UK Parliament
POST

The Future of Biometrics

– closed POST lunch briefing event

Wednesday 6th February 2019, 13.00 – 14.30, Room P Portcullis House

POST held this event for parliamentarians to discuss with academia, industry and the third sector the effectiveness and limitations of biometric technologies, and the ethical and privacy issues around the use of biometric data in the UK. Focus was also given to the challenges and opportunities for future biometric technologies and their regulation by the UK government. The event was chaired by Stephen Metcalfe MP, Co-Chair of the All-Party Parliamentary Group on Artificial Intelligence (APPGAI) and member of the Science and Technology Select Committee. Attendees heard briefly from nine speakers during the discussion:

- **Dr Simon Whitfield, Deputy Director, Public Services Innovation, GO-Science***
- **Brenden Crean, Home Office Biometrics Programme Director**
- **Professor Paul Wiles, Biometrics Commissioner**
- **Dr Christophe Prince, Director, Home Office Data and Identity**
- **Silkie Carlo, Director, Big Brother Watch**
- **Dr Tony Mansfield, National Physical Laboratory**
- **Professor Sarah Stevenage, University of Southampton**
- **Professor Carole McCartney, Northumbria University**
- **Sue Daley, Associate Director, Technology & Innovation, TechUK**

*Sir Patrick Vallance, Government Chief Scientific Advisor sent his apologies that he was not able to attend the event due to a conflicting meeting in Brussels.

Lunchtime briefing summary

Stephen Metcalfe MP opened the event, stated that the event would focus on biometric technologies and the use of biometric data, and thanked the speakers for attending.

- **Dr Simon Whitfield**:

GO-science publishes reports of various sizes including a recent report, Biometrics: a guide, which is available online. The report aims to de-mystify biometrics so that policy makers and the public can take informed views on their use now and in future. The report focuses on the science and technology aspects of biometrics including different biometric modalities, such as finger printing and facial recognition, the accuracy of various systems and how this depends on context. The report also looks at the regulatory landscape and drivers of future developments in biometric technologies. The report was produced through bilateral and round table discussions with experts from academia, industry, government and agencies. The conclusion of the report is that biometric technologies are here to stay as they are hugely powerful and versatile, and there are a myriad of uses for industry and government when well designed and deployed within an appropriate regulatory environment.

- **Brenden Crean**:

Home Office Biometrics (HOB) programme has been working across government since 2014 and is due to finish 2021. Biometrics are already used extensively by the Home Office including for law enforcement, passports borders and visas. The HOB programme tries to bring various uses of biometrics across government together, looks at new technologies as well as working with other countries looking at similar issues around safeguarding national security and protecting the public.

The Home Office is also a member of the Biometric Institute. HOB programme focuses on three main modalities in biometric technology – fingerprints, DNA and facial recognition. In 2017, HOB established a biometrics gateway – "a common front door" or single access point to multiple datasets held by the Home Office. In the last 18 months, HOB has delivered strategic services on mobile phones to police to improve ease of fingerprint identification in the field via an App on police officers' smartphones. The App has a built-in audit function that records the person that the police has asked it to verify the identity of. HOB has also changed IT systems in custody suites in policing so that prints of the upper palm are also taken during fingerprinting. Biometrics are also used for passport and visa applications; for example, to check that the photograph submitted matches the image held on file. Future work HOB programme work will include upgrading the algorithms used for fingerprint recognition and validating new algorithms against Home Office data. They are also replacing the existing national DNA database later this year (2019).

- **Professor Paul Wiles**:

While much of the focus is on current uses of biometrics in policing, many of the same issues could arise in other uses of personal data by government and industry. Legislation only regulates the police use of fingerprints and DNA, not voice recognition or gait analysis. Ministers are not addressing proportionality and governance and legislation has fallen behind technology development and deployment. The police are already using facial matching and experimenting with voice recognition and personal data analytics are being developed more broadly in the Home Office. GDPR 's definition of biometric includes this behavioural data. The public interest case can be made for the police deployment of biometric technologies, but the biometrics data gathered are extremely intrusive. There needs to be proportionality between intrusion and protection. Who is going to address this balance? There is currently no steer from government, police chiefs are having to make their own decisions in some cases. Proportionality is a public issue and public issues should be decided by parliament. A new legal architecture is needed that is future proof against further technical developments. Existing examples include GDPR and the planned legislation in Scotland on the police use of any future biometrics. Clear rules are needed on who has access to which government databases for which purpose. Use of biometrics, particularly by the police, depends on maintaining public trust and trust could erode if there are not clear rules on the use of biometrics.

