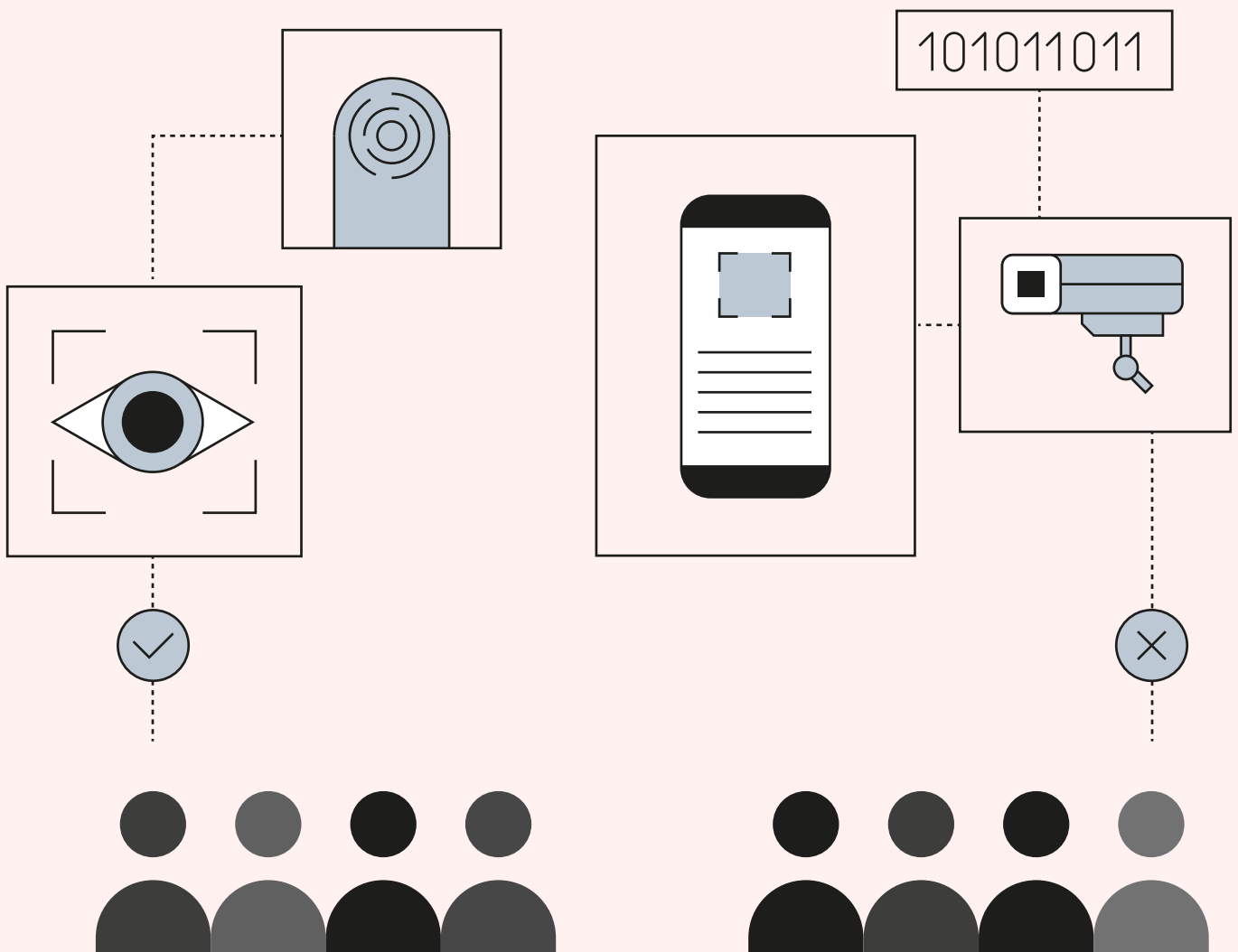


The Citizens' Biometrics Council

Recommendations and findings of
a public deliberation on biometrics
technology, policy and governance

March 2021



Contents

- 2 Overview
- 4 About this report
- 7 What are biometrics?
- 9 Background: a biometrics backlash?
- 14 Methodology
- 21 The Council's recommendations
- 24 Findings: the Council's deliberations
- 42 Conclusion: addressing the Council's recommendations
- 48 Appendix
- 51 About the Ada Lovelace Institute

What is or isn't ok when it comes to the use of biometric technologies?

Overview

Biometric technologies, from facial recognition to digital fingerprinting, have proliferated through society in recent years. Applied in an increasing number of contexts, the benefits they offer are counterbalanced by numerous ethical and societal concerns.

In 2019, the Ada Lovelace Institute called for a moratorium on facial recognition, arguing for a halt on its use until the societal, ethical and legal conditions for the responsible use of emerging biometric technologies were established.

Since then, a range of actors, from the commercial and political to the legal and academic, have continued to contribute to the debate around biometrics. But a crucial stakeholder group is yet to be consulted: the public.

Throughout 2020 the Ada Lovelace Institute established the Citizens' Biometrics Council to deliberate on the use of biometric technologies, bringing much-needed public perspectives to this debate.

Across 60 hours of in-person and online workshops, the Council considered a range of arguments and evidence about technologies such as facial recognition, voice recognition, digital fingerprinting and more.

The Council members included a diverse range of 50 members of the public, recruited to reflect different social, economic and political attitudes, as well as different perspectives on data and technology.

They heard from experts – including police strategists, technology developers, regulators, campaigners, tech ethicists and more – and debated on the opportunities and risks posed by these powerful technologies.

The Council's goal was to bring a range of people's voices to the debate on biometrics and build deeper understanding of their concerns, expectations and red lines.

To conclude their deliberations, the Citizens' Biometrics Council developed a set of recommendations to address the question: **what is or isn't OK when it comes to the use of biometric technologies?**

These recommendations cluster around three issues:

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

In this report, we share the Council's recommendations in full, explore their deliberations and describe next steps for policy and practice.

‘Trust is the one word that sticks in my mind throughout the whole process of biometrics discussions.’

The Ada Lovelace Institute established the Citizens' Biometrics Council to bring the public's voice into debates about biometrics

About this report

The Ada Lovelace Institute's 2019 call for a moratorium on biometric technologies like facial recognition was followed by a survey of public attitudes towards facial recognition, published in the report *Beyond Face Value*.^{1,2} The survey showed that not only did the majority of the UK public want greater limitations on the use of facial recognition, but that a deeper understanding of public perspectives was needed to inform what would be considered as socially acceptable for these technologies.

Following *Beyond Face Value*, the Ada Lovelace Institute began work to establish the Citizens' Biometrics Council, to create space to better understand public perspectives and bring their voice to debates about biometrics.

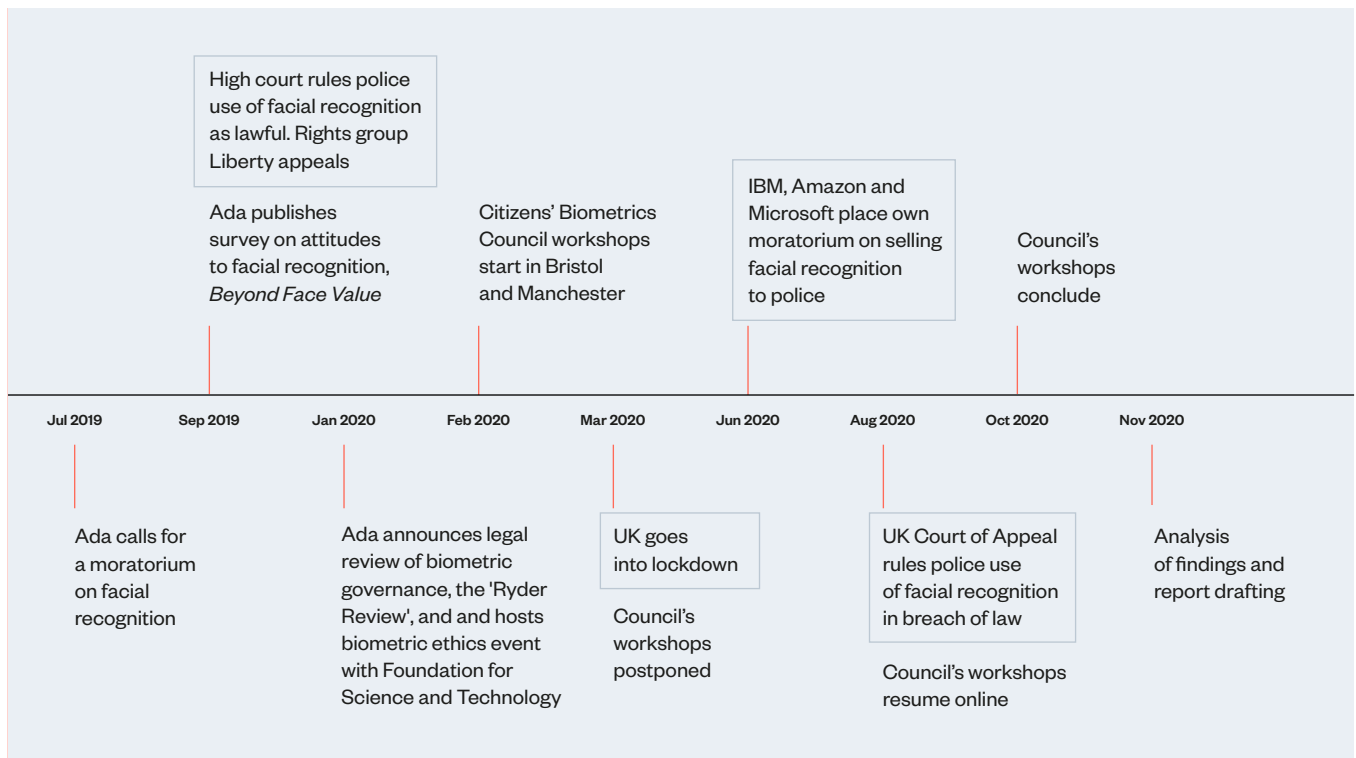
Concurrent to the Council, the Ada Lovelace Institute also commissioned an independent legal review of the governance of biometric data in the UK, led by Matthew Ryder QC, which is due to report in spring 2021.³ The legal review and the Citizens' Biometrics Council have led independent but parallel enquiries, and offer different types of evidence that are essential for contributing to the trustworthy and trusted use of biometrics.

