HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 578 June 2018

Biometric Technologies

Biometric technologies are increasingly being used in the UK to help identify individuals. This note gives an overview of these technologies, their applications, and the policy challenges that arise from their use.

Overview

- Biometric technologies enable the identification of people based on their physical or behavioural characteristics.
- They have the potential to make accessing services more secure and convenient, and to provide new tools for law enforcement.
- There is debate over whether the regulation of biometrics is adequate, especially for police use of facial recognition technology.
- Biometrics raise potential challenges, particularly relating to privacy, public acceptance and the potential for bias.
- The Home Office has just published its delayed strategy for biometrics.

Background

Biometric technologies identify individuals based on their distinguishing physical and behavioural attributes, such as fingerprints, face, and voice (Box 1).[1,2] Unlike passwords or traditional identity documents, biometric attributes are inherently linked to a person and cannot usually be lost or forgotten, potentially providing greater security and convenience. They are used in two main ways:

- **Verification** – ensuring that someone is who they say they are, by comparing a biometric attribute to a previously obtained 'reference' record, e.g. checking that an individual's face matches the photo in their passport.
- **Identification** – determining who a person is, by comparing a biometric attribute against a set of reference records collected from multiple people, e.g. comparing a fingerprint collected from a crime scene to a fingerprint database of previous offenders.

The global market for biometrics is estimated to grow to £21 billion by 2022 (a 130% increase on 2016).[3] Several factors are contributing to this rise, including the vulnerability and inconvenience of passwords,[4-6] increasing use of mobile devices with biometric capabilities,[7,8] and the growing power of biometric systems, which have benefited from advances in computing technologies such as artificial intelligence.[9-11] The Commons Science and Technology Committee and others have highlighted a lack of Government oversight and regulation of certain aspects of biometric technology.[12-14] The Home Office has just published a strategy for biometrics, which was originally expected in 2013.[15-18]

Box 1. Types of Biometric Attribute

In general, biometric attributes are universal and permanent. They can be measured and analysed to produce a digital signature that is sufficiently distinctive to an individual to enable their identification.[19] They are often split into two types:

- **Physical** – derived from a physical attribute, these include a person's **DNA** (from which an essentially unique DNA profile of 32 numbers can be derived),[20] **fingerprint**,[1] **iris**,[21] **hand geometry** (the shape and size of the hand),[1] and **face** (the spatial relationship between facial features).[21]
- **Behavioural** – derived from a behavioural attribute, these include a person's **gait** (how they walk),[22,23] **typing pattern** (how they use a keyboard or smartphone touchscreen),[1,24] **voice** (determined by factors such as accent and the shape and size of the vocal tract),[25] and **signature** (the way they sign their name).[1] Some behavioural attributes will also be influenced by physical characteristics.

Applications of Biometrics

The applications of biometric systems (Box 2) include securing access to financial and government services, restricting access to physical locations, controlling borders, and law enforcement.

Financial Services

As of 2016, mobile apps (software installed on a smartphone or tablet) are the most common way to access online banking services in the UK.[26] With smartphones increasingly having the ability to collect and analyse biometric data,[7] many banks now offer biometric verification on mobile banking apps, often using fingerprint or facial recognition.[27-29] Some banks, such as HSBC and Barclays, offer voice recognition as a means of identity verification

Box 2. Biometric Systems

Biometric systems are essentially pattern matching systems, which involve four main processes:[1]

- **Data capture –** a sensor captures the biometric characteristics of the user, e.g. a camera taking an image of a person's face.
- **Feature extraction** – the biometric data captured by the sensor are processed into a digital form containing only the key distinguishing features required to identify the user.
- **Storage** – biometric features are stored for future comparison as a reference record, either on a central database or on local storage (such as on a passport).
- **Comparison** – an algorithm compares input biometric data with one or more reference records and gives a score for how close the match is. Depending on whether the score is over a certain threshold, the system declares either a match or a non-match.

