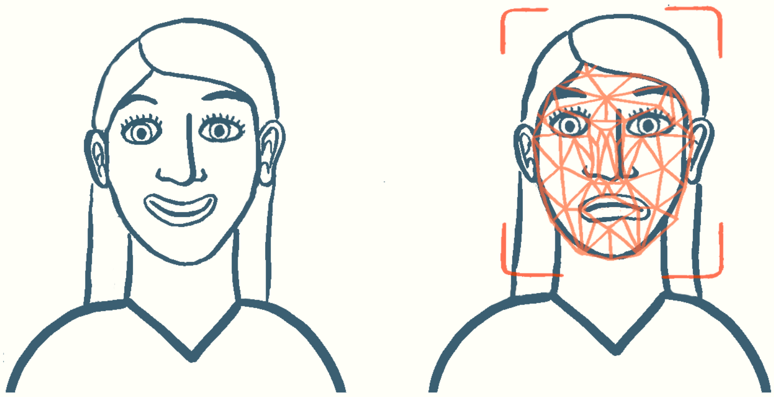
Responsible Facial Recognition Technologies

Doteveryone's perspective

Jacob Ohrvik-Stott and Catherine Miller
June 2019



Facial recognition technologies can be applied to many areas of society, from identity verification to the detection of criminals and missing people. But the technology is plagued by concerns around discrimination and bias, lack of accuracy and human rights violations. And an absence of accountability and regulation in the UK and globally means it's largely unscrutinised.

Doteveryone champions responsible technology. We advocate bold policymaking that will shape the impacts of technology on society and ensure technology works for more people more of the time. This paper discusses the challenges facing facial recognition technologies, outlines the current landscape for oversight and gives Doteveryone's perspective on how to make facial recognition technologies more responsible.

What is facial recognition?

Facial recognition technologies identify, categorise or verify people by analysing digital images of their faces. The most advanced forms typically use software and artificial intelligence (often trained on a large database of facial images) to map the features of an individual's face. This map can then be compared to a database for a match, or to categorise the individual on the basis of inferred characteristics such as age, gender, ethnicity or emotion.

Facial recognition has the potential to radically transform a wide range of sectors and services by automating and accelerating processes that rely on identification or verification - for example, streamlining airport customs enforcement, strengthening security of digital devices and enforcing age-restrictions on the purchasing of alcohol or social media use. Intelligence services and police forces around the world are also embracing facial recognition technologies with the aim of expanding their capabilities to detect suspected criminals and people of interest.

In 2018, police in New Delhi tracked down 3,000 missing children in four days with the help of facial recognition.[1] It can make it easier for farmers track errant livestock, guide historians trying to identify soldiers who died in war and help the visually impaired to read the expressions of people they interact with.[2]

Globally the facial recognition sector is predicted to grow to a value of nearly $9 billion by 2022.[3]

What are the concerns?

Facial recognition has been found to have significant technical failings and a worrying range of impacts on people's rights and freedom.

Some facial recognition technologies are being deployed despite **high levels of inaccuracy**. Eight trials of facial recognition conducted by police in London between 2016 and 2018 resulted in a 96 per cent rate of "false positives" – where software wrongly alerts police that a person passing through the scanning area matches a photo on the database - with two deployments reaching a 100% failure rate.[4]

Systems have been shown to have in-built **bias and discrimination**, for example research by MIT on Amazon's *Rekognition* software uncovered much higher error rates in classifying the gender of darker-skinned women than for lighter-skinned men.[5]

There is also a track-record of **privacy violations**. The photo storage company Ever recently caused outrage when it was revealed that it licenced its facial recognition technology to law enforcement agencies and the US military without users' explicit consent. And in March 2019, IBM were exposed for scraping over 1 million photos from Flickr to train their own facial recognition tools.[6]

Its widespread use has also caused concern about the **normalisation of hyper-surveillance of citizens**. Singapore plans to instal facial recognition technology into over 100,000 lamp-posts to keep tabs on the public and visitors, while in Shenzen, China, jaywalkers are shamed with projected images of their face onto a public screen.[7]