Where the Citizens' Biometrics Council offers public perspectives on the conditions for proportionate and responsible biometrics, the legal review will provide detailed analysis of the current state of the law concerning the governance of biometric data, and recommendations for legislative changes required to provide greater oversight of the technology.

This report describes the Citizens' Biometrics Council. It outlines the background to the current landscape around biometrics; details

-
- 1 Kind, C. (2019) *Biometrics and facial recognition technology – where next?*, Ada Lovelace Institute. Available at: www.adalovelaceinstitute.org/blog/biometrics-and-facial-recognition-technology-where-next (Accessed: 23 February 2021).
 - 2 Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. Available at: www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology (Accessed: 23 February 2021).
 - 3 Ada Lovelace (2019) *Ada Lovelace Institute announces independent review of the governance of biometric data*. Available at: www.adalovelaceinstitute.org/news/independent-review-governance-of-biometric-data (Accessed: 23 February 2021).

the methodology used to deliver the Council; lists the Council's recommendations; analyses the core themes that emerged during their deliberations; and describes three topics that the recommendations cluster around, highlighting the direction that policymakers and practitioners should take to respond to the Councils' deliberations.



Timeline of events

How to read this report...

The Council's recommendations ([page 21](#)) are statements generated by the Council members as they concluded their deliberations, and give direct voice to their perspectives. The recommendations are the key findings from the Council.

...if you're a policymaker, researcher or regulator thinking about biometric technologies:

- The methodology ([page 14](#)) describes how the project was designed to generate robust and relevant findings.
- The conclusion ([page 42](#)) describes three areas where the Councils' recommendations converge, and practical next steps for policy, governance and technology development. The findings of the legal

review, publishing in spring 2021, will provide detailed analysis and recommendations that build on these areas and more.

...if you're a developer or designer building biometric technologies:

- The findings ([page 24](#)) provide detail of the core themes that emerged during the Council's deliberations. These are crucial for understanding what responsible practices and technology design should look like: they are a guide for building better biometric technology.

...if you're procuring or deploying biometrics:

- The background ([page 9](#)) describes the current landscape around biometric technologies; where they have been deployed, the societal challenges they raise and the controversy that surrounds them. It demonstrates why public voice is needed to shape better use of biometrics.
- The findings ([page 24](#)) and the conclusion ([page 42](#)) describe the core themes of the Council's deliberations and options for policy and practice, which should be considered a guide for the responsible use of biometric technologies.

A note on quotes

Throughout this report, any text in quotation marks represents quotes from Council members' deliberations drawn from the transcripts of the workshops, unless otherwise attributed.

Some quotes have been edited to improve readability, for example by removing repetition or filler words used as Council members articulated their thoughts. There have been no additions, word replacements or other edits that would change the meaning or sentiment of Council members' statements.

All the quotes have been included to amplify the voices of the Council members, and demonstrate the richness of their perspectives.

What are biometrics?







Throughout this report, and across the Council's workshops, the terms 'biometric technologies', 'biometrics' and 'biometric data' refer to a range of technologies and systems which use digital devices, data science and artificial intelligence (AI) to identify people through data about their biological characteristics.

During the Citizens' Biometrics Council discussions, we put forward an explanation of biometrics for members to consider (and question), using a version of this infographic:

Biometric technologies use people's biological information for purposes like identification or verification.


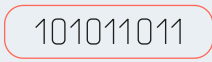

They use information about an individual's unique biological traits that can be measured, recorded and quantified.

Examples of biological traits can include:

		
Fingerprints	DNA	Faces
		
Gaits (how we walk)	Iris patterns	Heartbeat patterns

Measurements, descriptions or other information about these traits are **biometric data** and can be stored digitally as **templates**.

These are strings of letters and numbers which an algorithm or computer uses to process biometric data.

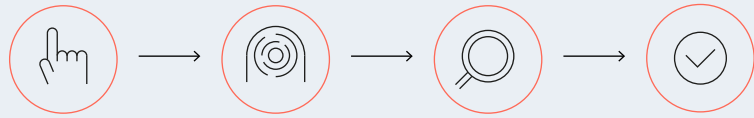
 →  → 

E.g. biometric data about an individual's face or fingerprint might not be stored as a picture, but instead as a piece of code generated to describe the important features of the picture.

Biometric technologies capture, record and process biometric data for a purpose, often to identify or verify individuals.

Identifying: determining who an unknown person is by matching their data with data already in a database.

Verifying: confirming a person is who they say they are, like checking an ID card.



An individual places their finger on a scanning device

The device scans their fingerprint, takes measurements and creates a unique **template**

The device searches to match this new template to a template stored in a database

The system identifies or verifies the individual if it finds a match

Biometric technologies may use a combination of techniques, like video image processing, machine learning or infrared detection (and many more).

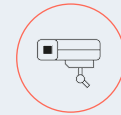
The data or templates they collect could be **stored**, either on the device or in a database connected by a network or the internet. Or they might be **deleted** immediately after the device has processed it.

Whether data or templates are deleted or stored (and how, and for how long) depends on the type of technology used and its purpose.

Biometric technologies can be **active** or **passive**.



Active: an individual actively provides information. E.g. by placing a finger on a scanner



Passive: a technology detects information about people. E.g. facial recognition camera

In 2020, with the arrival of the COVID-19 pandemic, digital tools using facial and other biometric data found new prominence

Background: a biometrics backlash?

Recent years have seen a snowball of developments in relation to biometric technologies. Digital fingerprinting found prominence in the consumer mainstream when Apple introduced 'Touch ID' to its smartphones in 2013. Customers who use telephone banking have become familiar with using their voice as their password. From 2016, South Wales Police and London's Metropolitan Police began trials deploying automated facial recognition in public places in the UK.⁴

In 2020, with the arrival of the COVID-19 pandemic, digital tools using facial and other biometric data found new prominence verifying people's identities in an increasingly contactless and online world.^{5,6} In Russia, facial recognition systems have been used to enforce COVID-19 lockdown restrictions, and in Singapore they have been adopted for online access to government services.^{7,8} In the UK, facial recognition has been suggested for the verification of a person's immunity or vaccination status,⁹ and law enforcement agencies in the US have continued to deploy facial recognition algorithms, including to retroactively identify violent protestors.¹⁰

-
- 4 See: Metropolitan Police Service (no date) *Update on facial recognition*. Available at: www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition; South Wales Police (no date) *What is AFR?*. Available at: <http://afr.south-wales.police.uk/what-is-afr> (Accessed: 23 February 2021).
 - 5 Biometrics Institute (2020) *COVID-19: Effective and responsible biometrics solutions and concepts in a time of pandemic-building a resilient response*. Available at: www.biometricsinstitute.org/?smd_process_download=1&download_id=6110 (Accessed: 17 November 2020).
 - 6 Burgess, M. (2020) 'Co-op is using facial recognition tech to scan and track shoppers', *Wired UK*, 10 December. Available at: www.wired.co.uk/article/coop-facial-recognition (Accessed: 11 December 2020).
 - 7 Dixon, R. (2020) 'In Russia, facial surveillance and threat of prison being used to make coronavirus quarantines stick', *Washington Post*. Available at: www.washingtonpost.com/world/europe/in-russia-facial-surveillance-and-risk-of-jail-look-to-make-coronavirus-quarantines-stick/2020/03/24/a590c7e8-6dbf-11ea-a156-0048b62cdb51_story.html (Accessed: 17 November 2020).
 - 8 MacDonald, T. (2020) 'Singapore in world first for facial verification', *BBC News*. Available at: www.bbc.co.uk/news/business-54266602 (Accessed: 17 November 2020).
 - 9 Onfido (2020) *The role of Digital Identity in Immunity Passports, written evidence submission*. Available at: <https://committees.parliament.uk/downloadfile/?url=%2Fwrittenevidence%2F2537%2Fdocuments%2F5286%3Fconvertiblefileformat%3Dpdf&slug=c190014pdf> (Accessed: 17 November 2020).
 - 10 Vincent, J. (2020) 'NYPD used facial recognition to track down Black Lives Matter activist, The Verge.' Available at: www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram (Accessed: 23 February 2021).

The contention that biometric systems are deployed in the public interest is counterbalanced by a range of societal and ethical concerns

The benefits and opportunities posed by biometric technologies include their ability to support effective law enforcement, ensure public safety and verify identities securely and virtually. Biometric technologies have been used in policing for decades, through DNA and fingerprint matching, and are widely deployed in other settings where safe and reliable identification of individuals is required, such as building or device security and at international borders. Emerging biometric technologies, such as automated facial recognition, have current and potential applications in improving services and online safety, and in tackling serious crime.

But the contention that biometric systems are deployed in the public interest is counterbalanced by a range of societal and ethical concerns. These concerns are driving a growing controversy around the use of biometric technologies and increasing resistance towards them, particularly towards automated facial recognition.

In the UK, the Court of Appeal ruled that South Wales Police's use of automated facial recognition was unlawful in response to a case brought by Ed Bridges and civil rights group, Liberty.¹¹ Journalists around the world have questioned the role of facial recognition in the treatment of Uighur Muslims in China.¹² In the USA, Portland became the country's fourth city to ban uses of facial recognition.¹³ Facial recognition company Clearview AI made controversial headlines when it was revealed it was scraping images from social media for its algorithms.¹⁴ And three major technology firms – IBM, Amazon and Microsoft – all announced they would stop or limit the use of their facial recognition systems by police forces in the wake of the Black Lives Matter protests.¹⁵

11 Ryder M. and Jones J. (2020) 'Facial recognition technology needs proper regulation' – Court of Appeal, Ada Lovelace Institute. Available at: www.adalovelaceinstitute.org/facial-recognition-technology-needs-proper-regulation-court-of-appeal (Accessed: 17 November 2020).

12 Mozur, P. (2019) 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority', *The New York Times*, 14 April. Available at: www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (Accessed: 23 February 2021).

13 Brandom, R. (2020) 'Portland, Maine has voted to ban facial recognition, The Verge'. Available at: www.theverge.com/2020/11/4/21536892/portland-maine-facial-recognition-ban-passed-surveillance (Accessed: 4 November 2020).

