Ada Lovelace Institute

Report focus
This report summarises the main messages from a survey of public attitudes to the use of facial recognition technology in the UK.

Beyond face value: public attitudes to facial recognition technology

September 2019

Key messages

1. **Awareness of facial recognition technology is high, but knowledge about it is low**, particularly with respect to the limitations of the technology. This warrants a more informed public debate about the deployment of facial recognition technology.

2. **Consent is an important safeguard** for many people, with nearly half of the public expressing the belief that they should be able to opt out of, or consent to, facial recognition technology. In practice, this and other safeguards are often missing. There is a need to review and clarify the legal framework for facial recognition and ensure it keeps apace with public expectations.

3. **People fear the normalisation of surveillance**, but the majority support facial recognition technology when there is a **demonstrable public benefit** and there are appropriate safeguards in place, warranting greater investment in testing and articulating the potential public benefits of such technologies.

4. **There is no unconditional support for police to deploy facial recognition technology**: rather, support is conditional upon limitations and subject to appropriate safeguards.

5. **The public does not trust the private sector to use facial recognition technology** ethically, necessitating further dialogue between the public, private sector and policy-makers in order to understand and address this lack of trust.

6. **Companies and the government have a responsibility to act now**. The public expects the government to be placing limits on the use of facial recognition technology, including by the police, and supports companies pausing sales of the technology in the intervening time.

Introduction

Ubiquitous digital identification systems are no longer the realm of futuristic fantasy or dystopia. Facial recognition technology can now be found in airports, commercial premises, and on personal devices. Police forces are beginning to use facial recognition in criminal investigations as well as at events and in public spaces. Facial recognition systems are being developed for schools, public transport systems, workplaces and health care facilities.

In the UK, facial recognition technology has become commonplace in some sectors: it has been used in airports at ePassport border security gates since 2008,[1] and there are plans to deploy it in place of check-in and passport checks at Heathrow Airport.[2] Central London shopping and business district Kings Cross has been monitored using CCTV systems equipped with facial recognition, and financial services hub Canary Wharf is considering installing facial recognition across its 97-acre estate.[3]

More speculative use cases have been trialled or proposed: some UK schools have trialled adopting facial recognition technology for pupil registrations,[4] and the deployment of facial recognition in place of ticketing has been mooted for public transport systems.[5] HireVue, a US company with London offices, offers facial recognition technology applied to video interviews, analysing word choice, tone and facial movement[6] and is used by companies such as Unilever, Vodafone and IKEA.[7]

There is an increasingly pressing public debate in Britain about the ethics of facial recognition technology. Police trials of facial recognition technology in public spaces in London and Wales have been met with vocal uproar[8] and legal challenge[9], while revelations about the use of facial recognition in central London districts and shopping centres prompted regulatory investigation[10] and political criticism.[11] Anxieties about the absence of proper public consultation on the introduction of the technology are central to much of the opposition to the roll out of facial recognition systems. These raise concerns about the lack of a fit-for-purpose policy and legal framework to ensure facial recognition and other biometric technologies are used in ways that are consistent with legal safeguards and human rights. As the Metropolitan Police Commissioner Cressida Dick has argued, “there isn’t enough...

public discourse about what is acceptable and what isn't... It needs to be a political decision informed by what the public want...".[12]

It is against this backdrop that the Ada Lovelace Institute commissioned YouGov to undertake the first survey of its kind to understand public attitudes in the UK to the emerging public and private sector deployment of facial recognition technology. The survey covers a nationally representative sample of 4109 adults across the UK. It captures the UK public's initial response to a range of scenarios outlining specific applications of facial recognition technology in different sectors, for various purposes. You can read more about the research methods we deployed at the end of this report. We have also published the quantitative data that underpins this report.

The research shows that, despite knowledge about facial recognition being low across the UK, the public is developing nuanced opinions about the acceptability of facial recognition technologies, and the trade-offs it entails. The survey reveals public support for safeguards and government-imposed restrictions. Our findings call into question the assumption that police have carte blanche to adopt new technologies, and support efforts to review current legal and policy frameworks with a view to strengthening public consultation and consent mechanisms to build trust and increase the public legitimacy of biometric technologies.

This report summarises the key messages from the survey, identifying six main messages for policy-makers, public sector institutions and companies to consider. Key among those messages is a lesson for all stakeholders: public consultation and engagement must be a critical precursor to the adoption of data-driven technologies. Without involving the public in the design, deployment and evaluation of new technologies, we undermine their potential benefit, and threaten critical societal values as fundamental as human agency and democracy.

Facing the facts: the ethical concerns with facial recognition technologies

Accuracy
Trials of live facial recognition technology in policing contexts in the UK have reported more than 90% incorrect matches.[13] This exceptionally high error rate reflects the challenges of deploying the technology outside of controlled development environments. Much more work needs to be done to design and conduct rigorous field tests of live facial recognition technology in a range of policing contexts before the technology can be said to be fit for purpose.

Validity
The validity of some approaches to facial recognition technology is in doubt. Affective recognition is a subset of facial recognition that tries to identify people's emotions or personality traits from photographs or video. AI Now's 2018 Report connects affective recognition with physiognomy, "a pseudoscience that claims facial features can reveal innate aspects of our character or personality", which was widely dismissed by the research community as a means of scientific racism and discrimination.[14] There is a lack of evidence that affective recognition systems work across different people, contexts and cultures.[15]

Bias and discrimination
Facial recognition technology is typically worse at identifying women and people of colour, and is more likely to make inaccurate assessments of those same groups.[16] These limitations relate to concerns that the processes and datasets that support the development of facial recognition technology are not equally representing and responding to the diversity of society, and thus their use risks embedding problematic bias and inaccuracies for some groups in society more than others.

Transparency, privacy and trust
Facial recognition technology also raises questions of trust and transparency, privacy and autonomy. The technology has the potential to be deployed semi-covertly (on existing CCTV cameras), and pervasively. As the lines between public and private space become increasingly blurred, it is not clear to people how the technology works, when it is being used, and by whom it is being deployed. This not only undermines public trust in the technology, but also normalises surveillance and deprives individuals of agency when it comes to the privacy and protection of their personal data.

Security
Biometric data can reveal a range of intimate information about an individual and the context in which they live. The consequences of its misuse, abuse, loss, or theft are potentially more grave than the loss of other personal data – if one's bank details are stolen, they can be changed, but one can't easily change biometric data such as one's face or fingerprints.[17]

Key findings

1. Most people do not know enough about facial recognition technology to have an informed opinion on its use

The top line

Most people are not in a position to develop an informed opinion on the deployment of facial recognition technology. Although most are aware of the use of technology in the UK (90%), when pressed, only 53% say they know something about it.