Most biometric systems are probabilistic and thus always involve some degree of error.[30] A key consideration is the threshold set for accepting a match. A high threshold will lead to fewer false matches but more false non-matches (failures to identify a genuine match), and vice versa.[31] The threshold chosen depends on the application. For example, at passport control, a high threshold may be set to reduce false matches that would lead to someone being wrongly admitted. For less secure applications (e.g. unlocking a smartphone) a lower threshold may be used to minimise users being falsely rejected. Other considerations include the speed of comparison and system cost.[31]

for their telephone banking customers.[32,33] Internet commerce fraud in the UK increased from an estimated £135 million in 2010 to £309 million in 2016.[34] A new EU Payment Services Directive aims to address this by requiring users to provide at least two pieces of information to prove their identity, one of which can be a biometric attribute.[35] MasterCard says that all customers will be able to use fingerprint or facial recognition to verify their identity for online payments by April 2019.[36]

Government Services

Currently, biometrics are not widely used to access public services in the UK. HM Revenue and Customs allows users to access its mobile app using a fingerprint and uses voice recognition to speed up security checks for people telephoning them.[37] The Government Digital Service says that it is working with Government departments to support their use of biometrics.[38] Some countries use biometrics more extensively for public service provision. For example, Portugal's citizen card holds fingerprint data, allowing biometric verification when accessing public services.[39] India's Aadhaar identity scheme has collected fingerprints, iris and facial images of over one billion Indian residents, to facilitate access to government services.[40]

Physical Area Access

Biometrics have been used to restrict access to buildings or other sites since the 1970s.[41,42] Today, uses include:

- **Controlling access to critical infrastructure** – e.g. the British Army uses fingerprint and iris recognition to control access to some of its bases.[43]
- **Controlling access to construction sites** – e.g. hand geometry and iris recognition were used to manage access to the site of London's Olympic Park.[44]
- **Reducing document use** – e.g. British Airways is trialling facial recognition technology for self-service boarding without presenting a boarding pass or passport.[45]

Box 3. Government Databases

UK Government databases that hold biometric information include:

- **IDENT1** – fully operational since 2004, this replaced the National Automated Fingerprint Identification System. As of December 2017, it contained the fingerprints of around 8m people and just under 2m unmatched crime scene fingerprints.[13]
- **NDNAD** – the National DNA Database was established in 1995.[20] In March 2018, it contained the DNA profiles of an estimated 5.3m people and almost 0.6m crime scene profiles.[46,47]
- **IABS** – the Immigration and Asylum Biometrics System came into operation in 2012. In 2015, it contained the fingerprints and facial images for around 15.5m people who had applied for visas or asylum in the UK.[48-50] It can be searched by the police.[48]
- **PND** – the Police National Database has been in place since 2010 and enables sharing of intelligence information between UK police forces. As of February 2018, it held 21m images from people who had been arrested. An estimated 12.5m of these were searchable using facial recognition software.[17]

Borders and Immigration

All passports issued to UK citizens since September 2006 have been biometric.[51] They contain an electronic chip that holds a digitised image of the passport holder's face, which can be used to automatically verify the holder's identity. When a traveller presents the passport at an 'ePassport gate', the gate takes a photo of the traveller's face and compares this to the image on the chip using facial recognition technology.[52] HM Passport Office also uses facial recognition technology to automatically identify potentially fraudulent passport applications.[53,54]

People applying for a visa or seeking asylum in the UK have their fingerprints and photo taken during the application process, which are stored on a central database (IABS, Box 3).[49,55] New applications are checked to see if an applicant has applied before under a different name, by comparing with biometric records held in the database. A search of the national police fingerprint database (IDENT1, Box 3) is also used to check for any criminal history. The person's identity can be verified upon entry to the UK, by comparing their fingerprints with those in the application.[56]

The EU is adopting an entry/exit system, which will register the fingerprints and facial images of non-EU nationals on entry and exit from the Schengen area.[57] This will help identify people inside the EU who are undocumented or have overstayed their visa.[58] This system is expected to enter operation in 2020, and raises the possibility that the biometric information of UK nationals will be taken and stored on entry to the EU after Brexit.[59]

Law Enforcement

Biometric technologies used for law enforcement include fingerprints, DNA, facial recognition and voice recognition (POSTnote 509).[60,61] This use is subject to the legislation outlined in Box 4. Biometric data are held in multiple databases (Box 3). The Home Office Biometrics Programme aims to replace existing Home Office biometric databases with a single system for accessing biometric data (Box 5).