- **Dr Christophe Prince**:

Use of biometrics is growing in both the commercial sector and also in government e.g. border control, e-passports. The Home office are supportive of the use of biometrics in other settings, including in policing where they can help identify a person with a higher degree of certainty. The biometric strategy recognised the personal nature of biometrics and provided a framework for use of different technologies in different settings. When considering new uses questions that needed to be considered included who was using the data, how robust is the technique and what oversight there was in those settings. This was, alongside questions of necessity or proportionality and how the public were engaged. There will always be some risk to individuals, groups, or users so a key question was how those risks were mitigated. Increasingly there is a need to look at these questions in an integrated way – joining technology, operations and policy including governance and oversight – to ensure we can make use of technology whilst maintaining the confidence of the public. The Home Office committed to returning to parliament with a review of the governance of biometrics in June this year (2019).

- **Silkie Carlo**:

Big Brother Watch (BBW) uses the term "body data" to explain biometrics in order to exemplify how personal and intrusive the data can be. BBW have analysed the effects of biometric technology use, which can be rights-altering, particularly in a policing context. There needs to be a legal basis for the use of technology as at present there isn't a legal basis for the use of facial recognition technology by police. For example, BBW observed deployment of facial recognition by the Met Police in Romford last week, with people were stopped and searched after objecting to having their face scanned. Mobile fingerprinting with phones was also carried out as well as face scanning, and facial recognition technology being used on mobile devices by plain clothed detectives was witnessed by BBW. This is a new technology; no public engagement work has been done on its use despite it representing a significant change to policing and the relationship with the public, as well as changing the experience of civil liberties in public spaces. Another example is the custody image database which contains 12.5 million biometric photos of faces, many of whom are innocent members of the public. The database is not able to automatically delete images of innocent people. A third example is the HMRC which holds the biggest state-held biometric voice database in the world containing 7 million voice IDs. Voice IDs were taken without seeking consent and in the absence of lawful basis. Originally it was not possible to delete these voice IDs, but BBW campaigned for this function to be installed. It cannot be assumed that existing data regulations provides a legal basis for biometrics. There are opportunities from biometrics, but there is a need to be a sensitivity to the ways they can alter and undermine people's rights.

- **Dr Tony Mansfield**:

The NPL is the national measurement institute, and one of its roles is to evaluate the performance of biometric technologies. There are a lot of effective applications for government and private business with a range of different modalities, but there are also less-effective applications e.g. facial recognition, where more testing is required. Biometrics need to be tested in standard/ideal conditions and also in operational contexts, as performance will vary. Different applications/contexts will produce different performances e.g. sensors at different angles, different test populations (young, old) give different results. Therefore, multiple tests are required that are specific to the application of interest. The standards for performance measurement are that it must be repeatable, relevant, and allow for fair comparison between systems. We need to understand uncertainties with measurements and dependencies on other factors. On privacy and ethical issues, we need to be careful of 'function creep' - if an individual gives consent for one application, consent needs to be limited to that application. Encryption of biometric data can be used to prevent this 'function creep', but it is not always applicable e.g. for government usage where access to the image is needed. A second issue is bias. Algorithms for facial recognition have small but consistent biases in detecting different demographic groups. However, algorithms are not the main source of bias, context e.g. the composition of the watch list that the police are checking facial images against will have a bigger impact. A lot of the challenges with biometrics have been addressed, as the costs of doing so are coming down, performance has improved, standards exist and there is some public acceptance.

- **Professor Sarah Stevenage**:

Three human dimensions to consider in use of biometric technology: human capability, human limitations, and social acceptability and proportionality. On human capability, humans often perform better than algorithms or biometric systems. For example, humans are better at coping with changes in light, detecting transient changes in emotion on people's faces, and matching human irises than artificial intelligence (AI). It is also important to remember that humans deliver evidence in courts of

law and are often used as back-ups to AI systems. We need to build humans into AI systems, but we also need to recognise human limitations. For example, humans have limited cognitive capacity, as the brain gets tired and can't process two things at once. Humans also have biases; they may be impacted by the emotionality of a crime or the position of a fingerprint sample on the page. Automated systems are therefore needed, as long as it is clear how machines reach decisions. Some biometrics are easier to obtain and less obtrusive than others. Some biometrics are not always present e.g. religious clothing may cover the face, or fingerprints may be worn off. The social acceptability and proportionality of biometrics is key. High value biometrics (e.g. fingerprints) may be inappropriately used for low value purposes (e.g. paying for school meals). We need to combine machine algorithms with human analysts to get robust decision making, drawing on multiple biometrics to capture flexibility. There is a need for transparency and explain-ability so that human decision making can be facilitated rather than confused by the introduction of technology. This will also help achieve social acceptability and proportionality.