The details

- **Awareness of facial recognition technology is high, but knowledge about it is low.**

  While 90% of people are aware of the use of facial recognition technologies in the UK, few people claim to have any deep or informed knowledge of the technology.[18] For instance, very few people surveyed are aware that facial recognition technology is being used outside of policing and airports: less than 15% of people know that facial recognition technology is being used in some workplaces, shops and commercial premises.[19]

- **There are many assumptions about the reliability and accuracy of the technology.**

  There are also low levels of knowledge and understanding about the technical limitations of the technology. When asked, for example, why they are comfortable with the police using facial recognition technology:

  — 24% say that the technology used by police is indiscriminate e.g. by race or gender;
  — 18% say it is accurate.[20]

What does this tell us?

Low levels of public knowledge matter. They limit the public's ability to engage in an informed debate about the benefits and risks of these emerging technologies. **Further public engagement and education would strengthen the democratic basis for new technologies** such as facial recognition technology, while empowering individuals to take an informed stance on the issue.

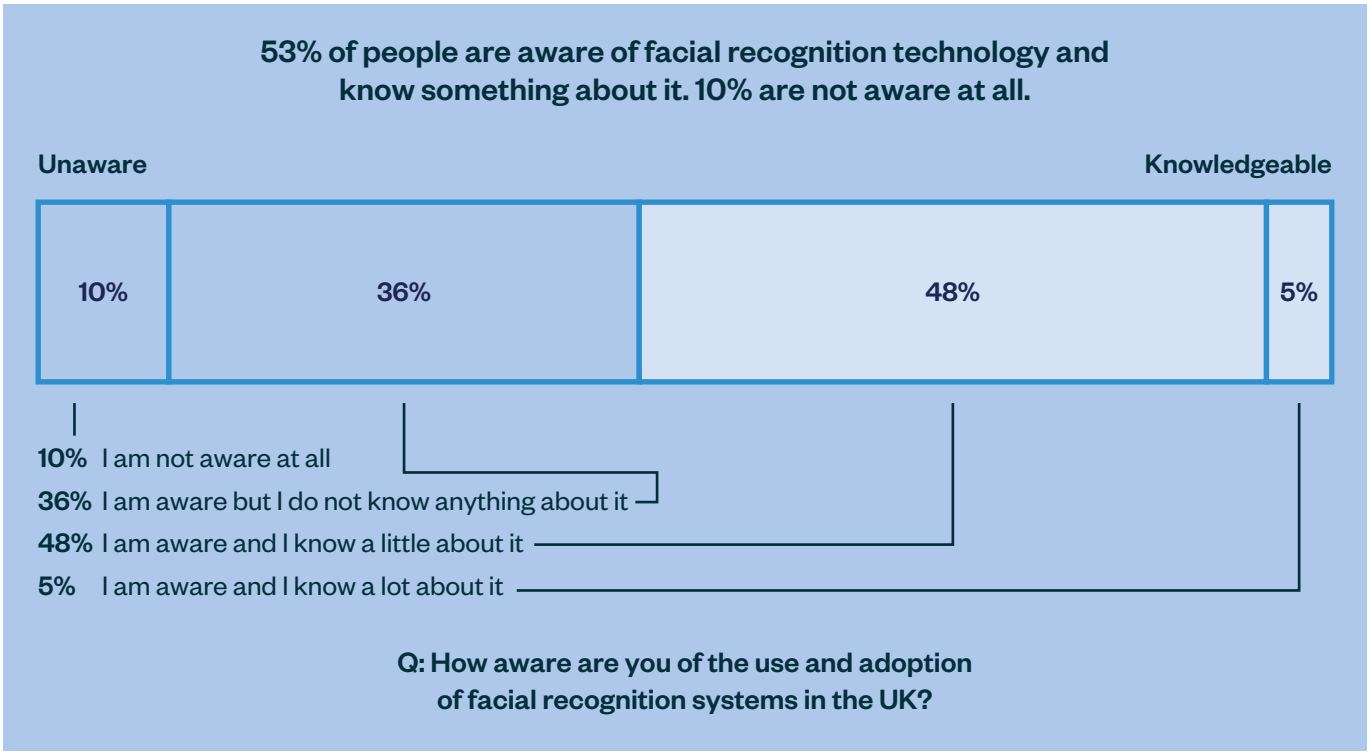

53% of people are aware of facial recognition technology and know something about it. 10% are not aware at all.
Unaware
Knowledgeable
10%
36%
48%
5%
10% I am not aware at all
36% I am aware but I do not know anything about it
48% I am aware and I know a little about it
5% I am aware and I know a lot about it
Q: How aware are you of the use and adoption of facial recognition systems in the UK?

Figure 1

2. The ability to consent to, or opt out of, facial recognition technology is an important safeguard

The top line

Nearly half (46%) the population think they should be able to consent to, or opt out of, the use of facial recognition technology.

The details

- **Consent and/or being able to opt out matters.**

  People place considerable importance on being able to consent to, or opt out of, facial recognition technologies. More people agree (46%) than disagree (28%) that the public should be given the opportunity to consent or opt out of being subjected to facial recognition technology.[21]

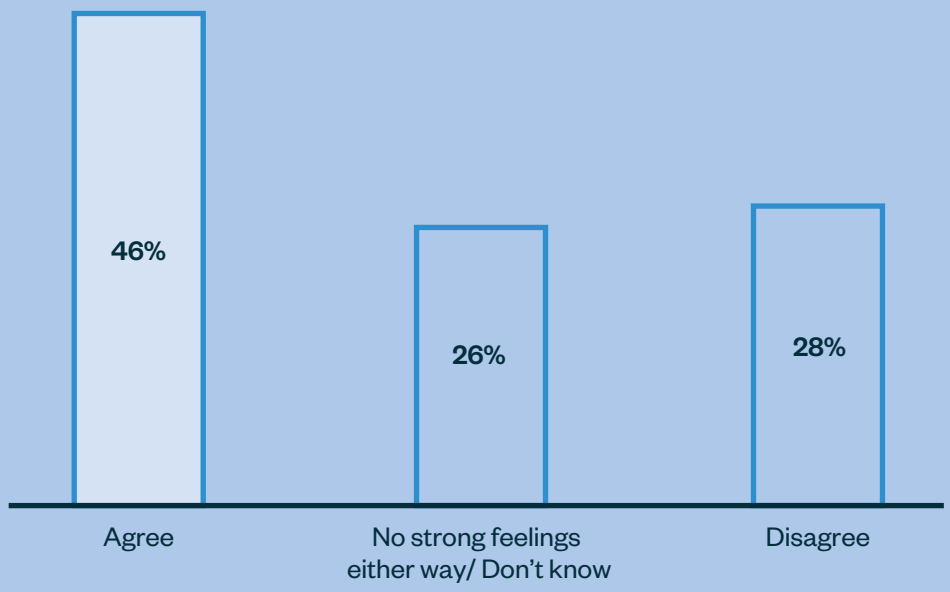
- **Consent and/or being able to opt out matters even more to ethnic minorities, for whom the technology is less accurate.**

  Survey respondents from black, Asian and minority ethnic (BAME) groups are more likely to agree with the notion that the public should have the opportunity to consent (56% of BAME respondents versus 46% of all respondents).[22] People of colour are more likely to be subject to the established problems with facial recognition in policing systems, such as inaccuracy or discrimination.[23]

What does this tell us?

