The Foundation for Science and Technology
Debate Record Note

Facial Recognition and Biometrics: Technology and Ethics

Date and Location: 29th January 2020 at The Royal Society

Chair: The Baroness Kidron OBE, House of Lords

Speakers:
Carly Kind
Director, Ada Lovelace Institute
James Dipple-Johnstone
Deputy Commissioner, Information Commissioner's Office
Professor Carsten Maple
Professor of Cyber Systems Engineering and Deputy Pro Vice Chancellor, University of Warwick
Matthew Ryder QC, Matrix Chambers

Report Author: Dr Fay Bound-Alberti
Foundation Future Leader, FST and UKRI Future Leaders Fellow, University of York

Partner: The Ada Lovelace Institute

Audio/Video Files: www.foundation.org.uk
Hash tag: #biometricsdebate . Twitter Handle: @FoundSciTech .

THE BARONESS KIDRON OBE introduced the session by highlighting its importance and timeliness. In 2019 the House of Commons Science and Technology Committee published a report on biometrics and forensics in which it called for a moratorium on the current use of facial recognition technology until a legislative framework is introduced, with appropriate guidance and oversight. It called for an independent review of the legal framework. The intense concern for facial recognition technologies at different levels – public interest, safety, legislation and privacy – shows how fast-moving the landscape has become. Baroness Kidron expressed gratitude to the Foundation for Science and Technology and the Ada Lovelace Institute for convening the event.

CARLY KIND Ada Lovelace Institute extended her thanks to the Foundation for Science and Technology for partnering with the Ada Lovelace Institute, to Baroness Kidron and the other speakers. She began by introducing the Ada Lovelace Institute, a research institute and deliberative body, with a remit to ensure that AI works for people and society. Established in 2018 by the Nuffield Foundation, the Institute is an independent voice around the ethical and public impacts of data and AI, and to ensure the benefits are consistent with social justice and wellbeing.

The Ada Lovelace Institute began working on facial recognition technologies in summer 2019, with a media-reported proliferation of facial recognition technologies on the streets and more off-the-shelf products. From Hong Kong protests to police trials in Romford and South Wales, to India, China and the US, concern about facial recognition technologies erupted, along with a growing awareness of its ethical challenges.

There are three important issues to consider: the importance of a nuanced debate, the range of questions that we need to ask, and the process we should follow to answer them. The spectre of facial recognition technologies has grabbed the public attention but there are differences between phone technologies and that used by police, or that used in China, in India, and in Britain. It is different when used by supermarkets and by airports or the security services. It is different when used in historic ways by the police and when used to detect people in live time. There are different feelings involved as users of the software, and differences in the kinds of software available – that which uses facial recognition technologies to predict expressions and infer emotions, but doesn't store the data, compared to that which does store and uses it.

The origin of technology is important – such as the innovation of facial recognition technologies in China that is being used in particular ways – but the future is also important. We need to consider technologies now, as well as their unforeseen uses. What is critical at the heart of all these questions is: by whom, for whom and overseen by whom?

Research by the Ada Lovelace Institute found differences in public confidence and comfort in facial recognition technologies where used by public versus private authorities, in the public development/interest versus convenience or private sector. So it is important to separate all these different technologies and uses, which involve specific legal and social factors. It is problematic to speak in all or nothing, absolutist terms, as there are many social values at work. It hampers agency when decisions are seen as inevitable or there are no choices in when and how technology is deployed.

Historically, technology is deployed in answer to the question: what can we do? But a more relevant question is: what should we do? And whose interests should prevail? Who gets to answer that question? It is important to ask how good the technology is. Does it work? Is it biased? MIT Media Lab research has shown that inaccuracies exist when facial recognition technologies are used for women or people of colour. Concerns about accuracy abound, and the Met police acknowledge there is gender bias in the system.

The technologies are improving year on year, but false positives and bias is only part of the problem. Focusing exclusively on them risks obscuring other questions, including legality. Do facial recognition technologies meet the current regulatory frameworks and do we need new policy? Are facial recognition technologies effective at delivering intended outcomes and can this be independently verified? Are there other, less intrusive methods? Will facial recognition technologies harm certain groups? How will facial recognition technologies affect decision making and the use of public funds? And might they exacerbate existing structural inequalities?

Carly stressed that public legitimacy matters. How do we ensure facial recognition technologies are legitimate and trustworthy in the public eye? And what are the implications of normalising facial recognition technologies and surveillance? Does the approach we take map onto future biometrics technology, such as heart beat recognition or rapid DNA analysis?