- **Professor Carole McCartney**:

Head of multi-disciplinary research centre on crime and justice, focusing on fingerprints and DNA and the ethical and legal frameworks for their regulation. Legislation is slow and reactive, as shown by the example of the DNA database, people get carried away with possibilities of new technology and law is far behind. Laws regulating such technologies need to be well written with supplementary guidance and codes of practice that are accessible for practitioners. Precision of the law will sometimes preclude flexibility to cover possible future uses, so a key question is how the law is policed. Are there real penalties to breaching codes of practice? Oversight is needed, for instance from commissioners sitting on a board, but the success of this approach depends on the resources and powers the commissioners have, such as whether they have the power to take action? There are also problems of jurisdiction. For example, will private and public sectors be governed by the same framework? Will the framework only include the UK? Europe-wide? What about biometrics collected on entry to the US? The final point is that proportionality is a question not an answer; who has decided use of biometrics is proportionate? It is the start of an investigation that determines what criteria we are going to build into legal frameworks.

- **Sue Daley**:

Represent 900 UK tech companies (large and small). Technology is a thriving industry in the UK. Many members are developing tools and techniques using biometrics. What's different now: AI and computing power, pervasiveness of data collection, volumes of data. The market is moving towards biometrics, particularly around digital identity online as passwords are becoming more vulnerable. Biometric technology offers a lot of opportunities and challenges. Examples of commercial uses include verifying identity in transactions, such as financial services/open banking, fraud prevention using voice recognition in banking sector, verifying age for retail, such as alcohol purchase, building access without passes, such as boarding planes at Heathrow without showing passport. Opportunities to improve efficiency and save costs, but more importantly improve security as the online threat environment is continually evolving. There are social, legal, and ethical challenges e.g. 'deep fakes', always people trying to challenge the system. Need to get around these issues before they arrive. TechUK is looking at issues including transparency, accountability, biases and fairness. GDPR gives the legal basis for uses of data. GDPR has to be the starting point for further regulation. New technologies will raise new issues, so gap analysis is needed. TechUK is launching a paper on digital identity (includes biometrics) and the implications for society and economy today.

Discussion

The following points were raised by different participants during the debates around the issues highlighted by the speakers:

- It was noted that science on biometric palm prints is less well developed than fingerprints and this should be considered as the Home Office begins to collect palm print data.
- Data storage at the Home Office was discussed. The 'common front door' instigated by the Home Office Biometrics programme does not mean databases are merged, it just provides a single access point to multiple databases. Who is given permission to search those databases in a matter for legislators and policy makers, subject to appropriate oversight, to decide. There is a wider discussion ongoing in the Home Office on how to handle removal of facial recognition data from databases, currently legislation only regulates police use of fingerprint and DNA data. For example, it is an active consideration of the Home Office to ensure it is easier (or automatic) to delete images from custody image database of innocent people.
- Data security around the Home Office Biometrics System was also discussed. There are significant security controls around all biometric holdings and a security group within the Home Office Biometric programme. There is a minimum requirement for workers on the programme and suppliers to have the requisite level of security clearance. in addition, users of the systems would need permission and relevant accreditation to access the data. The key issue is who has access rights to the data. They would need justification which is set at business level and which is subject to oversight and governance from several sources, including the Biometric Commissioner's office where appropriate. It is important to be careful that data is not inappropriately released at any stage.
- The potential applications of biometrics were discussed. Current focus in the Home Office is on particular uses of biometrics e.g. passports, but they are also used for banking and building access. It could be used for other options, but proportionality is key. Need to get the balance right between protecting people and privacy issues. Potential uses of the technology are there, but public attitudes on them are not.
- The need for a regulatory framework was discussed. Some participants suggested different police forces are interpreting rules differently, effectively creating a postcode lottery with civil liberties that is unacceptable. The Home Office biometrics strategy is quite thin on detail of a regulatory framework; are ministers engaged in setting a regulatory framework? The Home Office has publicly committed to a biometrics governance review and the government has also set up a biometric oversight board that considers new biometric use cases across policing.
- Evaluation of how technologies are used and how they should be deployed by the police may reduce regional variation in technology usage, although local circumstance will vary as will political direction by police and crime commissioners. A national framework needed, similar to the forensic regulator's framework. It will be relatively easy to get scientists to agree on a framework, the challenge is to get all 42 independent police chiefs to sign up. For example, the South Wales Police evaluation of facial recognition technology has come to one set of conclusions and it is not clear if the Metropolitan Police evaluation will come to the same conclusion when completed.
- The importance of data sharing across agencies was mentioned, particularly in the context of sexual exploitation of young people, where historically agencies failed to share information.