When it comes to consent, **there are problematic gaps between current practice, what the public expect, and what the law prescribes**. As the Information Commissioner's Office has confirmed, data protection law applies to facial recognition technology.[24] Whether or not the deployment of facial recognition technology is subject to an individual's consent depends on numerous factors, such as whether it is being used to uniquely identify an individual, or whether it is being used by police and for what function. There is a disjointed legal and policy framework in the UK which has not yet established overarching rules around the use of biometric technologies such as facial recognition. Even if the public expect they should be given the opportunity to consent to facial recognition technology, this may not always be what the law requires, especially when the tech is being used by the police. **As such, there is a need to review and clarify the legal framework and ensure it keeps apace both with changes in technology and public expectations.**

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



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

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

Figure 2

3. People fear the normalisation of surveillance, but will accept facial recognition technology when there is a clear public benefit

The top line

People are concerned about the normalisation of surveillance as a result of increased use of facial recognition, but are inclined to accept the trade-off when facial recognition technologies serve a demonstrable public benefit.

The details

- Most people think facial recognition technologies should be permitted for use by police in criminal investigations (70%), on smartphones for locking systems (54%), and in airports to replace passports (50%), assuming appropriate safeguards are in place.[25] In a policing scenario presented to survey respondents, 80% of those comfortable with the use case say this is because it is beneficial for the security of society.[26]