Some of these questions will be answered by independent research and by legal cases brought by campaigning organisations. Others, the Ada Lovelace Institute will continue to address as an independent thinktank and research institute, including the commissioning of an independent review of the legal framework Chaired by Matthew Ryder QC. That review will be overseen by an advisory group drawn from people working in law, data protection, civil liberties, genomics, policing and digital identity. The Ada Lovelace Institute is also initiating a public deliberation initiative, called a Citizens Biometrics Council. Over three months, 60 members of the public will be consulted on questions like: what are the minimum necessary conditions to secure public trust in biometric technologies?

Carly concluded by saying that the Ada Lovelace Institute will continue to advocate for private companies to voluntarily pause further deployment of facial recognition technologies as the consultation and regulatory process is underway. Government use should also be paused pending further public consultation and legislative assessment in order to ensure trust and legitimacy in the use of facial recognition technologies.

JAMES DIPPLE-JOHNSTONE Information Commissioner's Office introduced the Information Commissioner's Office (ICO) as the UK's independent data protection authority, an organisation that fulfils several different functions: part investigator, part regulator, researcher, advisor and complaints-handler. He noted that the issues and challenges raised at this event are among the most important issues in the ICO's brief.

The UK's approach has been to investigate and observe the development of live facial recognition technology as it has emerged. By comparison with other areas of data protection, its arrival has been rapid and the pace has picked up over the past year. In 2019, the ICO concluded their first investigation into the theme, focusing on how police forces use facial recognition technologies in public spaces. It found support by the public in general, but also concern. The ICO concluded improvements were needed in how police authorise and deploy facial recognition technologies in order to ensure public confidence. These views were set out in the Information Commissioners Opinion (October 2019) into the regulation of the processing of personal data around law enforcement.

James noted that as the technology advances, the questions grow more complex. Moving on from police use of facial recognition technologies, decisions need to be made for commercial applications, where technology and data sets are also involved. And there is an important international context. Privacy authorities around the world are wrestling with the same questions, though drawing on their own legal and cultural traditions. How to share that learning and find synergies is part of the ICO's work.

Although facial recognition technology is being used throughout the UK, the ICO also sees a large number of organisations who are testing and considering its potential capabilities rather than using it routinely. So although the ICO's role principally concerns those who are using technology as part of their core business or at scale, it needs to be reactive to new ways of using the technology and innovation in the field.

Facial recognition technologies are a subject of public and media concern at the same time as organisations are launching new approaches. The ICO recognises the public safety implications of appropriately regulated, governed and deployed facial recognition technologies. So one of the questions under GDPR is around fairness. There needs to be a balance between privacy in everyday life and the surveillance needed for authorities to carry out their role. Weighing up the potential benefits and drawbacks for society is critical. To comply with the privacy rules, sound evidence is required from forces that the technology is strictly balanced, necessary and effective in each specific context (including addressing accusations of bias).

The question of fairness becomes a little different in the commercial context, where facial recognition technologies are principally used to improve customer service, make it easier to live our lives and reduce costs, but also to predict behaviour and make decisions in education and recruitment. The processes are not always transparent, so we need to consider how people in a retail place might expect facial recognition technologies to be used. How could that happen in a fair manner? How is the public data managed and handled in private and public duties?

Overall, facial recognition technologies can be attractive in helping organisations streamline their processes, give more accurate access and even support vulnerable groups, but these uses have to be lawful, necessary, justified and proportionate in order to ensure public confidence. In the 1970s, data protection emerged to meet the concern that society needed the confidence embrace technology. So it is not innovation or privacy that must be sought, but innovation with privacy. Privacy by design is at the heart of the Data Protection Act and applied in multiple contexts.

What does ICO expect as the regulator? A clear, lawful basis and where appropriate, transparency. Rigorous impact assessments are expected, including how data protection laws are met and implemented. The ICO is also able to sanction and enforce, including issuing financial penalties, in the case of serious interventions.

In addition to regulating, the ICO has been investigating public attitudes to facial recognition technologies. It found that 80 per cent of people approve of facial recognition technologies, with 75 percent wanting them in permanent use in high-crime areas. Support tails off for lower level crimes. When and where it is used is crucial, and people want to be informed. Along with guidance for police enforcement agencies, public opinion is detailed in the Information Commissioners Opinion (2019).

Where facial recognition technologies are used, that must be according to clearly defined rules around collection and retention and use of data, with a lawful basis being identified The ICO is keen to strengthen the legal framework with the support of a statutory or binding Code of Practice issued by Government. A stronger framework is needed for this new technology with significant uses. The absence of a Code and guidelines will result in compliance failures, lack of consistency, privacy concerns and loss of public trust.

PROFESSOR CARSTEN MAPLE University of Warwick opened his talk with the wide range of uses of facial recognition technologies and biometrics, which influenced their acceptance. Carsten acknowledged James' emphasis on the use of facial recognition technologies being necessary and proportionate – but asked how far we can judge what is necessary and proportionate if we don't understand what facial recognition technologies can do, or how they connect to wider social and historical processes.