Fingerprints and DNA

Fingerprints recovered from crime scenes can be used to search the national police and immigration databases

Box 4. Legislation Governing the Use of Biometrics

General Legislation

- **Data Protection Act 2018** – implements the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive.[62] It explicitly classifies biometric data as a 'special' type of data, making it subject to stricter processing rules.[63-65] The Act defines biometric data as physical, physiological or behavioural characteristics that allow the unique identification of a person. The Biometrics Commissioner has suggested that this definition may also include patterns of social behaviour or 'sociometrics'.[13]
- **Human Rights Act 1998** – states that everyone has the right to respect for their private life.[66] The European Court of Human Rights (2008) and the UK High Court of Justice (2012) have ruled that the retention of fingerprints, DNA, and facial images by police interferes with this right, and hence must be justified and proportionate for the purposes of public safety.[67,68]

Law Enforcement Legislation

- **Police and Criminal Evidence Act 1984 (PACE)** – allows police to take and retain fingerprints, DNA and facial images following arrest, for the purpose of solving or preventing crime.[69] Before the Protection of Freedoms Act 2012, DNA and fingerprints could be held indefinitely.
- **Protection of Freedoms Act 2012** – amended PACE in response to a ruling from the European Court of Human Rights that the indefinite retention of fingerprint and DNA data from people not convicted of a crime was unlawful.[67,70] The new regime generally requires the automatic deletion of fingerprint and DNA data from people who are not convicted. However there are exceptions, for example, DNA and fingerprint data from those charged with a serious offence may be kept for three years. DNA and fingerprint data from those convicted of a recordable offence may be retained indefinitely. The Act created the roles of the Surveillance Camera Commissioner, who encourages compliance with the Surveillance Camera Code of Practice, and the Biometrics Commissioner.[71,72] It also created a strategy board to oversee the police DNA and fingerprint databases.[73]

(IDENT1 and IABS, Box 3).[19] A match must be manually verified by a fingerprint expert before being used as evidence in court.[74] DNA profiles generated from crime scene DNA can be compared to profiles in the National DNA Database (Box 3).[75] A match provides strong evidence of association between an individual and the crime scene object that the DNA was recovered from (the chances of two unrelated people having identical DNA profiles is less than one in one billion).[76,77] DNA evidence is used in court, but is the sole evidence only in exceptional cases.[78] The quality of fingerprint and DNA evidence in the criminal justice system is overseen by the Forensic Science Regulator.[79,80]

In 2015, the UK voted to join the Prüm convention, which enables the sharing of access to DNA profile, fingerprint and vehicle number plate data between EU states for the purposes of solving crime.[81] Interpol procedures for sharing this information exist, but take an average of 143 days for DNA data compared to 15 minutes under Prüm.[82] The UK is due to fully connect to the system in 2020, although it is unclear how this will be affected by Brexit.[83,84]

Facial Images

Since March 2014, police have been able to use images (e.g. CCTV footage) to search against facial images (custody images) on the Police National Database using facial recognition software (Box 3).[89] The system calculates a ranked list of potential matches, which are manually inspected to confirm or reject a match. Matches are used for intelligence purposes; the Home Office has said that results are not treated as definitive evidence of identification.[89]

Box 5. Home Office Biometrics Programme (HOB)