- Public trust and acceptability were discussed. A participant queried whether there is a risk of eroding public trust in biometrics by trialling technologies in a way that recalls an 'oppressive state' and cited the use of facial recognition technology in Romford as an example. Will this have impacts for public acceptance of biometrics for other applications as happened in the health sector? Public trust is vital for opportunities for biometric technology in the future. A number of participants suggested the current approach by the police is not sequenced properly and is possibly alienating people from use of biometrics. It is important to remember that in contexts outside of law enforcement, people have the right to not hand-over biometrics and it can't be assumed they will choose to do so. The NHS wanted to use biometric data (care.data), but a lot of patients didn't have confidence in the plan and withdrew their data.
- There were views expressed that there needs to be a set of clear principles of use that the technology is developed within. There is no specific legal basis for live facial recognition, but there are other regulations in law such GDPR and policing rules. Important to note that the way the police interact and follow up on biometric data will be conducted under the rules of policing Including the data protection legislation Part 3 and surveillance camera code. Technology may change the way the public interact with police forces, so public engagement and transparency are key.
- Public vs. private collection and use of biometric data were discussed, including data collection by large internet companies and that by HMRC. The public generally have a greater tolerance of the private sector as they want the services provided. There is a need to look at enforcing the same rules/framework in the private sector as in the public sector. The framework needs to establish what technology can be used in the future as producing regulation afterwards on a reactive basis is rarely satisfactory. It is important to ensure we are making use of technology to deliver things expected from government e.g. identifying innocence earlier, tackling crime. There are also possible advantages for personal privacy as well as disadvantages. For example, the ability to confidently connect two records in different databases may stop the need to send large amounts of personal data to different agencies, reducing data protection risks.
- Public perception of technology is context dependent. The perception of who benefits from use of data – companies or government – may be very localised. Investigations needs to explore in which contexts it would be socially acceptable or the 'norm' for these technologies to be applied. For example, citizen juries or similar mini-public methods could be used.
- Public engagement and attitudes to biometric data were discussed. The best is got out of technology when there is customer or citizen engagement, such as the South Wales Police's system for engaging with the public on ethical issues. These forums can be an important source of information.
- How best to engage with the public to help them decide the balance between loss of privacy against benefits gained? Problems for users might be further down the line when two pieces of biometric data they gave away are linked to create data they do not find acceptable. It is difficult to engage public on issues that are not currently a risk to them.
- Public attitudes to biometric data collection tend to fall into two groups: 1) I have not done anything wrong so there isn't a problem, 2) technology changes so you need to comply. The attitude from the public sector is often, 'If private sector does it all the time, why not the police?'. Data is the fuel driving the fourth industrial revolution, but people are not being asked whether data is being used or shared for other purposes. The Cambridge Analytica

scandal has raised awareness. There will only be a public debate on these issues if politicians lead it, but leading discussion with the public on data usage is difficult as it is a dry and niche issue. Public often tick data usage agreements without considering it and don't realise the consequences until too late.

- When data could have been used to address security risks, the public is also likely to object to it not being used. To bring the public along on the journey they need to be clear about the benefits of biometrics technology and what the benefits are to individuals, families, and society as whole to be able to use this data. Need to find a narrative on what the technology is used for and how it can help people.
- A key element missing in starting the debate is the failure of parliamentary process e.g. home office legislation. This is major concern as the uses already happening are concerning, with individual police commissions taking decisions rather than Parliament in a legislative context. For example, the ID card program was rejected as significant parts of parliament didn't think it was appropriate.
- This is a nuanced debate which benefits from having all perspectives in the room.

Stephen Metcalfe MP drew the event to a close, thanking all attendees for their contributions.