14 Hill, K. (2020) 'The Secretive Company That Might End Privacy as We Know It', *The New York Times*, 18 January. Available at: www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Accessed: 18 November 2020).

15 Heilweil, R. (2020) 'Big tech companies back away from selling facial recognition to police. That's progress.' Vox. Available at: www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police (Accessed: 17 November 2020).

In the UK, the Information Commissioner's Office, former Biometrics Commissioner and former Surveillance Camera Commissioner have all argued that the law related to biometric technologies is no longer fit for purpose

Campaigners and legal scholars have articulated the powerful ways that biometric technologies can subject citizens to undue surveillance, infringing on people's privacy, civil liberties and data rights. Researchers have demonstrated how many of the market-leading and widely-deployed facial recognition algorithms contain biases which reduce their accuracy for ethnic minorities and women, particularly Black women.^{16,17} When used in contexts already characterised by structural injustice, these factors could compound and amplify the institutional racism and other biased outcomes that already persist.¹⁸

In the UK, the Information Commissioner's Office (ICO), former Biometrics Commissioner and former Surveillance Camera Commissioner have all argued that the law related to biometric technologies is no longer fit for purpose.¹⁹ In August 2020, the Court of Appeal of England and Wales concluded that there were 'fundamental deficiencies' in the legal framework surrounding the police use of facial recognition.²⁰ An editorial in the world's leading science journal, *Nature*, argues biometrics needs an 'ethical reckoning', calling for researchers, funders and institutions working in the fields of computer science and artificial intelligence to respond to 'the ethical challenges of biometrics'.²¹

There are efforts to address these gaps: researchers have developed frameworks to support audits of facial recognition systems, some technology developers are committed to demonstrating responsible uses of biometrics, and arguments for a US Federal Office for facial

-
- 16 Buolamwini J., Geburu T. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.' *Proceedings of Machine Learning Research* 81:1-15, Conference on Fairness, Accountability, and Transparency.
- 17 Leslie, D. (2020) Understanding bias in facial recognition technologies. Zenodo. doi: [10.5281/zenodo.4050457](https://doi.org/10.5281/zenodo.4050457)
- 18 Chowdhury, A. (2020) 'Unmasking Facial Recognition: An exploration of the racial bias implications of facial recognition surveillance in the United Kingdom.' *WebRoots Democracy*. Available at: <https://webrootsdemocracy.org/unmasking-facial-recognition> (Accessed: 18 March 2021).
- 19 Information Commissioner's Office (2019) *The use of live facial recognition technology by law enforcement in public places*. Available at: <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf> (Accessed: 27 November 2020); Wiles P (2020) *Biometrics Commissioner's address to the Westminster Forum: 5 May 2020*, GOV.UK. Available at: www.gov.uk/government/speeches/biometrics-commissioners-address-to-the-westminster-forum-5-may-2020 (Accessed: 17 November 2020); Porter, T. (2020) 'Facing the Camera: Good practice and guidance'. Surveillance Camera Commissioner. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.
- 20 Ryder M., Jones J. (2020) 'Facial recognition technology needs proper regulation', *Ada Lovelace Institute*. Available at: www.adalovelaceinstitute.org/blog/facial-recognition-technology-needs-proper-regulation (Accessed: 18 March 2021).
- 21 Nature editorial (2020) 'Facial-recognition research needs an ethical reckoning', *Nature*, 587(7834), pp. 330-330. doi: [10.1038/d41586-020-03256-7](https://doi.org/10.1038/d41586-020-03256-7).

What constitutes trustworthy, responsible, proportionate use of biometric technologies is one of the most complex and urgent questions facing our society today

recognition have been put forward.^{22,23,24} The former Surveillance Camera Commissioner has also issued guidance for the use of facial recognition by UK police forces.²⁵

However, to date little public debate has taken place about what legal and ethical checks and balances are needed – particularly in the UK – and the lack of adequate regulation and oversight leaves potential for misguided use of biometrics at best, and misuse at worst. While many stakeholders with commercial, legal or research interests in biometric technologies have contributed to debates about how biometric technologies can be deployed in the public interest, a crucial stakeholder group is yet to be consulted: the public.

What constitutes trustworthy, responsible, proportionate use of biometric technologies is one of the most complex and urgent questions facing our society today. Addressing this question requires a range of inputs, from legal inquiry and ethical analysis to political scrutiny. But it cannot be addressed without public input.

The Ada Lovelace Institute convened the Citizens' Biometrics Council to bring perspectives of informed members of the public to debates about biometric technologies. We believe the Council's recommendations are a crucial component in responding to the increasingly ubiquitous role biometric technologies appear set to play in our world.

‘Public interest tests [relating to the use of biometrics] ought to be informed by the sentiment of the public, but that sentiment is not best read from simple public opinion surveys, although methodologically more sophisticated work may have a part to play.

22 Ho, D. E. et al. (2020) 'Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains', *Stanford Institute for Human-Centered Artificial Intelligence*. Available at: https://hai.stanford.edu/sites/default/files/2020-11/HAI_FacialRecognitionWhitePaper_Nov20.pdf (Accessed: 18 March 2021).

23 See: *Safe Face Pledge*. Available at: www.safefacepledge.org (Accessed: 23 February 2021).

24 Erik Learned-Miller et al. (2020) 'Facial recognition technologies in the wild'. *Algorithmic Justice League*.

25 Porter, T. (2020) 'Facing the Camera: Good practice and guidance'. *Surveillance Camera Commissioner*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf (Accessed: 18 March 2021)

For citizens to reach an informed view they need to be informed by a public debate – the sentiment of the public should be formed based on such evidence and reasoning.’

Paul Wiles, Biometrics Commissioner 2016–2020.²⁶

Deliberative approaches such as those used in the Council enable detailed understanding of people's perspectives on complex topic areas

Methodology

The Citizens' Biometrics Council ran from February to October 2020, in-person and online. It involved 50 members of the public who took part in 60 hours of deliberative workshops. During the workshops, they considered evidence about biometric technologies, heard from experts from a range of backgrounds, and participated in facilitated discussion.

The Ada Lovelace Institute conceived of and designed the Citizen's Biometrics Council to address the following aim: to give an understanding of an informed public's expectations, conditions for trustworthiness and red lines when it comes to the use of biometric technologies and data.

Throughout the process, all members of the Citizens' Biometrics Council became informed on the topic, and considered the information and their task with thought and scrutiny. They concluded by developing a set of recommendations that respond to the urgent need for public voice on the use of biometric technologies.

Deliberative approaches such as those used in the Council enable detailed understanding of people's perspectives on complex topic areas. Valuable in their own right, they also complement quantitative methods, such as surveys or opinion polls, like our *Beyond Face Value* report. A survey can offer population-level insights on attitudes, while qualitative and deliberative methods, such as those used with the Council, offer insight on why people hold certain opinions, what values or information inform those views, and what they would advise when informed.

Recruiting for the Council

We recruited Council members to include a broad and diverse range of perspectives while maintaining a manageable number of participants that could engage meaningfully in rich, facilitated discussions. We initially sought to recruit 60 participants to meet this aim within the bounds of our capacity.

Mini-publics such as the Citizens' Biometrics Council can never be statistically representative of the wider population, nor should they aim to be. Instead, they should reflect the diversity of views within a population.²⁷

To achieve this, we used a purposive approach to recruitment, inviting participants to the Council via a market research recruitment agency with selection criteria to ensure the representation of a diverse range of perspectives on the Council, and to account for the disproportionate and biased impacts of biometric technologies on underrepresented and marginalised groups.

We recruited participants against the following selection factors:

- gender
- age
- ethnicity
- disability
- life stage
- current working status and type
- socio-economic background
- urban or rural place of residence
- attitudes to the use of data.

Council members were recruited from both the Bristol and Manchester areas, creating two groups of 30 participants who came together to participate in workshops. We chose these locations to avoid a London-centric bias, and as they offer diverse populations but would enable participants to travel easily and meet face-to-face.

We paid participants incentives at industry best-practice rates for each workshop they attended, to remunerate them for their time and contributions to the Council.

Due to COVID-19, some participants had to withdraw from the project, and we additionally recruited some participants to ensure we maintained diversity against our criteria. Ultimately, the Council consisted of 50 people who participated in the majority of workshops and contributed to the development of the Council's recommendations.

27 Steel, D. et al. (2020) 'Rethinking Representation and Diversity in Deliberative Minipublics', *Journal of Deliberative Democracy*, 16(1), pp. 46–57. doi: [10.16997/jdd.398](https://doi.org/10.16997/jdd.398).

The Council workshops

The Council's deliberations were designed around a series of three weekend-long workshops. These workshops were planned to take place between 10:00 and 16:00, Saturday and Sunday across six weekends in February, March and April 2020 (so that each Council group in Bristol and Manchester took part in three workshop weekends).

Each workshop involved a combination of:

- **Considering a balanced range of information and evidence about biometric technologies and the challenges they pose.** Evidence was drawn from: news articles, academic research, research carried out by the Ada Lovelace Institute, public information provided by technology companies, policy papers and other literature. Where necessary, researchers at the Ada Lovelace Institute, and facilitators at Hopkins Van Mil summarised the evidence, or made it more accessible.
- **Hearing from, and posing questions to expert speakers** who represented technology developers, organisations deploying biometrics, civil rights advocates and campaigners, academic researchers, government bodies and regulators. (See [appendix](#) for a list of speakers).
- **Engaging in facilitated discussion and deliberation** with other Council members and expert speakers to address questions and develop recommendations.

The workshop structure

Weekend	Topic	Items explored/discussed	Expert speakers
1	Getting to grips with biometrics	<ul style="list-style-type: none"> • biometric technologies: what they are, how they work and examples of recent cases • the Council's purpose and role, and the structure of the process • initial reflections on benefits and harms, including bias, discrimination, trust and data privacy • considering and developing the central question the Council will address 	Technology developers, regulators, police and national security technologists, Surveillance Camera Commissioner
2	Exploring the benefits and harms	<ul style="list-style-type: none"> • privacy and surveillance • consent • bias, discrimination and accuracy • public safety • data protection 	Civil rights advocates, academic researchers, ethics specialists
3	Drawing conclusions and developing recommendations	<ul style="list-style-type: none"> • legislation and policy landscape • developing recommendations • presenting recommendations to a policy panel 	Regulators, policy experts, technology developers, legal experts, Biometrics Commissioner

Although the two groups met separately, they took part in the same workshop structure, and there were no notable differences in the topics and themes discussed between the groups. This report reflects the perspectives of Council members from across both groups.