The Home Office Biometrics programme was initiated in 2014 to provide a single point of access to biometric services for law enforcement and the Home Office, including HM Passport Office, Border Force, and UK Visas & Immigration.[85] It aims to provide cost savings, make data sharing more efficient, and ensure service continuity when contracts for IDENT1 and IABS expire in 2019.[86] There will be biometric matching algorithms for fingerprints, DNA and facial images, and the capability to use additional types of biometric data in the future. The Biometrics and Forensics Ethics Group (which provides independent ethical advice to the Home Office) has set up a working group to provide feedback on the privacy impact assessments carried out by the Home Office during the programme.[87,88]

Automated Facial Recognition

UK police are trialling real-time automated facial recognition technology (AFR). This identifies people automatically from live video footage (e.g. CCTV), by comparing their face to a database of facial images.[90] The Government has said that this database is a bespoke "watch list" that may include people banned from attending certain events, known criminals, and people wanted in connection with an investigation.[91] The Metropolitan Police trialled AFR at the Notting Hill Carnival in 2016 and 2017.[92,93] South Wales Police tested AFR at sporting events, shopping centres, and other events.[94,95] Over a trial period from June 2017 to March 2018, 8.7% of matches were found to be correct.[96]

Other countries are also using AFR. For example, the Singaporean Government is conducting trials to combine facial recognition with video and audio data to automatically detect unusual activity and persons of interest in public spaces.[97] In China's Xinjiang province, the government is reportedly using facial recognition to alert authorities if a person of interest leaves certain areas.[98]

Policy Challenges

Biometric technologies raise challenges in relation to legislation and regulation, data security, privacy, performance testing, cost-effectiveness, the potential for bias and public acceptance.

Adequacy of Legislation and Regulation

Questions have been raised about the adequacy of current legislation and regulation relating to the retention of custody images and to automated facial recognition.

Custody Images

UK legislation (Box 4) allows police to retain indefinitely the custody images of those they arrest, regardless of whether they are later convicted. In 2012, the High Court ruled this unlawful, on the basis that it is disproportionate to make no distinction between convicted and non-convicted people.[68] Following a Home Office review in February 2017,[89] those who are not convicted can ask for their custody images to be deleted. Unlike DNA and fingerprint records, deletion is

not automatic, and police can refuse requests in certain circumstances. The Biometrics Commissioner (Box 4) has questioned whether the changes made by the Home Office review will be sufficient in the face of future legal challenges.[13] In its Biometrics Strategy, the Home Office has said that it will enable more efficient review and automatic deletion of custody images by linking them to conviction status.[15] The Home Office's Biometrics and Forensics Ethics Group suggests that people who have been arrested are unlikely to be aware of their right to request the deletion of their images.[99] As of October 2017, 67 requests had been made (to 37 of 43 police forces).[100]

Automated Facial Recognition

No UK legislation specifically relates to the use of CCTV with facial recognition capabilities.[101] The Surveillance Camera Code of Practice states that police use of facial recognition needs to be justified and proportionate,[101] although the Surveillance Camera Commissioner has no power to enforce this.[102] The Information Commissioner's Office's Code of Practice for surveillance cameras also applies.[103] The Biometrics Commissioner's remit does not cover police use of custody images or AFR.[104] He has acknowledged the potential benefits of AFR to policing, but has also called for debate and legislation from Parliament to address its use.[105] The Biometrics Strategy says that the Home Office will: create an oversight and advisory board for AFR and facial images; update the Surveillance Camera Code of Practice; and consult with stakeholders on biometrics governance.[15,91,106]

Data Security

Biometric attributes cannot be altered easily and could be permanently compromised if obtained by an impostor.[107] Additionally, some biometric attributes are inherently public, increasing the risk of them being obtained without consent.[1,108] For example, an impostor might try to use a photo of someone's face, taken without their knowledge, to trick a facial recognition system.[109] Systems are being developed to counter this by detecting when biometric data comes from an artefact, rather than a living person.[110] Security can also be enhanced by transforming the data before storage in such a way that the original biometric data cannot be recovered if the stored data are stolen.[108]

