulated, explicitly regulated (e.g. specific laws or provisions in laws) or alternatively banned from being used.



Optimism about the future of biometrics integration in society

Q13. On balance, and based on your experience of the survey, how do you think biometric systems will impact society in the future?



A.3. Qualitative survey results

Alongside multiple-choice questions, for some of the questions, respondents were also given the opportunity to provide free text comments. These were added to understand their rationale and whether there were additional considerations missing from the list of options given. The project team manually analysed these comments before clustering them based on themes, with an illustrative selection displayed below.

Attitudes towards different biometric applications and risks

When it came to comfort levels with biometrics use cases, those who provided free text comments reported higher levels of comfort for applications that provide users with a high degree of control (e.g. unlocking a mobile phone); enable greater speed, convenience and/or security to daily activities (e.g. not needing to carry paper ID documents); or help to reduce criminal activity (e.g. the use of FR systems by the police in crowded public spaces).

'These applications would make everyone safer and securer than alternatives like key cards or passwords, and would aid authentication processes.'

'I think when it comes to sensitive data that is held important to individuals, biometric methods of entry are the best way to go as it can protect people's data in the most secure way.'

'More than happy to use biometrics as it's an easy way to be identified without needing to carry ID or remember passwords, etc.'

'I find the idea of facial recognition for online purchases more intimidating than if it's just my device that's using it.'

'Ones that protect my personal safety are acceptable but not the other uses.'

'Face/fingerprint ID has been a feature of smartphones for a long time, and is generally faster than typing in a pin/passcode so it's quite normalised compared to other use cases.'

Conversely, respondents were less comfortable with applications that involved their biometric data being shared with other organisations over fears of data misuse, as well as novel classification and inferential use cases, due to concerns with the scientific validity of these systems and their potential discriminatory implications.

'I am not sure whether the companies would keep this data confidential.'

'I think it's a bit much for a retailer to hold my finger print on record.'

'I think there are folks who don't conform to neurotypical standards who may be seen as being unenthusiastic when that isn't the case. The moral ramifications of suspect identification and racial profiling is also terrifying.'

'I don't believe lie detectors are always accurate so wouldn't want police to rely on things like facial expressions.'

'I'm broadly uncomfortable with the systems being used for inferring details (such as facial expressions, telling the truth etc) as these don't seem that far a leap from things like polygraph tests. There is little 'ground truth' for these datasets to be validated against.'

'I think it gets difficult when there is a high racial diversity, the police can be accused of profiling.'

In relation to risks from biometric systems, comments clustered around fears of a disproportionate invasion of privacy; the technology making mistakes that could have major implications for individuals (e.g. wrongful arrests); and how secure the systems are from unauthorised intrusions to prevent identity theft or data breaches.

'Very easy for breaches to happen either by officials or by hackers of the like, hard to justify if such an outcome would have happened.'

'Some things would concern me a little and if the system failed and then my data was used by criminals or used for anything I was unaware of then I would be very concerned and upset.'

'Only takes one error to potentially raise suspicion to police of an innocent person who looks similar to the perpetrator, could result in minor confusion or large consequences.'

'I am mostly concerned with the wrongful identification of individuals, especially in a criminal setting.'

I am generally accepting of these systems though remain sceptical about their data and privacy implications.'

Trust in different organisations using biometric systems

On questions exploring trust in organisations that may use biometric systems, free text comments highlighted low levels of trust in commercial entities, such as employers and retailers, due to concerns over how biometric data would be handled, and the safeguards in place to ensure appropriate usage of systems.

'I don't feel that private companies, including an employer, would have a person's best interests at heart regarding biometrics.'

'I do not trust private sectors organisations to necessarily care or invest in either data validation or avenues to challenge decisions. Public sector organisations have a duty to be fair and so should have some interest in that.'

'Some employers may use the information to put pressure on employees.'

'If there is a financial gain to using this data then it will be misused eventually.'