Community Voices workshops

The project was designed specifically to involve and amplify the voices of people from minority ethnic groups, members of the LGBTQI+ community and people with disabilities. Existing research, and our 2019 survey *Beyond Face Value*, showed that these groups are often disproportionately impacted by biometric technologies, and face unique challenges in response to them but are too-often underrepresented in debates about technology.

In addition to the Citizens' Biometrics Council workshops, we convened one Community Voices group for each of the above groups, including between seven and twelve members in each, recruited via community groups and charities. The Community Voices groups met once before the main Council workshops began, and again during the reporting phase after the Council's workshops ended, for around two hours each time. The Community Voices workshops aimed to ensure these groups' perspectives were embedded in the Council's deliberations by:

- informing the design process by considering what topics and concerns the groups felt the Council should consider
- focusing on how to address the experiences of marginalised groups and the disproportionate impacts of biometric technologies
- reviewing the Council's findings and recommendations to feed back on how to amplify the perspectives of marginalised groups
- ensuring that the entire process is informed by, and appropriately weighted to consider, the views of minority ethnic groups, members of the LGBTQI+ community and people with disabilities.

At least one participant from each group also participated in the Council's workshops. Members of the Community Voices workshops, as well as all members of the Council, were engaged through an intersectional approach that encouraged them to speak from their own pluralistic experience, rather than represent 'the view' of one particular demographic.

The discussions these groups had are reflected throughout this report as part of the overall project, as well as in other reports by the Ada Lovelace Institute.²⁸ In particular, bias, discrimination and inequality became core themes throughout the Council's deliberations, strengthened and enriched by the contributions of the Community Voices groups.

COVID-19: disruption and going online

Planning for the project began in September 2019, long before the COVID-19 pandemic arrived. This meant the project was designed to take place in-person, and was adapted to work online following the implementation of lockdown restrictions.

The Citizens' Biometrics Council was midway through its workshops in March 2020 when the UK began to witness a rise in Coronavirus cases, and the UK Government implemented lockdown restrictions. At this time, the Manchester group had completed their first weekend of workshops, and the Bristol group had completed its second weekend.

28 See: Patel R., Peppin A. (2020) 'Making visible the invisible: what public engagement uncovers about privilege and power in data systems'. *Ada Lovelace Institute*. Available at: www.adalovelaceinstitute.org/blog/public-engagement-uncovers-privilege-and-power-in-data-systems (Accessed: 8 January 2021); Ada Lovelace Institute (2020) *No green lights, no red lines*. Available at: www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf (Accessed: 8 January 2021).

Moving the format online required considerable thought in redesign, but ultimately presented a different way of conducting the workshops

We immediately postponed the process, aiming to reconvene in Autumn 2020. Initially, we had hoped to reconvene the Council in-person, but as the world rapidly adapted to online working, and as it became clear that meeting in large groups would continue to be unsafe until the arrival of a vaccine, we explored approaches to bringing the Council together online.

In the intervening months, many public engagement organisations and researchers began to iterate and develop tools and methods for conducting public engagement deliberative workshops in online environments.^{29,30} We drew from these to adapt the remaining workshops to work online, via Zoom, as well as establishing an online forum where we could continue to share some materials, create 'homework' tasks and keep in contact with participants.

The Manchester group resumed their deliberation in September completed their second workshop online across evenings and weekends. Both Manchester and Bristol groups then conducted their final 'weekend' via a series of online workshops in October 2020.

The online workshops were one-and-a-half to two hours long, and followed developing best practice about suitable lengths for a comfortable and productive online session. Moving online led to some challenges, for example, participants couldn't enjoy the creative benefits of being in the same room, nor could they work together to craft and explore ideas on paper.

However, the online workshops had no travel requirements, and some participants found it easier to fit them into their schedule. Online workshops also offered different ways of working, such as using breakout rooms or chat messaging to capture spontaneous thoughts, and some participants felt more comfortable contributing from their own home environment. It also meant we could engage a broader range of expert speakers, who could easily participate for short sessions without needing to give additional time for travel.

29 Hughes, T. (2020) 'Digital tools for participation: Where to start?', *Involve*. involve.org.uk. Available at: www.involve.org.uk/resources/blog/opinion/digital-tools-participation-where-start (Accessed: 23 February 2021).

30 Mckeon, A. (2020) 'Moving Online', *Traverse*. Available at: <https://traverse.ltd/moving-online> (Accessed: 23 February 2021).

Moving the format online required considerable thought in redesign, but ultimately presented a different way of conducting the workshops. The end result was a robust and rigorous deliberation, which produced an insightful set of recommendations. It is likely that the benefits and challenges offered by online engagement will continue to be understood, as public dialogue, engagement and deliberation projects continue while social distancing remains. Online participation will become a common method that practitioners opt to use even after the ability to meet in-person returns; there will be times where the qualities of online participation lend themselves to a particular topic or project.

Project delivery, oversight group and evaluation

The design and delivery of the Citizens' Biometrics Council was guided by an oversight group consisting of experts in: biometric technology, technology industry practices and policies, public attitudes towards technology, and responsible and trustworthy data use and technology (see [appendix](#)). The group gave advice on the topics and evidence discussed by the Council, the issues the Council should address, and on ensuring the process was balanced and robust. Some oversight group members also acted as expert speakers to the Council, and shared feedback on reporting.

The Council was delivered in partnership with public engagement specialists, Hopkins Van Mil (HVM). The Ada Lovelace Institute conceived the Council and developed its overall design and objectives, and commissioned HVM to act as a delivery partner, responsible for participant recruitment, project logistics and administration, workshop design and facilitation, and transcription. The Ada Lovelace Institute was responsible for researching materials, speakers and content, supporting workshop design, project management, analysis and reporting.

The project was also independently evaluated by Ursus Consulting, who observed workshops and planning meetings, and gathered feedback from participants, expert witnesses and other stakeholders. The evaluation aims to offer insight into the project to help understand the processes strengths, limitations and impact. The evaluation findings will be reported separately.

The Council's recommendations

The Citizens' Biometrics Council developed a set of recommendations in response to the question: **What is or isn't ok when it comes to the use of biometric technologies?**

These recommendations were developed at the end of the Council's 60 hours of deliberative workshops. In their final workshop, the Council members were asked to reflect on all the perspectives, evidence and topics they had considered throughout their deliberations, and develop recommendations for addressing the challenges raised by biometric technologies.

Rather than seek agreement from the entire Council on a small list of recommendations, these statements were developed through several smaller facilitated discussion groups to ensure each Council member had the space to reflect and contribute, and to ensure we captured the entire range of their ideas. Their recommendations should therefore not be seen as consensus, but instead a range of conclusions.

We present their recommendation statements here in full and in the Council members' own words.³¹

With feedback from a subset of Council members and the project oversight group, the Ada Lovelace Institute developed categories that group the recommendations according to where they overlap or converge around common themes.

31 We have made minor grammar and phrase edits for readability.

Category**Council recommendation**

Numbers correspond to the order recommendations were collated from Council member's workshop groups, and do not represent order of preference or hierarchy

Independent oversight body, legislation and regulation

1. Legislation should be created to define the boundaries of what is or isn't ok in the use of biometrics, and there should be a legal body which holds people accountable for breach.
2. An independent body should bring governance and oversight together. There are too many bodies currently all trying to do different things in this space. The independent body should have some ability to decide what's ok and what's not, through a licensing process that considers permission to collect certain data, why they are using the data, how it is stored, and that it won't be shared with other companies. There should be recompense when companies don't do the right thing, and the body must have some teeth (e.g. the Financial Conduct Authority).
3. There needs to be an independent body overseeing the development, implementation and legislation of biometric technologies and it needs to have all major players involved to create safe practices.
4. Until legislation is put in place and laws are set these biometric technologies shouldn't be rolled out on a large scale.
5. Strong legislation, The Biometrics Act 2020 set, these should be created and kept up to date (reviewed annually). It should include punitive measures – not just fines, i.e., someone could go to prison. All the data must be transparent, and able to be reviewed by the public – it must be published. There needs to be a framework for opt in/opt out. There need to be human accountability built into the system. As such we want to see a 'Biometrics Officer' in every company that's going to deal with the Ethics Committee (see recommendation 6) and be accountable.
6. We recommend establishing an Ethics Committee which sets out the ethical and moral framework for assessing all uses of biometric technologies including commercial use and advertising. Biometric data shouldn't be sold on by companies. The committee should have representatives from across society on it. Committee findings must be published.
7. Legislation should be developed with a diversity of perspectives and should have 'real teeth' to enforce penalties for breach of the law. E.g. the penalty for breach should be greater than the benefit of selling data to a third party. In order to ensure this occurs, neither business nor government should take the lead, but it should be co-developed with an independent panel/group, including members of the public.
8. A continually evolving framework of governance that includes a register to use biometric technologies, that is overseen by a broad representative group of individuals (and including public).
9. Governance standards need to be futureproofed – regular reviews written into new legislation to take into account new technology as it changes over time. Accurate now and reviewed to allow for adaptations to be kept current.

Data management

10. Data collection, storage and handling, length of storage are all important areas for consideration. Biometric information should be destroyed once a data subject leaves an organisation/ company; e.g. only held for as long as a person uses the gym/bank. Specific details could be broadly broken down in to three categories:
 - financial/private sector
 - regulation for police
 - general productivity (social media/mobile uses/going to the gym).
11. Increase data security to minimise chances of biometric data being stolen.
12. Improving data security is CRUCIAL before the usage of biometrics becomes even more widespread and mainstream, to reduce the risk of biometric data (that can't be changed, e.g. retinal scan) being stolen.
13. Commercial use: private companies shouldn't share data between themselves (e.g. Asda sharing with your gym: why?) to prevent them forming a bigger picture on you.