In the 19th century, Alphonse Bertillon applied anthropometry to law enforcement to develop a scientific system based on physical measurements (head length and breadth). It was not exact. So how do we determine how useful biometrics are, given we use them for many different reasons, including who we are, whether we have access rights, and to classify people by type. This is not the same as identifying a person. So we need to work out the different ways in which facial recognition technologies and biometrics are intended to be used, and what biases might emerge.

There are other biometric measures other than facial recognition technologies. How might they change the conversation? Detecting crowd size for evacuation purposes, for instance does not depend on identifying individuals. And infrared is another way of measuring biometrics. Where we do use biometrics to identify individuals, it is critical that the data produced is unique. Facial recognition is universal, since most people have something distinctive about their face. But biometrics around fingerprints can be problematic in the case of amputees. Biometrics also have to be permanent. Physical weight is a constant in that it is universal, and doesn't radically change day by day. But it does change.

In addition to uniqueness and permanence, biometric measures need to be accurate and robust. There are ways of circumventing biometric systems. Since Carsten works in security issues, he is interested in how attackers might circumvent a system. We need algorithms to be resilient, and that is a separate, overlapping question to facial recognition technologies. The issue is therefore not about facial recognition as an isolated issue, but as part of a system. Is it privacy preserving? Is it transparent? Is it reliable? In answering these questions, secure systems development is critical. Carsten identified the privacy enhancing technologies in use for perturbing data, rather than saving it, and the ways encrypted data might be used. He concluded by confirming the need for a joined-up approach: that developing systems for verification and understanding the threats facing society need to be considered alongside biometrics and facial recognition technologies.

MATTHEW RYDER QC, Matrix Chambers opened by talking about his experience as a Barrister in biometrics, and as Deputy Mayor where he oversaw the Mayor's work with London Datastore. The Mayor has launched a new project around using data more efficiently. We tend to focus in discussions on the law enforcement paradigm, but there are many benign public organisations using tech to deliver public services effectively, and these are equally in need of guidelines.

Matthew first worked in this area of law in 2002, when he was a junior Barrister. A 12 year-old boy known as 'S' brought a claim against South Yorkshire police because a change in law had resulted in a change of policy. DNA samples were being retained indefinitely for anyone arrested, even in the case of children. The policy had developed because of a rape case where an earlier, unlawfully retained DNA sample of a suspected burglar resulted in his arrest for the rape. In a short timeframe the UK had the largest collection of DNA evidence in Europe, including children and people who had not committed any crime, and a disproportionate number of black and minority ethnic people.

The case being brought by S was challenging this policy on biometrics. At that time it wasn't being framed according to biometrics but according to Article 8 [of the European Convention on Human Rights]. The case failed in the High Court, and at the House of Lords, who rejected the claim that Article 8 impacted on biometrics. The case went to the European Court of Human Rights and S won. But the law did not change until 2012 with the Protection of Freedoms Act.

So it took ten years from the start of S's claim to the Protection of Freedoms Act, during which time the technology had transformed and it was a new world to that which was initially being addressed. Since 2002, in thanks to awareness that built during S's case, an understanding of biometrics data has developed in the legal context. In law, we understand regulation of fingerprints and DNA better. And there is evidence now (through the 2013 case of Edward Snowden) how law enforcement agencies can work with private companies to access information about individual data. This relationship between public and private collection is important, but it was secret and unregulated until the 2016 Investigatory Powers Act.

A historically permissive culture allowed the DNA database to be established, and it has also facilitated the UK development of the largest use of CCTV coverage in Europe. Unlike in 2002, there is evidence of the dangers of governments or societies modelled around a wider use of biometric data to improve/enhance lives, that also demonstrate aspects of human rights concern. So law and regulation has not kept pace with changes. The UK now has general data protection regulation (GDPR) and an Information Commissioner, whose role was transformed in 2001 and has embraced the role of regulation over an expanding area of technology. This is one of the most expanding briefs of any regulator, that covers everything from Freedom of Information to nuisance calls and now AI and machine learning.

The 2012 Act gave the UK a biometric commissioner, but that was for DNA and fingerprints and less to do with the wider biometric implications, so it has adapted to embrace a wider remit. Since 2012, there is also the CCTV Commissioner. But these new roles were not developed within a comprehensive legal regulatory overview, and they therefore overlap around facial recognition technologies, in ways that can be helpful but also confusing. The Met police's decision to roll out facial recognition technologies , moreover, shows that though the regulators might have a view, the police are entitled to make their own interpretations and act accordingly. How far regulators can control behaviour is still open for debate. Some police forces, including London, have ethics advisors that help with these challenges, and they use analogies from bioethics in order to understand newly developing areas.