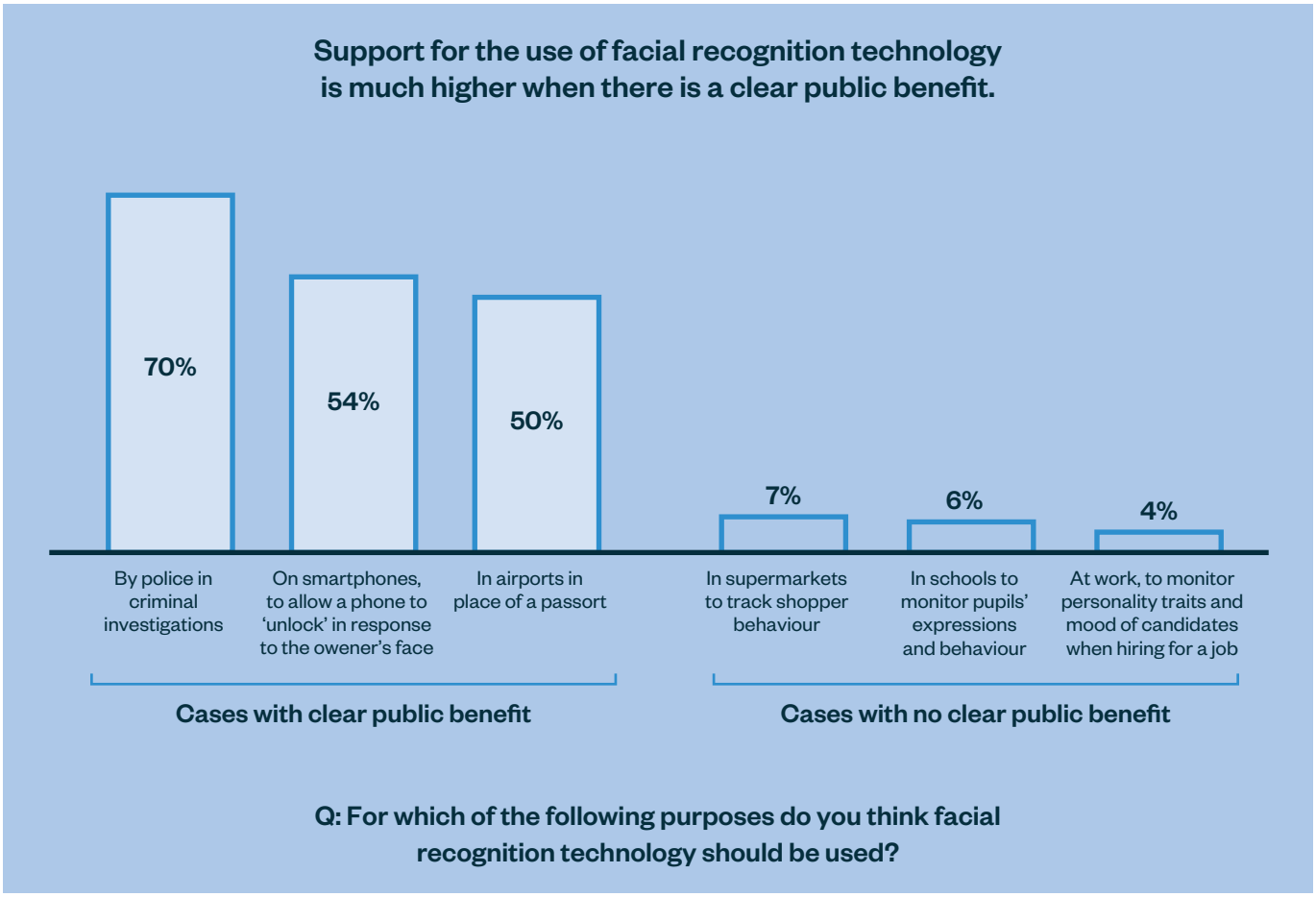


Figure 3

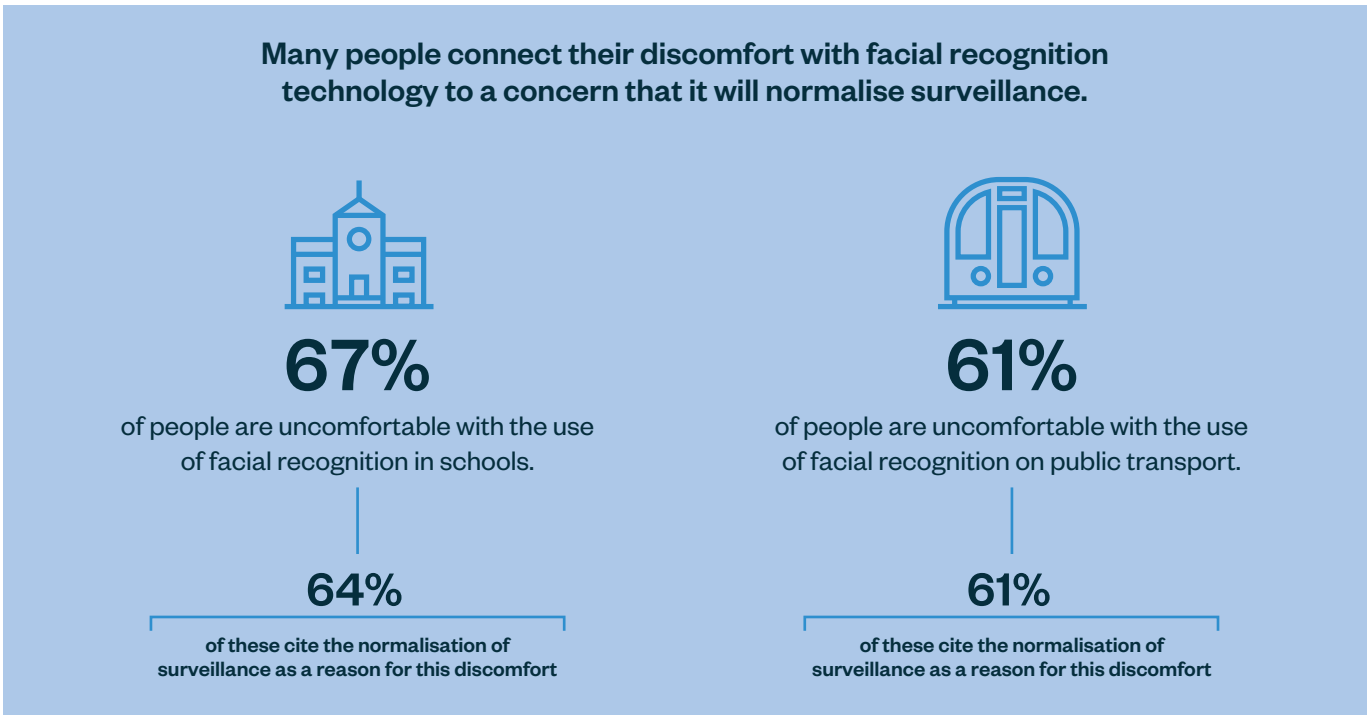


Figure 3.1

- **Despite potential public benefits, people are concerned about the normalisation of surveillance.**

  Although the public will accept the use of facial recognition technologies where there is a clear public benefit, particularly to societal or personal security, there is public concern about the normalisation of surveillance. Most people surveyed are uncomfortable with the idea that facial recognition technology could be used in schools (67%)[27] or on public transport (61%),[28] with a majority connecting their discomfort with the prospect that it will normalise surveillance (64% and 61% respectively).[29]

What does this tell us?

The public has identified **a trade-off between public benefit and the normalisation of surveillance** or reduction in privacy. In cases without a clear public benefit, people are less likely to feel comfortable with the use of facial recognition technology. This highlights the need for those developing and deploying facial recognition technology to take seriously the **need to consider these trade-offs, as well as to engage the wider public in understanding how to navigate them.**

Those commissioning and using these technologies should identify at design and planning stages whether the use reflects public expectations and norms. Tools such as public benefit audits and equalities impact assessments may assist public and private sector entities in evaluating trials of facial recognition technology and ensuring that there is broad social licence for its use.

4. There is no unconditional support for police to deploy facial recognition technology

The top line

The public's support for the police's use of facial recognition technology is limited to specific circumstances. The public expects safeguards to be in place and to see a demonstrable impact on reducing crime. Nearly one third of the public are uncomfortable with police use of facial recognition technology, and those voices need to be reflected in debate on policy and practice.

The details

- **The public expects government regulation, safeguards and limitations on police use of facial recognition technology.**

  Most people believe that the police should be able to use facial recognition technology, **assuming appropriate safeguards are in place.**[30] However, this support comes with significant caveats. The public feels differently about the police using facial recognition technology in different circumstances.[31] There is **majority support (55%) for government regulation to limit the use of facial recognition technology to specific circumstances.**[32]

55%

of people think the government should limit police use of facial recognition to specific circumstances

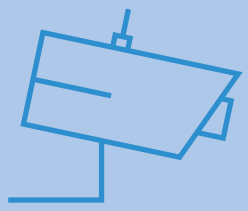


Figure 4

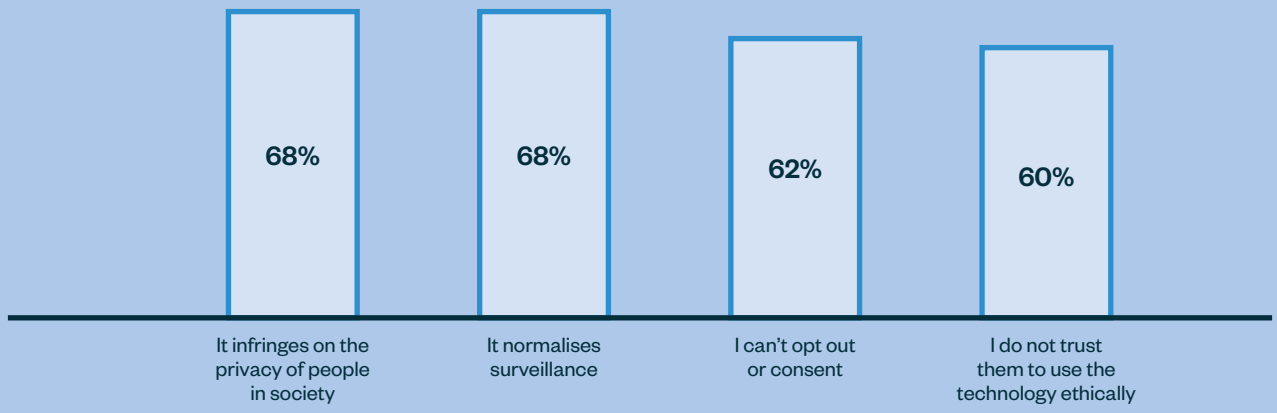
- **Public support for use of facial recognition technology in public spaces seems to be conditional on a demonstrable impact on reducing crime.**

  For instance, 71% agree with the statement 'The police should be able to use facial recognition technology on public spaces, provided it helps reduce crime'.[33]

- **Despite being in the minority, a significant number – nearly one-third (29%) – of people say they are uncomfortable when presented with a scenario of police use of facial recognition technology.**[34]

  The reasons they give for their discomfort include infringement of privacy (68%), normalisation of surveillance (68%), lack of opt out or consent (62%) and lack of trust in the police to use the technology ethically (60%).[35]

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



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

Figure 4.1

What does this tell us?

The police do not have unconditional approval to deploy facial recognition technology. The public expects facial recognition technology in policing to be accompanied by safeguards and linked to a public benefit. **Further public engagement, evaluation and regulation are needed to meet these expectations.**

Public approval of facial recognition technology varies by use case and impact on crime. **Each application of the technology requires its own public engagement process, trials and evidence base.** Regulation must consider the varied possible applications of the technology and seek to develop deeper understanding of public attitudes and views on specific scenarios.