Proportionality across different contexts	<p>14. It is not ok when biometrics are used for social control. We aren't fully comfortable with immunity passports and linking biometric data to wider (government) control of our health history or status. But biometrics have a role in delivering individual care.</p> <p>15. Mixed views in its use in crime prevention. Use in crowds – CCTV outside a railway station – seems ok, but at an individual level (body-worn cams) disproportionately affects Black and ethnic minorities and that's not ok.</p> <p>16. National security use needs proper definition: use of biometrics is warranted, and may involve holding data on us – need to accept that, so some compromises may be necessary.</p>
Bias, discrimination and accuracy	<p>17. Increase accuracy in biometric technologies to 99% for police uses and at least 95% in other uses, to build trust and fairness into the technology. Diversity in software development should be highly encouraged. Increase data security to minimise chances of biometric data being stolen.</p> <p>18. Technologies should not be deployed if they are going to be inaccurate – they need to be accurate at the outset. Without this people will lose faith in the tech and its use. Trial it more thoroughly.</p> <p>19. Technology needs to be 100% accurate (concern about damage to individuals if it isn't).</p> <p>20. We need to prevent bias, discrimination and ensure it is inclusive for everyone.</p> <p>21. At an individual level (body-worn cams) biometrics disproportionately affect Black and ethnic minorities and that's not ok. Technologies are not up to scratch with people that have darker skin tones. 1) Remove all racial bias first – fix the technologies. 2) Then they can be taken for review to an Ethics Committee.</p> <p>22. Representative algorithms should be developed in biometric technologies to enhance accuracy and trust in the tech as much as possible. More representative datasets, and also a more diverse group of software developers, for example.</p>
Consent and opt out	<p>23. The sharing of biometric data should be restricted to certain circumstances, e.g. health/national security. In order to ask for consumer consent in other circumstances, an app/company/body needs to have permission from a verified, legal, independent body.</p> <p>24. In respect to private-sector use, consumers need to be able to opt in to biometrics being used. We need to provide consent. Different approach for public sector where there is a need for red lines.</p> <p>25. Ideally there would be a practical and fair opt-out system for people who don't want their biometrics used, with the possible exception of health/national security in certain contexts.</p> <p>26. It's not ok to use biometric technologies where informed consent is not at the heart of its design.</p> <p>27. There must be opt in consent which is clear and easy to give, there cannot be assumed consent. We need to know what happens with our data: clear explanations.</p>
Transparency	<p>28. We need to be confident that biometrics are being used properly. This involves accurate tech, public information and education, and more openness about how it is being used.</p> <p>29. It needs to be clear to every individual/citizen what information is held, for how long and in simple language. There needs to be education (for people using, developing it etc.) and we need to prevent bias, discrimination and ensure it is inclusive for everyone.</p> <p>30. All the data must be transparent, and able to be reviewed by the public – it must be published.</p> <p>31. Biometric technologies are ok as long as we know they're being used, and there is a method personally available to you to investigate their use.</p>

Council members were given space to weigh the complexities of biometric technologies, and consider what might be needed to ensure their use is responsible and to protect people from their irresponsible use

Findings: the Council's deliberations

Through the deliberative process the Council members became better informed about biometric technologies; how they work, where they are used, and the ethical implications, controversy and resistance arising from their deployment.

Council members were given space to weigh the complexities of biometric technologies, and consider what might be needed to ensure their use is responsible and to protect people from their irresponsible use. The Council's recommendations are a product of their informed deliberations, and reflect the breadth and depth of their enquiry.

Here we provide an analysis of the core themes the Council considered throughout their deliberation, to describe how the Council reached its conclusions and offer deeper understanding of the members' concerns and perspectives.³² This analysis does not supersede the Council's recommendations, but instead offers additional understanding of their perspectives.

The following is the Ada Lovelace Institute's interpretation, and should not be considered a definitive representation of the Council's perspectives. That is presented only through their quoted words and their recommendations.

32 For an example of approaches to thematic analysis, see: Attride-Stirling, J. (2001) 'Thematic networks: an analytic tool for qualitative research', *Qualitative research*, 1(3), pp. 385–405.

'We've got to be able to see the justification for using it.'

Purpose, justification and proportionality

A primary theme in the Council's deliberations was the purpose for which a biometric technology is deployed and who benefits from its use. Council members recognised the reasons motivating the deployment of biometric technologies, and considered varied scenarios where they may be used, such as to support policing and public safety, or enable identity verification and age estimation in online or socially distanced shops.

Many of these uses, like online identification or unlocking smartphones, were considered 'uncontroversial', and Council members understood and often agreed with or supported aims to improve public safety and security. But the Council also acknowledged the pluralistic nature of biometric technologies, in which they may simultaneously pose both benefits and risks, as the following quote from a Council member illustrates:

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

Privacy and surveillance

The Council considered seriously issues of over-surveillance and infringements on people's liberties and privacy. As well as references to 'big brother' and 'police states', Council members raised concerns about how other countries, both historically and in recent years, have oppressed people and diminished their privacy through surveillance. The phrase 'who watches the watchers' was raised more than once in their discussions.

Many Council members considered some loss of privacy through surveillance as a trade-off for living in a society which is kept safe from crime or other harms: 'If it's for national security reasons, and now COVID, then I'm not too bothered.' But they also recognised that trade-offs must be balanced carefully, and some rights must never be infringed. They were interested to hear about mechanisms to limit over-surveillance and privacy infringement, such as requirements for police watchlists and immediate data-deletion. However, many Council members questioned

the extent to which such mechanisms are currently used at the discretion of those deploying biometric technologies, and according to varying interpretations of existing law and regulation:

'It's in the interest of public safety, [but] to what lengths does the law permit the police to go to, to protect us, life, property? To what extent can they go?'

'This line, "the use of surveillance camera systems always specifies purpose in pursuit of a legitimate aim", which ties in with what [the expert speaker] said – that these people are only observed if they're on the list. But you could have anything on the list. They've said you're on the list, but what's on the list? I could be observed because I went to the Extinction Rebellion protests in London.'

Another trade-off the Council recognised was that the use of a biometric technology often does not affect just one individual, but groups of people and often the whole of society. Many participants considered the tensions this raised when the impacts on, benefits for and rights of different people are in opposition. For some participants, the collective benefit or the 'greater good' was a priority:

'There's a fine balance between people's rights and safety. Whenever the public safety of a group comes into question, that always overpowers other's rights because it's obviously for the safety of the public.'

'I know there's a lot about individual rights: You can't take my photo and I want this and I want that... But it's not always about you, it's also about everybody else around you.'

Council members were interested in ways to assist with navigating the tricky balancing of such competing interests. The question of 'who benefits?' emerged often, both explicitly and implicitly.

Who benefits?

When the interests of members of the public were the priority, using biometrics was often considered to be 'more ok' than when the interests of private actors were put first. This was particularly clear in the Council's discussions after the lockdowns came into effect in the UK:

'There has to be a genuine need for it, in my opinion. With COVID, I've not heard anybody object to track and trace when I've been out in public. You either scan it or you give your details, because people can see that it's protecting the public.'

In addition to public safety and health, it was recognised that many biometric tools are used to offer better services. One example considered was a gym company that replaced its membership cards with a facial recognition system, leading one Council member to reflect that such systems make it 'easier to check in, as there's nothing worse than forgetting your code or your card to get into the gym. Whereas your face is always on you.' Unlocking mobile phones with 'face ID', voice or fingerprint was regarded as a similarly useful tool, particularly for people who may have difficulty typing.

However, participants were concerned with uses of biometrics where private organisations, government or other actors gained benefits at the expense of the public, or where people's rights were infringed. Some of these concerns centred around what happens to the data collected by biometrics systems.

'It depends on the context of the company, doesn't it? If it's a private business wanting to sell and market stuff like we've mentioned before, no I wouldn't be very pleased, but if it's being done for a particular reason that you think is positive, then I wouldn't mind my image being shared.'

'With the gym, it's just for sheer convenience. Don't get me wrong, it's handy but it's not like it's going to make the process that much quicker. It just feels like an extra layer that doesn't make that much difference, but all of a sudden [the gym have] got all this very personal information, and gym companies aren't renowned for their data security.'

'What is it going to be used for? Obviously, if it's for security, fine. But I think someone talked in the last webinar about how there's a lot of data on our Tesco Clubcard and that is really more useful for people to hack into and use against us.'

The Council calls for clearer consensus around what constitutes a proportionate use of biometrics

In addition to being less comfortable about uses that don't have a clear benefit for the public, some also considered that certain uses of biometrics were just simply inappropriate:

'It just feels like a bit of overkill – it is there to prevent fraud and prevent crime, but I think there's probably other measures that could be done, that don't need to use biometric data.'

The Council also considered how uses of biometrics that seem more beneficial, or even benign, could act as gateways to rolling out more controversial uses with less resistance, as the 'acceptance' of biometric technologies would become normalised.

Many of these discussions reflected questions about where and when the use of biometrics is acceptable, how those uses are justified, and what mechanisms exist to ensure proportionality and prevent uses which stretch beyond those limits. Ultimately, these are questions of whether biometrics are needed or not, and who gets to decide.

The Council's recommendations address these questions by calling for clearer consensus around what constitutes a proportionate use of biometrics, the prioritisation of public benefit over commercial or political gains, and diverse public representation in agreeing what acting in the public interest looks like for uses of biometrics.

'I've got no more trust in this than I would in a small-town horoscope or a crystal ball, to be honest'

Choice, trust and transparency

Consent

Even where biometric technologies may be considered proportionate and justified, Council members recognised that their use would still need to be trustworthy, responsible and accountable. Consent was a prevalent theme in relation to this, and Council members often referred to the importance of choice in how biometric data about them is collected and used, citing the other kinds of consent options made commonplace by the GDPR, like cookie notices:

'I think allowing consumers to opt in is very important. If I have to opt in to accepting cookies for every webpage that I visit, I should certainly be able to opt in to having my face recognised.'

'Have you seen the feature on Facebook where it says, "Your friend's got a photo of you that you haven't tagged yourself in?" So Facebook has a copy of my face, they've used biometrics for that. I think it's mad that when I go on to whatever website, I have to opt in to cookies but I don't have option about whether to opt in to having my face shared. With biometrics, it's much more important. If we can do it with cookies, we can do it with faces.'

During their deliberations about consent, Council members considered that opportunities to opt in to a use of biometric technology wouldn't pose genuine choice or agency if opting out meant being denied access to a service or place, or being treated differently:

'There's an element of being made to feel uncomfortable on the opt out, so you've got to wait in a queue and "Oh, do you really want to do that?" So all of a sudden, we're making people feel uncomfortable.'