This is the context in which the review chaired by Matthew is taking place, and why there is a need for some regulation. In May 2017 the Scottish Cabinet Secretary for Justice asked John Scott, a leading criminal QC, to chair an advisory group to review policy on the retention of custody images and review the law. That follows legal challenges around the retention and use of these images. It was broadened out to establish a human rights framework in the fast-moving area of biometrics. The report was published in March 2018, and in May 2019 the Scottish Government published the Scottish Biometrics Commissioner Bill with the UK Biometrics Commissioner. This widely praised initiative is a good example how independent review can help a regulator cover an area more comprehensively than if it were simply imposed.

Unfortunately the UK government in this area has been less impressive than the Scottish response. When it published its Biometrics Strategy in 2018, it summarised biometric use and set out general principles but there was little detail. Those delivering public services don't always have time to think about how they might be delivered, and guidance is essential.

Matthew concluded by setting out timings for the Independent Review he is chairing at the recommendation of the Commons Select Committee. A team and advisory group is in place, evidence will be taken April – June with a view to reporting in October. Matthew hoped that many people in the room would help inform that process.

DEBATE

The debate touched on many core themes that had been raised by the speakers, including the language used, the tensions between public safety and privacy, the broader role of technology in society, and the question of accuracy. Data driven and AI technologies are known to develop their own forms of bias (e.g. greater levels of inaccuracy with some groups of people, and more overt surveillance of some groups of people relative to others). When taken uncritically or adopted in combination with human bias the technologies can exacerbate structural bias in society. Biometrics therefore need to be related to the world around it. There are also limits to what facial recognition technologies can do. It was noted that the ability to detect facial identity is different from the ability to predict emotions and behaviour, and that emotional recognition (as used in gaming apps) needs to be separated out from other forms of facial recognition technologies. The importance of forensic science regulation, somewhat absent in the presentations, was also noted.

This led to a discussion about the need for a holistic or ecosystem approach, with legislation, evidence and consultation working hand in hand on an ongoing basis. This will ensure better collaboration between agencies and organisations (and between nations), and promote an understanding of facial recognition technologies within a broader remit of biometrics and identity. It is not only the face that marks our identity but also the ways we move. So we also need to consider how to protect or use those individual characteristics, such as gait recognition, rather than focusing exclusively on facial recognition technologies.

The public view is critical for the sake of trust in the system. And in the public eye there is a profound difference between facial recognition technologies and biometrics used for protection and those that are used by the commercial sector for profit. So while the focus of discussion tends to be on policing, we need to consider this wider use, which has a low level of public acceptance. These complex attitudes to facial recognition technologies and biometrics need to be considered in a wider sense – after all, we have different attitudes to biometric data being used on our phones to that which is held and stored by public or police authorities. At the same time, regulators are working to keep up with a fast-moving world of technological development and national differences. Building on what exists and collaborating with others is essential, not least because regulation can be contagious. Regulation goes hand in hand with innovation and we should not envisage them as separate states, or think that regulation simply inhibits creativity.

The question of environmental consequences was raised and whether the energy costs of technologies and data were being taken into account. This is not a side-line issue, as data centres are an increasing source of carbon emissions – it was estimated that 14% of carbon emission would be related to data technologies by 2040. Organisations need to work together to collect, share and store data in order to reduce this load. The UK is getting better at protecting data, it was asserted, and it is right that decision making about all aspects of data use is under scrutiny.

In thinking about facial recognition technologies, biometrics and responsibility, we also need to consider who is being protected, for what purpose and by whom? It is not simply a question of whether we are heading towards a dystopian Orwellian future of surveillance, but conversely what risks are involved if we don't regulate, and we surrender our liberties. Regulation and legal control and guidance are as relevant to the bodies protecting us as controlling us. Balancing these needs is critical, and a speedy resolution is essential. Yet due process needs to be observed – it is public consultation that ensures decisions made are accountable and transparent. Scenario planning, using a wide range of insights from across the academic disciplines, is essential if we want to imagine the "What ifs"?

Citizenship is a critical theme in relation to biometrics, facial recognition technologies, privacy and safety. It was suggested that we should not be restricting this analysis to adults. Children are 25% of the population, but also targeted by companies in order to develop the technology. Nor should we ignore what 'citizenship' means. It is not only UK nationals who need to be protected but also the many non-nationals whose fingerprints and photographs are taken by British authorities, and many of whom live in the UK. What about their rights? This question led to a discussion about the need to include the experiences of specific, often marginalised groups into discussions about facial recognition technologies and biometrics: children, migrants, BAME, neuro-diverse and LGBTQ+ people. A robust, critical, public deliberation is much needed.

Dr Fay Bound-Alberti