It is important to note the extent to which the data illustrates how the public are not unified in their views on facial recognition and policing. Through commissioning this survey, we have identified the need to undertake further in-depth research to better understand concerns expressed by minority groups who report lower levels of comfort with this use case.[36]

5. The public does not trust the private sector to use facial recognition technology ethically

The top line

Most people are uncomfortable with the use of facial recognition technology by companies for commercial benefit. The main reason given for public discomfort is a lack of trust in companies to use the technology ethically.

The details

- **People are less comfortable with the use of facial recognition technologies when they are used for commercial benefit.**
  - Most people are uncomfortable with the prospect that facial recognition technology could be used by shops for tracking customers, or by human resource departments recruiting candidates for entry-level jobs (77% and 76% respectively).[37]
  - The reason for discomfort is that people do not trust companies to use the technology ethically (70% and 63% respectively).[38]

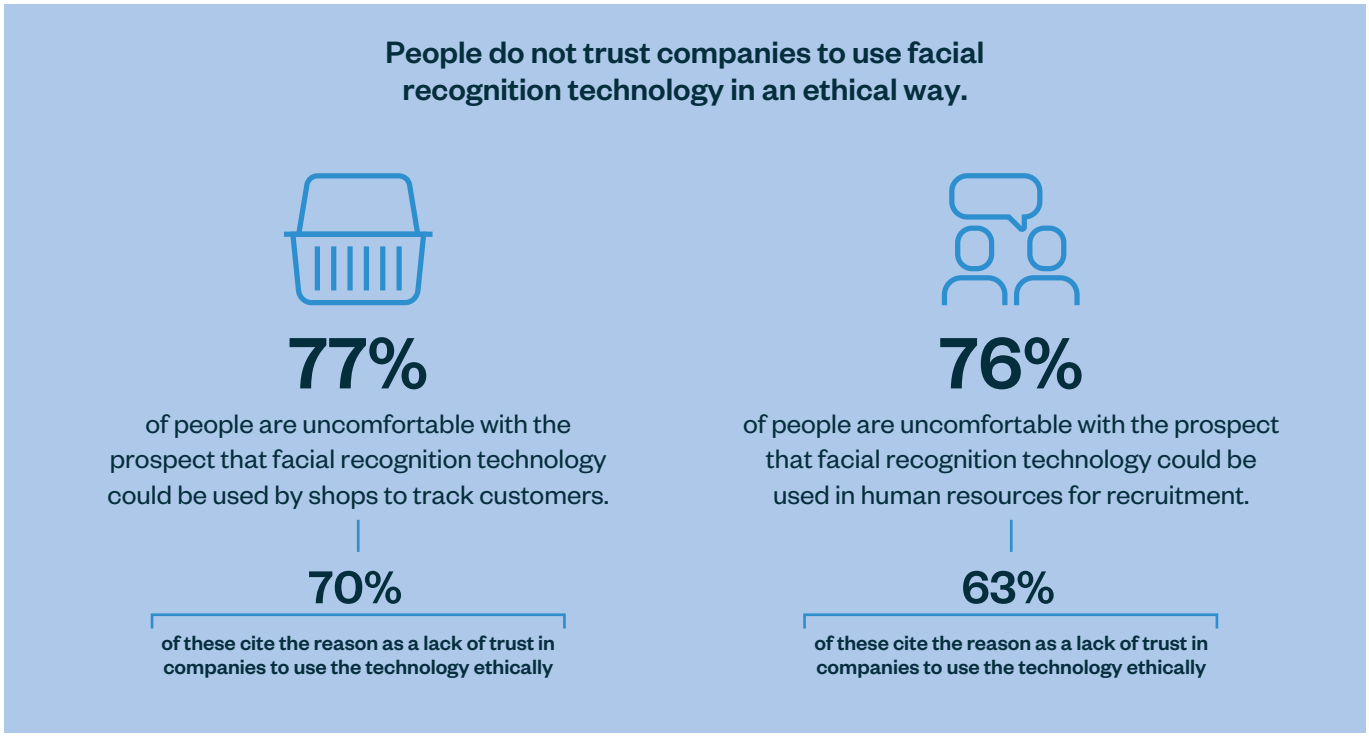


Figure 5

- **The purpose facial recognition technology serves matters to people.**

  When asked for which purposes facial recognition technology should be permitted, there are low levels of approval for use in supermarkets to track shopper behaviour, to verify age for alcohol purchases, or to monitor the personality traits of job applicants.[39]

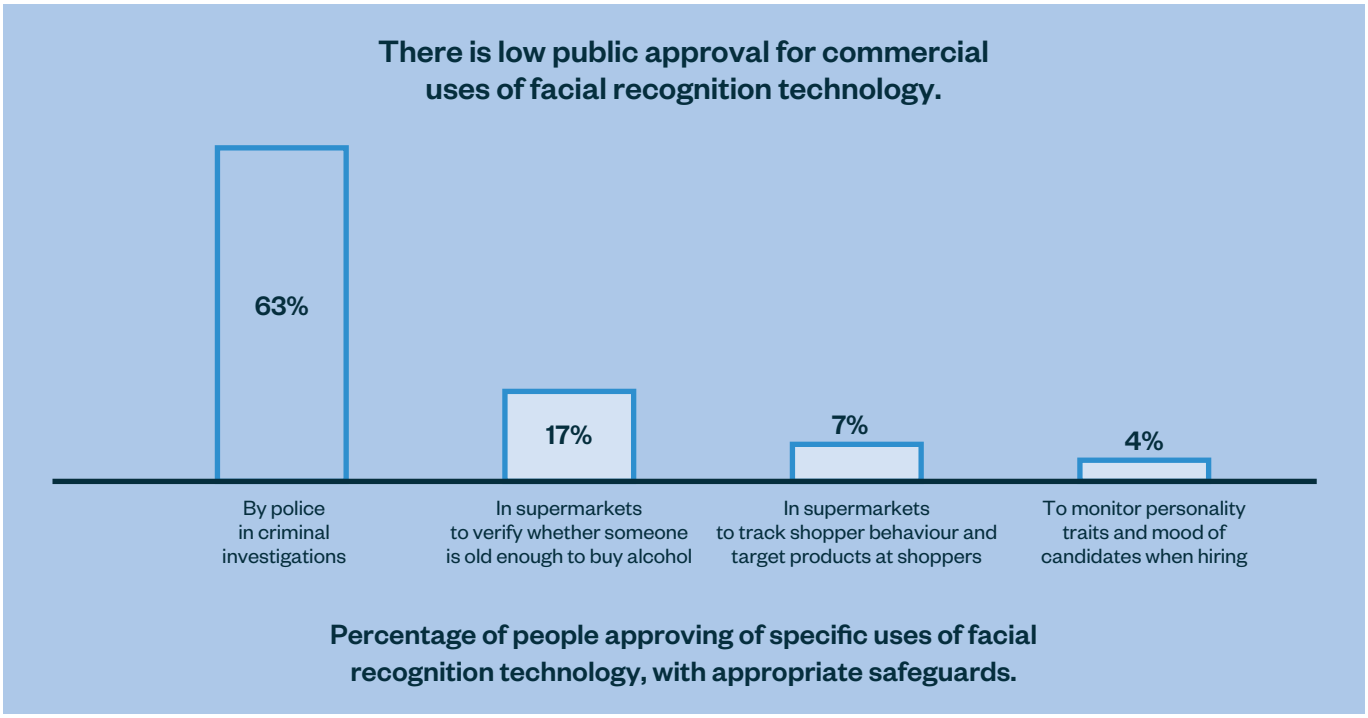


Figure 5.1

- **In general, there is limited awareness of the use of facial recognition technology for commercial benefit, compared to its use in policing.**