On the other hand, comments also revealed higher levels of trust in public sector organisations based on their respective levels of accountability and oversight, as well as clearer benefits for the public in terms of tackling crime and improving peoples' health.

'Government has many regulations and oversights, third parties and businesses not so much.'

'I'm not sure but I suspect there is far more regulatory and legal protection and systematic assurances surrounding police, the NHS and to a certain extent, intelligence agencies, which means their systems are more robust and less prone to human error or misjudgement.'

'The police and gov't agencies have strict information control measures already in place. I would trust them more as a result.'

'I tend to trust the police and intelligence agencies and the NHS - essentially departments designed to make people's lives safer & healthier. I am least trustworthy of employers and retailers who might have another agenda.'

Finally, some free text comments reflected a lack of trust in any organisation to use biometric systems responsibly, due to recent high-profile cases of public data breaches and misuse.

'There is some trust in the above people, however there have been too many cases in the past of human error that has led to huge data leaks. This stops me from completely trusting any of them.'

'Currently there are too many cases of personal information being hacked into from reputable organisations such as banks etc. I feel more security needs to be in place before further biometric information is stored by large companies or organisations.'

'There have been so many recent examples of various organisations and bodies mismanaging resources and abusing the power vested in them, so I feel there is good reason not to have confidence in them having access to such important and potentially life-changing technology.'

In relation to the specific question on comfort with biometric data sharing between the police and private entities (e.g. retailers) to tackle crime, several themes emerged within the free text comments.

Some respondents reported that they would be comfortable with the public safety benefits behind such a scheme, provided there was appropriate transparency, oversight and accountability.

'As long as the reason, such as the example, is genuine and can only be used for that reason, then that's fine by me.'

'If it helps prevent crime or find perpetrators then ok but should be transparent when it goes on & have checks on usage to make sure not being abused.'

'Providing the data is secure and can't be accessed by those who might use it for other purposes (e.g. identity theft) I cannot see any reason to worry about this.'

'As long as this is controlled and regulated in some way it could be a useful database to have but if it's abused or not proportionate then it's not good.'

Others shared these sentiments, caveating that they would only feel comfortable if data sharing was a one-way process from commercial entities to the police (and not the other way round).

'Would not be comfortable with police sharing data with private companies - less concerned about the other way round.'

'As long as the data is shared only in one direction from shops to the law enforcement agencies and not vice versa.'

Finally, a remainder of participants responded with opposition to a data sharing scheme entirely, on the basis that it opened up too much risk for abuse and an invasion of privacy.

'How can it be known that the data will only be used for the exact purpose stated, and not for example sold if handed over unscrupulously?'

'Why would the police need biometric samples from large groups? The job of the police is to enforce the law and the job of private business is to make money by selling me things I want and need.'

'I don't think I would like my data to be shared at all. I would much prefer that it is verification for the one service that I have provided this information to. It adds risk of data loss and incorrect data being passed on.'

Biometric governance and regulation preferences

Respondents were invited to share any additional governance or regulatory options which would make them more comfortable with the integration of biometrics.

One set of free text comments reported that stricter penalties for misusing biometric systems should be introduced, beyond just fines.

'Jail sentences for official misuse.'

'Stringent access controls to and restrictions on use of the data, backed up with laws mandating imprisonment (not fines – that'll just be seen as a cost of doing business) for even minor violations.'

'Extremely harsh penalties to those who misuse/abuse the systems so that they act as a strong deterrent.'

Another set of comments highlighted that individuals should have clear rights to not use biometric systems or have their biometric data processed when it is not essential, as well as rights to view information held about them.

'No implications for a person who refuses to provide biometrics.'

'Clear ability to not use these systems. To not have biometric data stored. To not be discriminated against for not using it.'

'The right to know if these systems are being used and the right to see what information is collected on you, unless there are good grounds for this information being withheld e.g. terrorist related surveillance.'

A final cluster of free text comments suggested a range of other governance mechanisms, including independent oversight bodies and ethics committees.

'Independent public oversight for all governmental or mandatory biometric systems.'