'[If you want to go to a restaurant during COVID], you either have to do the track and trace on your phone or you have to give written information. If you're not prepared to do it, then you're basically asked to leave. There is no choice there, but I think people accept that this is to try and keep us all safe and protect us.'

Council members also considered how offering consent in some circumstances posed practical and technical challenges, such as gathering consent in public places or assuming consent is given by virtue of participation:

'One of the things that really bugs me is this notion of consent: in reality [other] people determine how we give that consent, like you go into a space and by being there you've consented to this, this and this. So, consent is nothing when it's determined how you provide it.'

'So, entering a supermarket, you go to a self-service checkout, are you consenting for them to capture your image?'

'I think sometimes we do share information and quite naively don't realise that we are giving consent with, say, for instance, social media, and I think then you're getting into murky waters. Although, you could argue that yes, you've put it out there, you know it's out there.'

Council members also acknowledged that consent could undermine the effectiveness of deploying biometric tools in certain contexts, such as policing, where enabling everyone to opt in or out would mean that those intending to break the law would 'opt out of everything so the police just wouldn't be able to track [them].'

Recognising both the importance of consent and the practical challenges related to it, some Council members considered that different levels of consent are needed for different circumstances.

Where public health and safety is the goal, consent could be obtained by broad public consensus or approval – such as seen in the measures introduced to tackle the pandemic. Here public debate would be needed to understand what is acceptable, and uses must still meet expectations for proportionality with sufficient checks, balances and oversight in place.

Where biometric technologies are used in other settings without such 'high stakes', such as age verification in shops, fraud prevention or membership systems, Council members considered explicit consent mechanisms and adequate opt-out options for individuals to be necessary.

There was a strong sense that current information about how and where biometric technologies are used is 'woolly', 'unclear' and in some cases perhaps even 'deceptive'

Transparency

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

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

'You get those terms and conditions, really lengthy terms and conditions, I think that's not the way to go about it. Companies need to be more concise and open with what data they're taking and how they're going to use it.'

Improving transparency, for many Council members, requires going beyond the '10,000 pages of gobbledygook' that constitute many data privacy notices or terms and conditions, to provide clear, accessible, intelligible information about how biometric technologies are used, what data is collected and why. There was a strong sense that current information about how and where biometric technologies are used is 'woolly', 'unclear' and in some cases perhaps even 'deceptive'.

Council members expressed the need for the public to be provided with general information about biometric technologies, reflecting that greater digital literacy is needed to better equip people to navigate an increasingly digital world, and better understand how data is collected and used. For many, those deploying the technologies have a role to play in enabling transparent and accountable biometrics.

Transparency was considered as more than just good practice or a nice-to-have. It was considered a fundamental aspect of enabling people to feel they have more control over how their biometric data is used, how biometric technologies are deployed in society and how to hold those using them to account.

'The most important thing is to be able to query it, challenge it. Because I don't want to be misidentified. [...] If we all know what's going on, we can all be okay with it. If we don't really know what's going on, it just feels like Big Brother doesn't it?'

'No system
is going to be
100% accurate'

Bias and accuracy

Accuracy

The Council considered a range of evidence about the accuracy of biometric technologies. This included information about how biometric technologies aim to improve accurate identification of individuals in contexts where humans will usually perform the task of identification – often inaccurately and inefficiently.

However, while Council members recognised that digital tools do not get distracted or tired, as human ID-checkers might, they also considered research about how many facial recognition systems are systematically less accurate for minority ethnic groups such as Black and Asian people. They also considered examples of where real-world conditions can mean biometric systems do not perform as well 'in the wild' as they do 'in the lab'.

The accuracy of a biometric technology can be understood in a variety of ways. The Council heard from a number of experts who discussed technical aspects of how to measure and assess aspects like false positive or negative rates, or how thresholds for match probabilities can vary depending on the context. When discussing these aspects, Council members were interested in how technical accuracy can be improved, and considered that all efforts should be made to ensure accuracy of any biometric system.

Council members were concerned that inaccuracy – in whatever form – means technologies can cause erroneous or harmful outcomes. Many shared personal experiences where they, or someone they knew, had suffered because of a technical error. Throughout all their discussions, the Council was concerned with how inaccuracies and errors can cause harms and damage trust, a perspective highlighted by the pandemic:

The Council was concerned with how inaccuracies and errors can cause harms and damage trust

'These technologies shouldn't be deployed if they're bound to be inaccurate or imprecise, because it affects people's lives in so many different ways. If a technology's going to be deployed out there – say, the track and trace app – the Government has to be sure that it will deliver. [...] If it's not going to deliver then there is no point because it will just bring a lot more confusion and people might not believe in it.'

It was clear from the discussions, and in the Council's recommendations, that measures to minimise errors, and ensure people have the option to challenge outcomes and seek redress, would be fundamental to making biometric technologies acceptable. Or, in the words of one Council member, 'What we really, really need to have is a way of challenging false results.'

As part of this, many Council members felt that 'humans in the loop' would be crucial to not only minimising errors, but also enabling recourse:

'I think that the combination of human and technology is going to be safer, stronger, more resilient and robust, than either one or the other.'

'You need people that are trained in errors. When things go wrong – because you can't just say I'm sorry, I've got the wrong person – you need to actually explain what happened and be empathetic to the situation.'

Moreover, inaccurate technologies run the risk of damaging trust and confidence in the use of technology:

'It has to be accurate. If we hear stories that things are failing, things aren't working, then it's going to lose confidence with the general public, isn't it?'

While recognising that inaccurate technologies are a problem, some of the expert speakers posed a challenge to the Council: what if biometric technologies were completely accurate, meaning those using them for surveillance have even more powerful tools to do so?

Here, Council members largely felt little difference between biometric technologies that are accurate and those that are prone to error. In their view, all biometric technologies pose risks and require safeguards.

Some Council members considered inaccuracy and error to be so concerning that biometric technologies cannot be deployed unless they are completely accurate, articulated powerfully by one member of a Community Voices group who said: 'I don't see the point in it being 70% accurate, 80%. It's got to be 100%. That's going to stop mistakes happening and further issues.' Here, the link between accuracy and errors – or 'mistakes and further issues' – that negatively affect people is clear.

These sentiments around the need for accuracy and error minimisation are reflected throughout the recommendations made by the Council.

Identity, bias and discrimination

Much of the Council's concern around accuracy was in response to the disproportionate impact biometric technologies have on marginalised groups.

These disproportionate impacts occur when the technologies deployed reflect and amplify biases that can exist in unrepresentative datasets, be baked into poorly designed algorithms, or be prevalent in institutional and social norms. Council members heard how datasets used to train many facial recognition algorithms, for example, do not contain diverse representations of the populations they are then used on, which can lead to those algorithms performing less accurately for minority ethnic groups.

When those inaccuracies are combined with existing discrimination or prejudice in society and institutions, biometric technologies may exacerbate, not ameliorate the harms. Some Council members shared and discussed personal stories about how they have experienced discrimination or negative experiences through biases reflected or amplified by technology:

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

The Council raised many concerns about how institutional racism could be compounded by biometric technologies

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

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

For instance, for people who are transgender, 'incorrect medical data about their gender and sex can put them in danger'. Council members felt that biometric technologies pose similar risks for transgender people when they do not account for a spectrum of gender identities, particularly in countries with weaker equality laws or more discriminatory attitudes. Council members were particularly concerned to hear about unethical research using facial recognition and other biometrics to attempt to identify people according to their sexuality or target them because of their gender:³³

'Biometric technologies are fundamentally about bodies – what we do with them and how we allow them to be used. Queer bodies are often stigmatised and there is still a huge historic association with sin and moral transgression.'

Another injustice the Council were concerned about was structural and institutional racism. Here, some Council members appreciated the potential for technologies – if built and used correctly – to reduce human biases, for example in the action of powers like stop and search:

33 For more on the ethical concerns surrounding research using biometrics, see: Noorden, R. V. (2020) 'The ethical questions that haunt facial-recognition research', *Nature*, 587(7834), pp. 354–358. doi: [10.1038/d41586-020-03187-3](https://doi.org/10.1038/d41586-020-03187-3).

Many Council members expressed concern about 'one-size-fits-all' approaches to technology design

'We already have stop and search laws, which are very controversial. Certainly when they were introduced they were extremely unfair, and they have been abused by the police in a lot of ways. [...] How does facial recognition make the existence and the abuse of that law any worse? In fact, are there ways in which it could make it better: is it going to be as biased in the same way that human beings are?'

However, the Council raised many concerns about how institutional racism could be compounded by biometric technologies, particularly when they are less accurate for ethnic minorities:

'The system, and the information that goes in, is dependent on who is putting it in. If you've already got companies who have a racial bias, then the system is basically useless. Ultimately all you're doing is transferring a human bias into a computer. Before those kinds of things are implemented and put out into communities, race prejudice and discrimination needs to be sorted out.'

'It comes back to the trust, it's coming down to who is owning these companies who are collecting the data. Are they racist? Are they this, are they that?'

On policing powers like stop and search in particular, Council members implicitly acknowledged how technologies aren't used in isolation from a social and organisational structure, but are intertwined with it:³⁴

'For me, I think it's about trust. Stop and search has been abused over the years and to add on top of that – to have technology that supports stop and search – it's not going to make young black males trust the police anymore than they already do.'

For many Council members, whether or not biometric technologies would exacerbate or minimise discrimination and injustice depends on how they are designed, built and deployed. In addition to concerns about how social and institutional biases can be amplified through the use of technology, many Council members expressed concern about 'one-size-fits-all' approaches to technology design:

34 For more on how trust and technologies are embedded across socio-technical systems, see: Ada Lovelace Institute (2020) *No green lights, no red lines*. Available at: www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf (Accessed: 8 January 2021).

'I suffer with a syndrome called Guillain-Barré syndrome. For me, the fingerprint on your phones, I never get right. It's lucky I can put in my passcode because the fingerprint from my phone, it's never the same. It always changes. I also, and others like me, can get Bell's palsy, so facial recognition is a no-no as well.'

In these discussions, and throughout their deliberations, the Council considered the significant potential for biometric technologies to have disproportionate impacts on already marginalised communities. Accuracy, bias and discrimination are incredibly complex topics, and each can manifest and be understood in different ways depending on what biometric technology is used and how.