Facial recognition also has **potential to enable human rights abuses.** Big tech firms are competing to sell facial recognition surveillance systems to the UAE, where the technology has been described as "absolutely terrifying" by digital rights activist Sarah Aoun.[8] The Chinese government has used it to profile, track and persecute millions of Uighur Muslims.[9]

In the UK, police use of facial recognition has been strongly criticised for **lack of oversight** and violating the public's right to privacy and freedom of assembly on a mass scale. Recently, a man was fined for covering his face when passing a police facial recognition trial in East London.[10]

The civil liberties organisation Big Brother Watch has called facial recognition "authoritarian, dangerous and lawless."[11] And even the facial recognition companies themselves acknowledge these issues; Brian Brackeen, CEO of facial recognition software firm Kairos, warns that, "there's simply no way that [governments' deployment of] face recognition software will be not used to harm citizens."[12]

Oversight of facial recognition: a broken picture

In the UK, oversight of facial recognition is spread across a patchwork of organisations and legislation:

- **The Surveillance Camera Commissioner** (SCC) oversees the Surveillance Camera Code of Practice covering the use of surveillance cameras in public places. The Commissioner's role is to advise on technical standards for surveillance technologies and, in theory, educate the public around their use. Although local authorities and police must adhere to the code of practice (other organisations can sign up voluntarily), breaches are not currently punishable with legal penalties.

- **The Information Commissioner's Office** (ICO), the UK's data protection regulator, is responsible for ensuring that the data generated by facial recognition technologies, as well as the databases of facial images stored to aid their development and use, are used lawfully.

- **The Investigatory Powers Commissioner's Office** (IPCO) oversees the use of investigatory powers, including surveillance, by the UK's intelligence forces, police forces and other public authorities.

- **The Biometrics Commissioner** ensures that the police's retention and use of DNA and fingerprint remains within the bounds of the law - but currently has no responsibility for their use of facial recognition data, which are not currently covered by UK biometrics law.

In their 2018 Biometrics Strategy, the Home Office promised to review these laws, update the Surveillance Camera Code of Practice and establish a new advisory board to consider law enforcement's use of facial recognition systems.[13]

But despite, or perhaps because of, this proliferation of bodies and oversight initiatives the regulation of facial recognition in the UK remains fragmented and riddled with significant gaps.

In a recent parliamentary debate Darren Jones MP highlighted that "*the Biometrics Commissioner, the Surveillance Camera Commissioner and the Information Commissioner's Office have all said exactly the same thing—this biometrics strategy is not fit for purpose and needs to be done again.*"[14]

For the UK's public sector, the legal ambiguity surrounding the use of facial recognition has resulted in a disjointed system, where the lack of a national governance framework has left police forces and local authorities responsible for developing their own policies.

> *"I have been deeply concerned about the absence of national level coordination in assessing the privacy risks and a comprehensive governance framework to oversee facial recognition technology deployment"* - Elizabeth Denham, Information Commissioner[15]

This debate is also taking place in the US. Microsoft, the industry leader in facial recognition, called in 2018 for federal regulation of the technology[16] and the bipartisan Congressional House Oversight and Reform Committee has also demanded measures to restrict its use before "it gets out of control."[17]

Making facial recognition more responsible

Given the rapid adoption of facial recognition technologies, it's vital that policymakers move quickly to meet the challenges they pose. These are the key issues to be addressed and Doteveryone's recommendations for action.

What's the public view on facial recognition?

If, how and where facial recognition should be used are questions of values. Decisions around the trade-offs inherent in these technologies - where the benefits of their application must be weighed against a complex set of privacy, corporate and state surveillance and security risks - must be made democratically, and in line with the public's expectations.

In the UK these decisions are currently made by government, public authorities and corporate organisations alone and out of public sight. It's essential that future policies are founded on a considered and open public debate.

> *"We need a more open, public conversation about what types of [facial recognition] use cases we are comfortable with - and what types of use cases should just not be available"* - Rashida Richardson, AI Now Institute

This needs to be accompanied by a comprehensive and urgent review of the existing landscape for legislation that we outlined above, identifying where the gaps lie and where there is tension between the use of facial recognition and fundamental human and democratic rights.   This will need to address the different issues around private and public sector uses and separate technological issues around accuracy rates and bias from concerns about the contexts where facial recognition is deployed.