  The public show low awareness of commercial uses of facial recognition technology, with 14% aware of use in supermarkets to track shopper behaviour around the store and just 4% aware of use by workplaces to monitor personality traits and mood of candidates when hiring for a job.[40]

What does this tell us?

The public do not have confidence in commercial uses of facial recognition technology and are insufficiently informed about its use. **Further dialogue with the public, private sector and policy-makers is needed** to understand what is driving this lack of trust. Public deliberation would enable a richer dialogue, given the low levels of awareness of the use of facial recognition technology. Without awareness, it is hard for the public to raise concerns or be included in debate.

The low levels of support for commercial use are based on best-case scenarios where appropriate safeguards are in place. In practice, there are few safeguards or regulations governing these use cases. There is a lack of evidence about the effectiveness of some of these commercial uses and applications. For instance, many experts have expressed concerns about discrimination and the validity of the use of facial recognition technology in assessing emotions or personality traits.[41]

Recent high-profile cases of private sector deployments of facial recognition technology[42] further undermine public trust and highlight gaps in regulation of commercial use. This reiterates the **need to legislate in a manner that ensures trustworthy governance and use of biometrics technologies**.

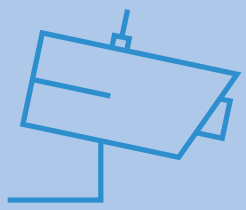
6. Companies and the government should act now

The top line

The public supports companies voluntarily pausing sales of facial recognition technology to police and schools to allow for further public consultation. Most people support government regulation to limit the use of facial recognition technology to specific circumstances.

The details

- **There is substantial public support for a voluntary undertaking by companies not to sell facial recognition technology to police or to schools for now, so that there can be public consultation.**
  - 50% of people agree the private sector should not sell the technology to police[43]
  - 70% of people agree the private sector should not sell the technology to schools[44]



50%

of people agree that the private sector should not sell facial recognition technology to the police

70%

of people agree that the private sector should not sell facial recognition technology to schools

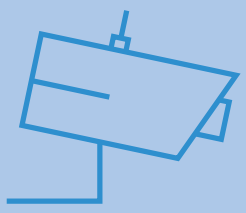
Figure 6

- **There is limited support for government to ban the use of facial recognition technologies.**

  For example, 65% disagree with a government ban on all facial recognition technology in policing.[45]

- However, the **majority support that the government should limit the use of facial recognition technology to specific circumstances**:
  - 55% of people agree the government should limit police use of facial recognition technology to specific circumstances[46]
  - 68% agree the government should limit schools' use of facial recognition technology[47]

- More people agree (40%) than disagree (30%) with the idea that the government should outlaw the use of facial recognition technology in schools.[48]



55%

of people agree the government should limit police use of facial recognition technology

68%

of people agree the government should limit schools' use of facial recognition technology

40%

VS

30%

More people agree than disagree that the government should outlaw the use of facial recognition technology in schools

Figure 6.1

What does this tell us?

There is considerable public support for a voluntary pause on the sale of facial recognition technology by industry, to ensure adequate public engagement and consultation is undertaken before its use. Companies and the government should act now to ensure that design, development and use of facial recognition technologies reflects public expectations and values.

In the face of a lack of trust in their ethical use of facial recognition technology, companies should consider whether to act on public support for a pause in the sale of this technology, as has previously been advocated by the House of Commons Science and Technology Select Committee[49] **and the Ada Lovelace Institute**.[50] This would enable further engagement with the public and the development of ethical and responsible regulation and practice for the use of facial recognition technology. It would also give companies an opportunity to address technical challenges of accuracy and discrimination, as well as identifying purposes that **provide public, not merely private, benefit**.

The government could use this voluntary moratorium period to develop governance and **legislation to limit use of facial recognition technology to specific circumstances** and to conduct **further dialogue** to establish, in cooperation with the public, what shape that should take.

Research methods

By exploring public attitudes to facial recognition technology under contrasting scenarios across the UK at large, the survey suggests a baseline from which public dialogues and discourse on regulation can be strengthened. Scenarios (listed opposite) were deliberately wide-ranging to obtain snapshots of attitudes and their underlying reasons.

4109 adults aged 16 and over in the UK responded to the online survey, administered by YouGov, between 12 and 16 July 2019. Perceiving that some groups would not be proportionately represented by the sampling method, and desiring as diverse as cohort as possible, we sought to reach a larger sample size than is standard in national opinion polls, of at least 4000 people. The national sample was weighted to the following UK demographics: gender, age, region and social grade. This meant that some other UK demographics were not fully captured, but could still be analysed. Black, Asian and minority ethnic groups (BAME) were under-represented (although still large enough in number for analysis), with an unweighted base size of 236 which forms 6% of the total survey response. Within the BAME response, there was a higher level of discomfort with police uses of facial recognition technology than the overall average. This will likely have significant implications for local areas with high minority populations, which are outside this survey's scope. We hope to conduct further exploration through future public engagement work.

The following brief definition was provided to introduce survey questions:

"Facial recognition technology is an emerging technology which aims to identify or observe individuals by detecting the features associated with a human face. The technology analyses and measures distances between specific facial features and generates a unique representation (a 'facial signature') of each human face.

This facial signature can then be compared against a database of stored images, in order to match it to similar images. Other types of facial recognition technology can assess the age of the individual whose face is being scanned or track their emotions and facial expressions. The technology can be used with the intent to uniquely identify individuals, although it sometimes has imperfections and does not always accurately identify individuals."