Privacy

The Information Commissioner's Office encourages the consideration of privacy implications from the start of a biometrics project, through privacy impact assessments.[111] The Biometrics and Forensics Ethics Group has also issued a set of principles for using biometric technologies, highlighting the protection of privacy.[112] However, balancing the societal benefits of biometrics with individuals' rights to privacy is not straightforward.[113,114] Some say that biometric technologies increase privacy by making personal data more secure and reducing the risk of identity fraud.[115] Others argue that biometric technologies, especially types that can identify people covertly and at a distance, present a threat to privacy by removing the possibility of anonymity. For instance, Big Brother Watch has raised concerns about the use of AFR by the police, as it automatically scans every face in view to check if it is on a watch list.[116] The centralised storage of biometric data has also raised concerns of 'function creep'. This is where information is used for purposes different to those that it was acquired for,[114] potentially damaging public trust in biometric technologies.[113] For example, India's Aadhaar identity scheme was initiated to give marginalised groups proof of identity and access to welfare. Though enrolment was initially voluntary, the government is now aiming to make it a requirement for accessing many other services.[117,118]

Performance Testing and Cost-effectiveness

The Commons Science and Technology Committee has said it is essential for biometric systems that impact on civil liberties to be tested, to ensure they are dependable.[12] This can be difficult and costly, as a large and demographically representative dataset is needed to test the accuracy of a biometric matching algorithm.[119] Some of the most comprehensive tests are conducted by the National Physical Laboratory in the UK and the National Institute of Standards and Technology in the USA.[120,121] Operating conditions are also important. For example, poor lighting can have a large impact on the performance of facial recognition systems.[9,122,123]

Whilst noting the important role of biometric technologies in policing, the Biometrics Commissioner has pointed to a lack of research proving their cost-effectiveness, compared with investing in other policing procedures.[19] The Home Office has said that it will commission research in this area.[124]

Potential for Bias

In some cases, facial recognition algorithms may be less good at recognising certain groups. One study compared several commercially available algorithms and found that accuracy was lower for people who were black, female or in the 18–30 years age group.[125] This may be due to the demographic make-up of the databases used to develop and train the algorithms; another study found that algorithms developed in East Asian countries were less accurate when identifying Caucasian faces, and that those developed in the West were less accurate for East Asian faces.[126]

Public Acceptance

Research on public attitudes to biometric technologies is limited. One academic research project found that use of biometrics was the most concerning authentication method for members of the UK public, who had strong associations between biometrics and state control and surveillance.[127] However, a UK industry survey from 2016 concluded that 61% of consumers thought that biometrics were just as secure, or more secure, than passwords, and 64% were comfortable using these technologies to access their online bank accounts.[128] Other industry studies have reported that consumers would prefer using biometrics over passwords to make payments.[4,129]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Khalil Davis for researching this briefing, to the Engineering and Physical Sciences Research Council for funding his parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lydia Harriss.