Council members recognised the motivations to use tools like facial and voice recognition to reduce bias or increase access. However, their deliberations and recommendations reflect that good motivations are not enough: they expect that biometric technologies must work for everyone, and must not unfairly disadvantage anyone.

'The key word for me was misuse'

Protections for people and data

Equalities and marginalised groups

Many of the expectations outlined in the Council's recommendations advocate for the importance of standards and protections. It is not enough to call for better accuracy and the reduction of bias if each developer or deployer of biometrics chooses for themselves what constitutes 'accurate' or 'unbiased'. The use of biometrics must adhere to widely agreed standards, not the values of any one group or organisation. One Council member expressed their disappointment that some technology companies cannot be relied on to demonstrate best practice:

'I would have hoped it would have been these huge corporate companies that saw it as a problem. That it was that one Black employee, and she was the only one who realised it was an issue, I thought that was pretty sad and alarming.'

For many Council members, the representation of a diverse range of perspectives needs to be included in not just the development of biometric technologies, but in the standards, governance and oversight relating to them

Many suggested that diverse datasets and developer teams should be the norm in an industry that develops these technologies, an idea which carried through in more than one of their recommendations.

However, some Council members, and particularly participants in the Community Voices workshops, acknowledged that sometimes standards aren't enough. This was reflected in discussions of how, without strong oversight, issues for marginalised groups can be overlooked.

This was exemplified even in the Council's deliberation itself, where the focus on some injustices was stronger than others. Members of the LGBTQI+ group highlighted that the discussion centred more on racial injustice than on the prejudice experienced by gay people or transgender people, for example. This may have been a consequence of the fact that much of the deliberation occurred while the Black Lives Matter protests were making headlines and very much on the minds of Council members. However, it may have also reflected a sense that:

'Some people are uncomfortable talking about LGBT issues. This is just an observation really about how hard it can be to raise issues in some communities, or issues can be received in silence. This is often how discrimination starts/is perpetuated.'

The difficulty in ensuring marginalised communities' perspectives are fully considered is highlighted by how, even in a process designed to specifically include those perspectives, 'it was never going to be fully possible to give time to challenging the implicit internal, often unconscious biases' that exist in society.

For many Council members, the representation of a diverse range of perspectives needs to be included in not just the development of biometric technologies, but in the standards, governance and oversight relating to them. Moreover, for those communities most at risk from the harms these technologies may pose, standards and oversight are not enough if they are not backed by law: 'Without that you aren't safe.'

Keeping biometric data secure was a serious concern for many

Data protection

Another concern where the Council had strong expectations for standards and protections was the management and governance of biometric data:

'The problem is you and I don't know where the data goes. That is the real issue, where the data goes. You stick your finger on some machine that reads it, but where does it go?'

In recent years, many people have become increasingly aware of, and knowledgeable about how data about people is collected and used by organisations for a range of purposes. Council members discussed how they suspect many of these uses do not benefit the data subject, but instead support commercial incentives, often at the expense of the data subject.

'You've got to remember, of all the systems you know about, the most valuable thing is the data. The technology isn't valuable, it's the data that is valuable.'

'Who has the data, how good is it and who has access to it? Can I trust them?'

'We have to assume as well that organisations do in fact sell, pass on and share information. So, we can't just say, "Oh, these ones are okay and those ones need to be controlled." They all need to be controlled.'

Council members also recognised the heightened sensitivity of biometric data, as it relates to unique and immutable characteristics, and is often used for high-stakes purposes like security and identification. Keeping biometric data secure was a serious concern for many:

'It's whether it's safe. We have a history of data going awry, either maliciously or otherwise.'

'If there was a data breach from the bank, if someone could have the raw data, my fingerprint, could they be able to replicate that electronically, and then utilise it on other websites? If it was to be hacked, would it still be safe?'

As with the protection of marginalised communities, Council members felt that the protection of biometric data should not be left to each organisation to determine for themselves, but instead would require standards and legislation. Though Council members recognised that many standards and laws for data protection already exist – the GDPR being the most prominent example – the recommendations reflect their discussions and expectations for stronger and more specific protections for biometric data.

'I feel that it's a double-edge sword. I think it's got huge potential, but we really need to think about how we control it and who has access to the data.'

Understanding what is and isn't ok

The Citizens' Biometrics Council deliberations covered the breadth, depth and complexity of issues relating to biometrics. Aside from the major themes discussed above, the Council also considered topics like scope creep, the perceived inevitability of some biometric technologies, the power dynamics between governments and corporations and individual citizens, and how the increasing use of surveillance and identification technologies can influence or 'nudge' people's behaviour, perhaps limiting their political participation or other liberties. There have also been themes, like trust and data protection, which have cut across many of the topics the Council discussed.

The Council members also considered and recognised the many benefits biometric technologies can bring, from improved services to better public safety. They saw why police forces and border security were exploring the use of facial recognition, why banks are using voice recognition and other biometrics to tackle fraud, and why supermarkets are turning to biometrics to provide services like age-checking in an increasingly contactless society.

Ultimately though, the Council's focus was on how to balance the opportunities of biometrics with the risks. Throughout their deliberations, the Citizens' Biometrics Council recognised that this is a far from straightforward task. The solution to this challenge, they felt, would require more than ideas like sweeping bans or relying on incremental existing governance and oversight.

Ultimately, the Council's focus was on how to balance the opportunities of biometrics with the risks

The interconnected nature of the themes the Council explored shows how complex and 'wicked' a problem biometrics pose.³⁵ Addressing one issue requires balancing complex trade-offs that have consequences on other challenges. In the figure below, we outline how some of the core themes relate to one another.

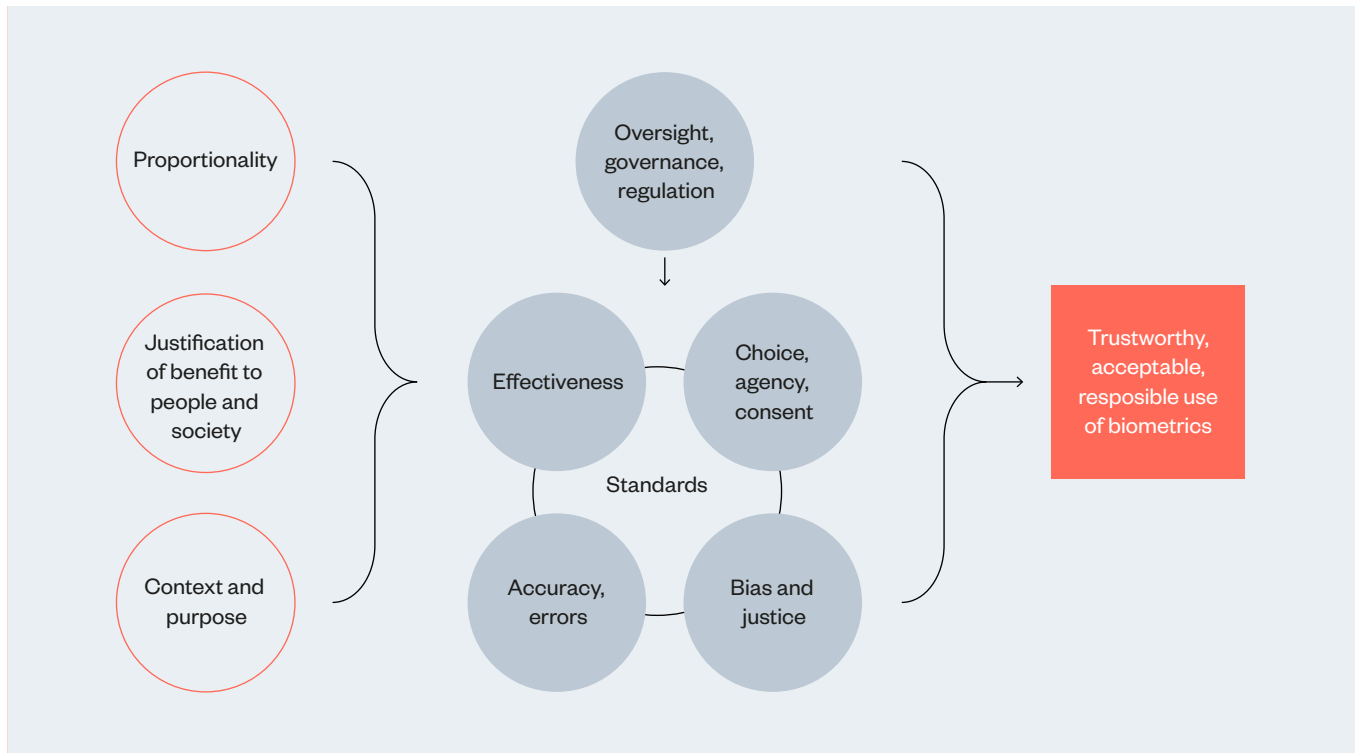


Image above

The core themes raised through the Council's deliberations show the way towards trustworthy, acceptable and responsible biometrics

³⁵ Churchman, C. West (1967). 'Wicked Problems'. *Management Science*. 14 (4): B-141–B-146. doi: [10.1287/mnsc.14.4.B141](https://doi.org/10.1287/mnsc.14.4.B141)

The Ada Lovelace Institute identifies three clear clusters that the Council's recommendations centre around

Conclusion: addressing the Council's recommendations

The Citizens' Biometrics Council's deliberations offer an in-depth understanding of what informed members of the public think makes the use of biometric data and technology responsible, trustworthy and proportionate. Their recommendations articulate their expectations, and what is required to enable acceptable uses and prevent unacceptable uses.

The Council's recommendations range from very specific ideas to broad expectations. This is appropriate, as the group's task was to express their informed opinions without being bound by any limitations.

Responding to such aspiring and broad recommendations poses practical and political challenges. The Ada Lovelace Institute identifies three clear clusters that the Council's recommendations centre around, which suggest the direction of travel that policymakers and practitioners must take to respond to the Councils' expectations:

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

These three areas were presented to the oversight group, the Community Voices groups and some of the Council members. Their feedback contributed to developing possible approaches for policy and practice to ensure the Citizens' Biometrics Council recommendations and expectations are addressed.