Respondents were given information about the proposed, potential or actual use of facial recognition technologies in the following cases:

Policing

— In criminal investigations, to identify suspects in CCTV footage from crime scenes

— In "day-to-day policing with the aim of reducing crime", at events such as football matches and carnivals

Schools

— In place of a "roll call", to register students as present in the school and in classrooms

— To monitor the facial expressions of pupils, and their behaviour

Companies

— To automatically monitor and analyse the facial expression and mood/personality traits of job candidates in videos that they submit

Supermarkets

— To track shoppers while in the store

— To uniquely identify shoppers and connect their movements to their loyalty card to help the store personalise its marketing to shoppers

Airports

— Instead of manual passport and boarding pass checks

Public transport

— In place of a rail pass or bank card, to identify everybody who is travelling on public transport and charge them accordingly

Access the results

The survey sought to look at public expectations of general use cases, reactions to specific scenarios, and expectations of government and of companies. Survey questions, results and analysis are provided on our website: **www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology**

References

[1] Home Office News Team. (2017). A history of the UK passport. [online] *Home Office in the Media*. Available at: https://homeofficemedia.blog.gov.uk/2017/12/22/a-history-of-the-uk-passport/ [Accessed 21 Aug. 2019]

[2] Heathrow Airport. (2018). Heathrow Airport launches first end-to-end facial recognition biometrics trial. [online] *Your Heathrow News*. Available at: https://your.heathrow.com/heathrow-airport-launches-first-end-to-end-facial-recognition-biometrics-trial/ [Accessed 21 Aug. 2019]

[3] Murgia, M. (2019). London's King's Cross uses facial recognition in security cameras. [online] *Financial Times*. Available at: https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c [Accessed 21 Aug. 2019]

[4] Levy, A. (2010) School installs £9,000 facial recognition cameras to stop students turning up late... [online] *The Daily Mail*. Available at: https://www.dailymail.co.uk/news/article-1317520/School-installs-9k-facial-recognition-cameras-stop-students-turning-late.html [Accessed 21 Aug. 2019]

[5] University of the West of England Bristol. (2017). 3D facial recognition technology on brink of commercial breakthrough. [online] University of the West of England Bristol News. Available at: https://info.uwe.ac.uk/news/UWENews/news.aspx?id=3630 [Accessed 21 Aug. 2019]

[6] Zetlin, M. (2018). AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews. [online] Inc. Available at: https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html [Accessed 21 Aug. 2019]

[7] HireVue. (2019). *Customers*. [online] Available at: https://www.hirevue.com/customers [Accessed 21 Aug. 2019]

[8] Big Brother Watch. (2018). *Face Off: the lawless growth of facial recognition in UK policing*. Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf [Accessed 21 Aug. 2019]

[9] Liberty. (2019) *Liberty client takes on police in ground-breaking facial recognition challenge – hearing opens today*. [online] Available at: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/liberty-client-takes-police-ground-breaking-facial-recognition [Accessed 21 Aug. 2019]

[10] Denham, E. (2019). *Statement: Live facial recognition technology in King's Cross. Information Commissioner's Office*. [online] Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/ [Accessed 21 Aug. 2019]

[11] BBC. (2019). London mayor quizzes King's Cross developer on facial recognition. [online] Available at: https://www.bbc.co.uk/news/technology-49343822 [Accessed 21 Aug. 2019]

[12] Cohen, C. (2019). Public expect police to be using facial recognition technology after seeing it in spy thrillers like James Bond, says Cressida Dick. [online] *The Telegraph*. Available at: https://www.telegraph.co.uk/news/2019/06/03/public-expect-police-using-facial-recognition-technology-seeing/

[13] Fussey, P and Daragh, M. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. [online] University of Essex Human Rights Centre. Available at: http://repository.essex.ac.uk/24946/ and Davies, B., Innes, M. and Dawson, A. (2018). An Evaluation of South Wales Police's Use of Automated Facial Recognition. [online] Cardiff University. Available at: https://crimeandsecurity.org/feed/afr [Accessed 21 Aug. 2019]

[14] AI Now Institute. (2018). *AI Now 2018 Report*. [online] Available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf [Accessed 20 Aug. 2019]

[15] AI Now Institute. (2018). *AI Now 2018 Report*. [online] Available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf [Accessed 20 Aug. 2019]

[16] Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, [online] Volume 81, p. 77–91. Available at: http://proceedings.mlr.press/v81/buolamwini18a.html [Accessed 20 Aug. 2019]

[17] Taylor, J. (2019) Major breach found in biometrics system used by banks, UK police and defence firms. [online] The Guardian. Available at: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms [Accessed 21 Aug. 2019]

[18] Q.5. Q: 'How aware are you of the use and adoption of facial recognition systems in the UK?' Base [unweighted]: all respondents (4109)

[19] Q.6. Q: *'In which of the following ways do you think facial recognition technology is currently being used in the UK?'* Base [unweighted]: all respondents (4109)

[20] Q.10, asked of the individuals who gave a score from 6 to 10 for a given policing scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are comfortable with police using facial recognition technology in this way, rating your level of comfort as [insert rating from previous question] out of 10. Which of the following are reasons why you are comfortable with this? Please select all that apply.'* Base [unweighted]: 2757

[21] Q.12, statement 6. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 6: 'The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology' Base [unweighted]: all respondents (4109)

[22] BAME is an acronym for black, Asian and minority ethnic. Q.12, statement 6. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 6: 'The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology' Base [unweighted]: BAME respondents (236), all respondents (4109)

[23] Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, [online] Volume 81, p. 77–91. Available at: http://proceedings.mlr.press/v81/buolamwini18a.html [Accessed 20 Aug. 2019]

[24] Denham, E. (2019). Blog: Live facial recognition technology – data protection law applies. *Information Commissioner's Office*. [online] Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/ [Accessed 21 Aug. 2019]

[25] Q.8. Q: *'And for which of the following purposes do you think the use of facial recognition technology should be permitted, assuming that appropriate safeguards are in place? Please select all that apply.'* Base [unweighted]: all respondents (4109)

[26] Q.10, asked of the individuals who gave a score from 6 to 10 for a given policing scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are comfortable with police using facial recognition technology in this way, rating your level of comfort as [insert rating from previous question] out of 10. Which of the following are reasons why you are comfortable with this? Please select all that apply.'* Base [unweighted]: 2757

[27] Q.19, with 'uncomfortable' referring to people scoring 1 to 5 on this question. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with schools using facial recognition technology in this way?'* Base [unweighted]: all respondents (4109)

[28] Q.16. 'Uncomfortable' referring to people scoring 1 to 5 on this question. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with your local public transport network using facial recognition technology in this way?'* Base [unweighted]: all respondents (4109)

[29] Q.21, asked of the individuals who gave a score from 1 to 5 for a given schools scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are uncomfortable with schools using facial recognition technology in this way, rating your level of comfort as [insert rating from Q19] out of 10. Which of the following are reasons why you are uncomfortable with this? Please select all that apply.'* Base [unweighted]: 2753 and Q.18, asked of the individuals who gave a score from 1 to 5 for a given public transport scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are uncomfortable with your local public transport network using facial recognition technology in this way, rating your level of comfort as [insert rating from Q16] out of 10. Which of the following are reasons why you are uncomfortable with this? Please select all that apply.'* Base [unweighted]: 2510