Within this, it's important to recognise that the technology is also not an inevitability.   The use of live, automated facial recognition on a mass-scale poses a serious threat to privacy and other rights. There is a case for saying that its use can never be justified within a democratic society.

And there needs to be consideration of how systems can be designed to be transparent and ensure individuals and groups can opt-out of facial recognition. Unilaterally imposing facial recognition systems on people risks irreparably breaking the public's trust in them.

Recommendations

1. **The Biometrics Advisory Council should lead a review of facial recognition legislation immediately.**
   This review should establish whether live use of automated facial recognition is ever compatible with human rights, be founded on extensive consultation and make recommendations on strengthening legislation relating to facial recognition for commercial and public sector uses. This review should inform the development of the code of practice outlined in recommendation 4 below.

2. **The ICO should lead a series of public dialogue events to explore the public's values towards facial recognition**.
   This engagement should inform the development of the code of practice outlined in recommendation 4 below.
3. **Place a moratorium on all uses of live automated facial recognition technologies until the legislation arising from the review is in place** - or permanently if the review and public consultation mentioned above find its use is not acceptable under any circumstances. With public confidence in government and facial recognition already low, continuing to use these technologies without safeguards could irrevocably damage trust.
4. **The ICO, Surveillance Camera Commissioner and Biometrics Commissioner should establish a joint Code of Practice for facial recognition**.
   This code should clearly set out where use of facial recognition is unlawful, as derived from the review and public consultations described in recommendations 1 & 2. It must be mandatory for all UK public sector authorities and commercial organisations, and should include:
    a. Clear guidance on where the use of facial recognition is not acceptable under any circumstances, and set out what (if anything) dictates "necessary and proportionate use" of facial recognition by police forces
    b. Powers for the lead regulator to audit facial recognition technologies and the facial image databases used to train them, and issue fines for non-compliance with the code
    c. Mandatory human rights impact assessments for all uses of facial recognition and reporting of locations where it is deployed
    d. Minimum standards for accuracy - applying to all demographics and protected characteristics
    e. Publicly-available transparency reporting for public sector facial recognition systems, including details on all locations where facial recognition is active, details on spending and companies public sector organisations purchase facial recognition from.
5. **The government should establish a one-stop-shop where individuals can seek advice on how to opt-out of facial recognition technology systems.**
   Individuals should be able to seek redress where these systems have been misused.

How should the UK's public sector be held accountable for their use of facial recognition?

In the UK, attempts to hold the public sector accountable for using facial recognition are being played out in the courts. The civil rights group Liberty are currently supporting a legal challenge against the South Wales Police brought by a man whose image was captured when shopping in Cardiff. [18]

The case will be an important first step in addressing the legal uncertainty around what - if anything - constitutes "proportionate & necessary" use of facial recognition by police. This ambiguity is emboldening police forces to experiment with facial recognition unchecked. With the public's trust in state institutions on the line the need for stronger oversight of facial recognition use in the public sector is particularly acute.

But with the legal system seemingly the only, rather than last, avenue for challenging the public sector's use of facial recognition the rest of the UK's institutions must catch-up. Parliament must no longer kick the can down the road when it comes to biometrics legislation, and regulators must be equipped to enforce it when these laws do come into play.

Doteveryone's *Regulating for Responsible Technology* research found that the UK's regulatory system lacks coordination, with many regulators slow-moving and lacking the resources and expertise to effectively respond to digital technologies.[19] Research by Accenture has found only 42% of British survey respondents are confident that the government would use artificial intelligence responsibly.[20]

The inadequate oversight of facial recognition reflects this wider landscape. Below we recommend reforms for ensuring regulation is flexible enough to respond to the future evolution of facial recognition technologies and inspires public trust.

Recommendations

6. **The Biometrics Advisory Council should lead the development of proposals for a governance framework for *all* public sector surveillance activities,** following the review of the existing legislation described in recommendation 1 above**.**
   The fragmented landscape of legislation for different surveillance activities is nonsensical and full of gaps. This framework will ensure legislation is consistent across different biometrics and surveillance activities, and ensure regulation remains relevant when future biometric and surveillance technologies inevitably emerge.