'Independent ethics commission overseeing the application of such technology.'

'I think there would need to be an independent body that is aware of the systems. The people reviewing the systems should be rotated to prevent any inherent biases forming'.

On the question around regulatory preferences for different use cases, some participants responded that classification and inferential systems should be banned, owing to fears around the subjective nature of the data processed and discrimination against different vulnerable groups in society (e.g. neurodivergent individuals).

'I don't know it could accurately tell if you were telling the truth. It would be terrible if it was used as evidence and then later proven to not work reliably.'

'There is a powerful subjective element that negates the accuracy of the process.'

'I really do not want employers or educators to try to get an idea about what may be going on in my head. That feels like it would be considerably unreliable and liable for false positives. Biometrics should not be used for emotional things.'

'The point about assessing someone's level of enthusiasm is inherently discriminatory. It is inherently discriminatory towards certain groups of people, such as neurodivergent people, and people with visible and not visible physical and mental disabilities'.

'Ban on employers and training organisations since it is simply invasive and dehumanizing. Ban on police determining whether someone is telling the truth since I think it may not be helpful to use biometric to ultimately determine the truth.'

A second group of participants also highlighted that when it came to applications where involvement was optional (e.g. unlocking your phone), less specific regulation would be required, as opposed to systems such as FR which could be used remotely without someone's awareness or consent.

'I think if the system is optional, for example the first option, or unlocking your phone etc then less specific legislation is needed.'

'If it's going to be used in a mandatory/enforcement way then specific legislation about the scope and purpose should be implemented.'

'Where used for personal verification no law required – where used for identification, should be regulated.'

Optimism about the future of biometrics integration in society

Finally, in relation to levels of optimism with integrating biometric systems more widely across society, free text comments shed light on the rationale behind the quantitative responses.

A first set of participants responded optimistically that the use of more biometric systems would help to increase both personal security through making hacking or identity theft more difficult, as well as helping to reduce crime.

'A secure biometrics system will cut down on the vast majority of online scams. For example, there should be no more need for email/password combos for accounts online.'

'Safe and secure environments should be a given, these data systems will help to provide these safe and secure environments.'

'For safety, for cybercrime or security breaches, I think biometric systems are a definite benefit.'

'The ability for criminals to be caught makes this technology very useful even though it has its flaws.'

'Crime fighting agencies need all of the help they can get and this technology will help them greatly.'

In contrast, others expressed concern over deeper integration of biometric systems due to the potential for mistakes and abuse to override the possible benefits.

'All these new technologies which are meant to improve lives disproportionately harm lower socio-economic backgrounds.'

'The benefits will apply more to governments and organisations. Individuals will not notice much benefit.'

'No matter how good this technology gets in the future, it is always going to invade people's privacy and be used by unscrupulous actors to target individuals and groups.'

A third set of participants were cautiously optimistic that, over time, improvements in algorithms will make biometric systems more trustworthy and accurate.

'As time goes, algorithms develop etc, the processes will become more accurate and the public will get more used to them.'

'As computer systems get more accurate and software development gets better, there is less to go wrong.'

'As it is tested and used more, I think it will be beneficial and simplify some processes.'

A final group reported that while biometric systems may bring benefits to society, appropriate regulation and oversight will be key to realising them.

'I think it will bring about a lot of exciting tools which allow higher identification of crime. If conducted correctly with transparency and rules it has a lot of benefits.'

'General feelings toward biometric data gathering is it is a good thing for the benefit of society but it is in early days and regulation is required.'

'These are very useful ways to keep us all safe as we are at more risk than we used to be as long as they are able to be regulated and only used by the correct people.'

'I believe that with the proper regulation and understanding, biometrics will be a really valuable tool – particularly in the realm of crime prevention. I think it can be used in other situations (verifying purchases, unlocking your phone), particularly for the convenience of the user, but if it is not regulated tightly it could pose a threat to one's security.'



Centre for Emerging Technology and Security

RESEARCH REPORT