[30] 70% thought the use of facial recognition technology should be permitted for police in criminal investigations, assuming appropriate safeguards are in place, based on Q.8. Q: *'And for which of the following purposes do you think the use of facial recognition technology should be permitted, assuming that appropriate safeguards are in place? Please select all that apply.'* Base [unweighted]: all respondents (4109)

[31] Whilst 70% thought the use of facial recognition technology should be permitted for police in criminal investigations, only 49% thought it should be permitted for use in day-to-day policing. Q.8. Q: *'And for which of the following purposes do you think the use of facial recognition technology should be permitted, assuming that appropriate safeguards are in place? Please select all that apply.'* Base [unweighted]: all respondents (4109)

[32] Q.12, statement 2. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 2: 'The government should limit the use of facial recognition technology so that the police can only use it in some specific circumstances, like on CCTV footage from crime scenes.' Base [unweighted]: all respondents (4109)

[33] Q.12, statement 1. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 1: 'The police should be able to use

facial recognition technology on public spaces, provided it helps reduce crime.' Base [unweighted]: all respondents (4109)

[34] Q.9, with 'uncomfortable' referring to people scoring 1 to 5 on this question. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with police using facial recognition technology in this way?'* Base [unweighted]: all respondents (4109)

[35] Q.11, asked of the individuals who gave as score from 1 to 5 for a given policing scenario on a scale of 'not at all comfortable' (1) to 'extremely comfortable' (10). Q: *'You said that you are uncomfortable with the police using facial recognition technology in this way, rating your level of comfort as [insert rating from question 9] out of 10. Which of the following are reasons why you are uncomfortable with this? Please select all that apply.'* Base [unweighted]: 1180

[36] A majority of BAME (61%) and lesbian, gay (63%) or bisexual (57%) respondents still reported comfort with the policing scenario, but to a lesser extent in comparison with the whole public (67%). This is important to explore further to ensure that minority group views are understood, represented and considered when evaluating the use of these technologies in policing – particularly given historical inequalities and concerns around bias and discrimination in facial recognition technology itself. Based on responses to Q.9, with 'comfortable' referring to people scoring 6 to 10 on this question. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with police using facial recognition technology in this way?'* Base [unweighted]: BAME respondents (236), gay or lesbian respondents (204), bisexual respondents (182), all respondents (4109)

[37] Q.23, with 'uncomfortable' referring to people scoring 1 to 5 on this question in response to a supermarket scenario. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with supermarkets using facial recognition technology in this way?'* Base [unweighted]: all respondents (4109) and Q.26, with 'uncomfortable' referring to people scoring 1 to 5 on this question in response to an HR interview scenario. Q: *'On a scale of 1 to 10, where 1 is not at all comfortable and 10 is very comfortable, how comfortable are you with companies using facial recognition technology in this way?'* Base [unweighted]: all respondents (4109)

[38] Q.25, asked of the individuals who gave a score from 1 to 5 for a given supermarket scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are uncomfortable with supermarkets using facial recognition technology in this way, rating your level of comfort as [insert rating from Q19] out of 10. Which of the following are reasons why you are uncomfortable with this? Please select all that apply.'* Base [unweighted]: 3160 and Q.28, asked of the individuals who gave a score from 1 to 5 for a given HR interview scenario on a scale of 'not at all comfortable' (1) to 'very comfortable' (10). Q: *'You said that you are uncomfortable with companies using facial recognition technology in this way, rating your level of comfort as [insert rating from Q16] out of 10. Which of the following are reasons why you are uncomfortable with this? Please select all that apply.'* Base [unweighted]: 3144

[39] Q.8. Q: *'And for which of the following purposes do you think the use of facial recognition technology should be permitted, assuming that appropriate safeguards are in place? Please select all that apply.'* Base [unweighted]: all respondents (4109)

[40] Q.6. Q: *'In which of the following ways do you think facial recognition technology is currently being used in the UK?'* Base [unweighted]: all respondents (4109)

[41] AI Now Institute. (2018). *AI Now 2018 Report*. [online] Available at: https://ainowinstitute.org/AI_Now_2018_Report.pdf [Accessed 20 Aug. 2019]

[42] Murgia, M. (2019). London's King's Cross uses facial recognition in security cameras. [online] *Financial Times*. Available at: https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c [Accessed 21 Aug. 2019]

[43] Q.12, statement 4. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 4: 'Companies should promise not to sell facial recognition technology to the police for now, so that the public can be consulted about its use.' Base [unweighted]: all respondents (4109)

[44] Q.22, statement 2. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 2: 'Companies should promise not to sell facial recognition technology to schools for now, so that the public can be consulted about its use.' Base [unweighted]: all respondents (4109)

[45] Q.12, statement 3. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 3: 'The government should outlaw the use of facial recognition technology so it cannot be used in policing at all.' Base [unweighted]: all respondents (4109)

[46] Q.12, statement 2. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 2: 'The government should limit the use of facial recognition technology so that the police can only use it in some specific circumstances, like on CCTV footage from crime scenes.' Base [unweighted]: all respondents (4109)

[47] Q.22, statement 1. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 1: 'The government should limit the use of biometric technology so that schools can only use it in specific ways, for example in ways that do not support monitoring pupils' behaviour or emotions.' Base [unweighted]: all respondents (4109)

[48] Q.22, statement 5. Q: *'Please can you tell us how much you agree or disagree with the following statements?'*. Statement 5: 'The government should outlaw the use of facial recognition technology so it cannot be used in schools at all.' Base [unweighted]: all respondents (4109)

[49] House of Commons Science and Technology Committee. (2019). *The work of the Biometrics Commissioner and the Forensic Science Regulator. Nineteenth Report of Session 2017–19*. [online] Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf [Accessed 21 Aug. 2019]

[50] Kind, C. (2019). *Biometrics and facial recognition technology – where next? The Ada Lovelace Institute*. Available at: https://www.adalovelaceinstitute.org/biometrics-and-facial-recognition-technology-where-next/ [Accessed 21 Aug. 2019]

About the Ada Lovelace Institute

The Ada Lovelace Institute (Ada) is an independent research and deliberative body with a mission to ensure data and AI work for people and society.

Ada has three main aims:

1. Build evidence and foster rigorous research and debate on how data and AI affect people and society.
2. Convene diverse voices to create a shared understanding of the ethical issues arising from data and AI.
3. Define and inform good practice in the design and deployment of data and AI.

Ada 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, the Omidyar Network for Citizens and Governance, techUK and the Nuffield Council on Bioethics.

Ada is 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.

adalovelaceinstitute.org

@AdaLovelaceInst

Nuffield Foundation
28 Bedford Square
London WC1B 3JS

T: 020 7631 0566

Registered charity 206601