7. **Develop mandatory procurement policies for public sector organisations purchasing facial recognition technologies.**
   Based on the legislative review and public consulation outlined in recommendations 1 and 2, these policies should set out the minimum technical standards required to protect the public from discrimination and harm**,** and give guidance to ensure a fair exchange of value between public authorities and the private sector organisations developing facial recognition.

How can we encourage international action on facial recognition?

In a globalised digital economy, governments and local authorities routinely procure technologies from foreign entities. This can create tensions when technology is owned by organisations and states with different politics and values and poses risks to national security.

China has been accused of subsiding facial recognition and surveillance tech in developing countries to export norms of citizen hyper-surveillance.[21] The Chinese company Hikvision, is one of the main suppliers of surveillance cameras to Britain, including the Parliamentary estate.[22] And of course problematic facial recognition services developed in one country can be accessed globally - such as the tool developed by a Chinese programmer based in Germany to help paranoid partners check whether their girlfriends have ever acted in porn. The tool, predictably, does not work on men.

Encouraging responsible facial recognition on a global scale needs coordinated action and diplomacy to bring it about.

Cities in the US are already pressing ahead with their own regulatory reforms. In December 2018, Cambridge, Massachusetts, introduced rules requiring public agencies to seek City Council permission before buying, acquiring, or otherwise using new surveillance technologies.[23] Five months later San Francisco became the first American city to ban police forces and all other government agencies from using facial recognition.[24]

Our recommendations below outline how local authorities and international bodies can capitalise on this momentum and lead a global push towards more responsible facial recognition.

Recommendations

8. **Cities and local authorities should establish a Responsible Facial Recognition Technology Coalition.**
   This coalition would share learning around regulating facial recognition, and publicly commit to using the technology responsibly emulating initiative such as the Safe Face Pledge.[25]
9. **The United Nations should issue a General Comment on human rights in relation to facial recognition technologies.**
   This document should clarify how the UN Human Rights Convention applies to facial recognition, giving institutions guidance on how to avoid human rights abuses.

References

1. https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html
2. https://www.citylab.com/equity/2019/05/government-surveillance-tools-facial-recognition-privacy/588712/
3. https://www.marketwatch.com/press-release/facial-recognition-market-2019-company-profiles-industry-segments-global-trends-landscape-and-demand-by-forecast-to-2022-2019-01-14
4. https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html
5. http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf
6. https://www.theatlantic.com/technology/archive/2019/05/ever-strava-ai-human-ignorance/589306/
7. http://herdem.av.tr/gdpr-perspective-where-does-facial-recognition-stand-in-the-world/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
8. https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision
9. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
10. https://twitter.com/BBCClick/status/1127961872286789634
11. https://bigbrotherwatch.org.uk/all-media/big-brother-watch-response-to-planned-police-use-of-authoritarian-facial-recognition/
12. https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936
13. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf
14. https://hansard.parliament.uk/commons/2019-05-01/debates/16A45B3A-6F02-4542-B5F5-2146CA0C6AB8/FacialRecognitionAndTheBiometricsStrategy
15. https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology-and-law-enforcement/
16. https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/
17. https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control/?noredirect=on&utm_term=.821c29b560a9
18. https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/cardiff-man-gets-go-ahead-bring-first-uk-legal-challenge-police
19. https://doteveryone.org.uk/wp-content/uploads/2018/09/Regulation-Paper-Final-Version-Google-Docs-compressed.pdf
20. https://newsroom.accenture.com/news/citizen-comfort-with-ai-growing-accenture-study-shows.htm
21. https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/
22. https://theintercept.com/2019/04/09/hikvision-cameras-uk-parliament/
23. https://www.sfchronicle.com/bayarea/article/Oakland-considers-banning-facial-recognition-13826426.php?psid=4rZeQ
24. https://www.telegraph.co.uk/technology/2019/05/15/san-francisco-becomes-first-us-city-ban-police-facial-recognition/
25. https://www.safefacepledge.org/