'It's remarkable really that everyone, without fail, that we've spoken to and heard from has said "This needs to be sorted." We need a framework and some legislation to provide oversight.'

The Council members articulated a clear expectation for more comprehensive legislation and regulation relating to biometrics in the UK

1. Legislation and regulation

The Council members articulated a clear expectation for more comprehensive legislation and regulation relating to biometrics in the UK. In their deliberations, they considered how current law has not 'kept pace with' the advances in technologies, creating grey areas for their lawful implementation, as well as gaps in the protections that ensure people's rights and prevent wider societal harms.

Through these recommendations, the Council expressed the desire that the UK Government must review and develop the governance relating to the use of biometric technologies and data. One Council recommendation calls for primary legislation: 'The Biometrics Act', while other expectations point towards secondary legislation, in the form of statutory codes of conduct or other rules created under existing acts such as the Data Protection Act 2018, or Equality Act 2010.

Whatever form it takes, the Council's recommendations articulate clear expectations for biometrics legislation and regulation:

- The law must cover biometric technologies and data comprehensively, across all contexts where they are deployed, not just law enforcement.
- Regulations must be designed with the input of a broad range of stakeholders, including members of the public and particularly those from marginalised groups.
- The law must be able to keep pace with rapid developments in technology. This could be achieved through adopting 'principles-based' legislation similar to the GDPR, supported by more specific and updated guidance or regulation.

The Council's recommendations for stronger regulation around biometric technology and data should be recognised by existing bodies that provide oversight of biometric data and technology, including the new Biometrics and Surveillance Camera Commissioner.³⁶

This new office, which combines the remits of two existing commissioners, should have a clear mandate to promote the

36 See: HM Governments Public Appointments, Biometrics and Surveillance Camera Commissioner. Available at: <https://publicappointments.cabinetoffice.gov.uk/appointment/biometrics-and-surveillance-camera-commissioner> (Accessed: 27 November 2020).

development of strong legislation around the use of biometrics, and not represent a weakening of regulation through the combined role.³⁷

The Council's recommendations for the need for clearer legislation and regulation are echoed by the independent legal review of current UK governance of biometric data, commissioned by the Ada Lovelace Institute and due to report in 2021, as well as our call for a moratorium on further deployments of facial recognition technology until adequate regulation exists.

2. Independent oversight authority

Many of the Council's recommendations express the expectation for a single, independent and authoritative body to provide oversight of the use of biometric technologies in the UK.

These recommendations respond to the evidence the Council heard about the currently fragmented oversight landscape for biometrics in the UK, as various offices and regulators provide different aspects of oversight in a manner that produces both overlapping remits and gaps. Council members expect a much clearer single point of oversight.

Council members also reflected that legislation, codes of conduct and other governance mechanisms will not be effective without enforcement, and people may not feel sufficiently protected without a body with the remit, authority and capacity to ensure biometric technologies are used in line with the law and with public expectations.

Such a body would need to fulfil a range of characteristics to meet the Council's expectations:

- It must represent a diverse cross-section of stakeholders, drawing on not only a range of expertise and sectors – from technologists to ethicists – but also including mechanisms for public participation and the involvement of marginalised groups.

³⁷ Rowe, S. and Jones, J. (2020) 'The Biometrics and Surveillance Camera Commissioner: streamlined or eroded oversight?'; *Ada Lovelace Institute*. Available at: www.adalovelaceinstitute.org/blog/biometrics-surveillance-camera-commissioner (Accessed: 12 January 2021).

- The body must have 'teeth' – the authority to hold actors to account through sanctions, fines or other mechanisms.
- It must be independent from financial or political influences which prevent it from acting in the interests of the public.
- The body should have the capacity to respond to complaints, carry out investigations, and the potential to perform ethical or legal reviews.
- The body should also have a remit which covers all uses of biometric technologies across public and private sectors.

To match all the Council's expectations, particularly around having the required authority, powers and independence, the body would require appointment by Government or another public institution, but given an independent remit.

Establishing a new body with the express remit to maintain legal, practical and ethical scrutiny over deployments of biometric technology raises a range of practical and political challenges, as well as potentially adding more noise, not clarity, to the oversight of biometrics use in the UK.

A more pragmatic approach lies in giving an existing body within the biometrics governance landscape the single authority, remit and resource to offer comprehensive ethical scrutiny and oversight. Such an opportunity is potentially posed by the incoming appointment of a combined Biometrics and Surveillance Camera Commissioner. This combined role offers an opportunity to meet the Council's expectations for a single point of oversight, if the new office is granted the appropriate powers and resource.

3. Minimum standards for the design and deployment of biometrics

Both legislation and regulation must ensure any biometric technologies are in line with the Council's expectations for what is responsible, trustworthy and proportionate. This can be addressed by the development of standards that biometric technologies must meet before they can be deployed in public settings.

Much like standards that assure the quality and safety of goods, minimum standards for the design and deployment of biometric technologies would ensure that biometric technologies, where

deployed, would be designed and deployed in line with the Council's recommendations. They would also prevent uses that fail to meet these standards, in effect prohibiting uses of biometrics that are not considered acceptable.

There are a range of considerations that standards for biometric technologies should cover to meet the Council's expectations:

- Biometric technologies must not create biased, discriminatory or unequal outcomes across the populations they affect.
- Inaccuracies and errors must be minimised as much as possible prior to deployment, not iteratively reduced after a technology is used in public.
- When used outside of public-sector settings, people must be offered mechanisms to consent to or opt into uses of biometric technologies, and be provided equal service or access if they choose not to.
- In addition to compliance with GDPR, standards for data protection and privacy, such as ISO 27001³⁸ should be adopted as a minimum starting point for good practice standards for managing and governing biometric data.
- Standard practices for transparency should make clear where and how any biometric technology is used, including accessible information such as what data is collected and how it's used, how people can consent or opt out (where necessary), and how they can challenge outcomes. Information about how proportionality has been justified must also be open to scrutiny.

This is a far from exhaustive list, and the Council recognised that though informed, they themselves should not be the sole authors of any list of design and deployment standards for biometrics. Rather, responsibility for developing standards for biometric technology should sit with the same independent authority advocated for by the Citizens' Biometrics Council.

38 International Organization for Standardization (no date) *ISO – ISO/IEC 27001 – Information security management*. Available at: www.iso.org/isoiec-27001-information-security.html (Accessed: 11 December 2020).

The principles informing these standards should be informed by broader public debate, and the standards themselves should be subject to a public review or appeal mechanism. Ultimately, any standards for the design and deployment of biometric technologies should be developed alongside legislation and should involve the input of a broad range of stakeholders, representing legal, technical, policy and ethical expertise, as well as a diverse cross-section of the public.

Public voice in the debate about biometrics

The Citizens' Biometrics Council is a crucial step towards bringing the voices and perspectives of informed members of the public to this debate

Public debate remains sorely needed to ensure biometric technologies are used for societal good and their harms are minimised. The Citizens' Biometrics Council is a crucial step towards bringing the voices and perspectives of informed members of the public to this debate.

The Council members have indicated a clear set of concerns and desires with regards to the use of biometrics, but among their key findings is that more work must be done to involve the public in the development of biometrics policy and responsible practice. Continued consultation with, and representation of, a diverse cross-section of society is fundamental to ensuring that biometric technologies are only deployed in a way that is trustworthy, responsible and acceptable.

As articulated by Council through the recommendations, their deliberations should represent the start, not the end, of public involvement in the development of biometric technologies and policies.

'If you put a frog into water, and you boil the water, it won't jump out. The water's boiling very slowly, and it doesn't detect that. A concern I have is, what if that represents the general population? What happens if, in 20 years' time, people don't realise what's happened until it's too late?'

Appendix

We are grateful to a number of colleagues for their time, expertise and supportive contributions to the Citizens' Biometrics Council.

Expert speakers:

Fieke Jansen Cardiff Data Justice Lab

Griff Ferris Big Brother Watch

Robin Pharoah Encounter Consulting

Julie Dawson Yoti

Ali Shah Information Commissioner's Office

Peter Brown Information Commissioner's Office

Zac Doffman Digital Barriers

Kenny Long Digital Barriers

Paul Wiles former Biometrics Commissioner

Tony Porter former Surveillance Camera Commissioner

Lindsey Chiswick Metropolitan Police Service

Rebecca Brown University of Oxford

Elliot Jones Ada Lovelace Institute

Tom McNeil West Midlands Police and Crime Commissioner's Office

Oversight group:

Ali Shah Information Commissioner's Office

Julie Dawson Yoti

Dr Jack Stilgoe UCL

Prof. Peter Fussey University of Essex

Lindsey Chiswick Metropolitan Police Service

Zara Rahman and Julia Keseru The Engine Room

Peer reviewers for this report:

Fieke Jansen Cardiff Data Justice Lab

Hetan Shah British Academy and Ada Lovelace Institute

Tom McNeil West Midlands Police and Crime Commissioner's Office

Lindsey Chiswick Metropolitan Police Service

Dr Jack Stilgoe UCL

Ed Bridges Cardiff University

Hopkins Van Mil:

Henrietta Hopkins

Suzannah Kinsella

Grace Evans

Sophie Reid

Mike King

Hally Ingram

Kathleen Bailey

URSUS Consulting:

Anna MacGillivray

The Citizens' Biometrics Council would not have taken place or been successful without the time, dedication and thoughtfulness of the Council members. We are incredibly grateful to all of them for taking part, and acknowledge by name those who gave us their permission:

Luisa H

Susan C

Rachel E

Tina D

Aaron T

Colin M

Elaine R

Ally B

Alistair C

Andrew T

Zoe E

Sue D

Kelvin H

Trevor A

Mary F

Sharon R

About the Ada Lovelace Institute

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

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

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

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

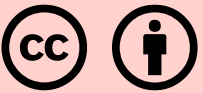
We are funded by the Nuffield Foundation, an independent charitable trust with a mission to advance social well-being. The Foundation funds research that informs social policy, primarily in education, welfare and justice. It also provides opportunities for young people to develop skills and confidence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

Find out more:

Website: adalovelaceinstitute.org

Twitter: [@AdaLovelaceInst](https://twitter.com/AdaLovelaceInst)

Email: hello@adalovelaceinstitute.org



Permission to share:

This document is published
under a creative commons
licence: CC-BY-4.0

ISBN 978-1-8382567-4-6