Endnotes

[1] Jain et al. Introduction to Biometrics, 2011
[2] Government Office for Science, Biometrics: A Guide, 2018
[3] Reportlinker, Global Biometrics Market - Competition Forecast & Opportunities, 2012 – 2022, 2017
[4] MasterCard, Lovisotto et al. Mobile Biometrics in Financial Services: A Five Factor Framework, 2017
[5] National Cyber Security Centre, Password Guidance: Simplifying Your Approach, 2016
[6] Deloitte, A World Beyond Passwords: Improving Security, Efficiency, and User Experience in Digital Transformation, 2016
[7] Counterpoint Research, More Than One Billion Smartphones With Fingerprint Sensors Will Be Shipped In 2018, 2017
[8] The UK Cards Association, UK Card Payments 2017, 2017
[9] NIST, The 2017 IARPA Face Recognition Prize Challenge, 2017
[10] Parkhi et al. Deep Face Recognition, 2015
[11] FACER2VM, FACER2VM project, 2017
[12] Commons Science and Technology Select Committee, Current and Future Uses of Biometric Technologies - Report, 2015
[13] Biometrics Commissioner, Annual Report 2017, 2018
[14] Big Brother Watch, Briefing for Short Debate on the Use of Facial Recognition Technology in Security and Policing in the House of Lords, 1st March 2018, 2018
[15] Home Office, Biometrics Strategy: Better Public Services, Maintaining Public Trust, 2018
[16] Home Office, Response to House of Commons Science and Technology Committee Report on Forensic Science, 2013
[17] Commons Science and Technology Select Committee, Oral evidence session 6 Feb 2018 - HC 800, 2018
[18] Commons Science and Technology Select Committee, Biometrics Strategy and Forensic Services, 2018
[19] Biometrics Commissioner, Annual Report 2016, 2017
[20] National DNA Database Strategy Board, Annual Report 2015/16, 2017
[21] ISO, Biometrics Tutorial, 2018
[22] The Royal Society, Forensic Gait Analysis: A Primer for Courts, 2017
[23] Connor and Ross, Biometric Recognition by Gait: A Survey of Modalities and Features, 2018
[24] Frank et al. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, 2012
[25] National Science and Technology Council (USA), Speaker recognition,
[26] UK Finance, The Way We Bank Now: An app-etite for Banking, 2017
[27] NatWest, Mobile App, accessed 11/04/18
[28] Lloyds Bank, Mobile App, accessed 11/04/18
[29] HSBC, TouchID, accessed 11/04/18
[30] National Research Council, Biometric Recognition: Challenges and Opportunities, 2010
[31] National Physical Laboratory, Best Practices in Testing and Reporting Performance of Biometric Devices Ver. 2.01, 2002
[32] Barclays Bank, Barclays Launches Voice Security Technology to All Customers, accessed 11/04/18
[33] HSBC, VoiceID, accessed 11/04/18
[34] Financial Fraud Action UK, Fraud: The Facts, 2017
[35] European Commission, Payment Services Directive (PSD2) Fact Sheet, 2017
[36] MasterCard, Biometric Identification Must be Made Available for all Mastercard Users by April 2019, accessed 11/04/18
[37] Gov.UK, Voice ID Showcases Latest Digital Development for HMRC Customers, accessed 11/04/18
[38] Government Digital Service, The Government Transformation Strategy - One Year On, accessed 11/04/18
[39] Gemalto, 10 years of eID: Portugal's Citizen Card, accessed 11/04/18
[40] Gemalto, Aadhaar: Facts and Trends 2017-2018, accessed 11/04/18
[41] National Science and Technology Council (USA), Hand Geometry, accessed 11/04/18
[42] Jain et al, Handbook of Biometrics, 2007
[43] Sopra Steria, Biometric Data Capture System, accessed 11/04/18
[44] Human Recognition Systems, MSite - London 2012 Olympic Park, accessed 11/04/18
[45] British Airways, British Airways Transforms International Boarding Experience, accessed 11/04/18
[46] Home Office, National DNA Database statistics, 2018
[47] Home Office, Protection of Freedoms Act 2012: How DNA and Fingerprint Evidence is Protected in Law, 2013
[48] Biometrics Commissioner, Annual Report 2015, 2016
[49] Gov.UK, Claim Asylum in the UK, access 11/04/18
[50] Home Office, Biometric Provision for UK Border Agency, accessed 11/04/18
[51] House of Commons library, Biometric Passports, 2012
[52] Gov.UK, At Border Control, accessed 11/04/18
[53] House of Commons, Passports: Fraud: Written question - 210301, 2014
[54] Planet Biometrics, UK Passport Office Implements Advanced Facial Recognition System, accessed 11/04/18
[55] Gov.UK, Tier 2 Visa, accessed 11/04/18
[56] Home Office, Establishing Identity for International Protection: Challenges and Practices, 2012
[57] European Parliament, Smart Borders: EU Entry/ Exit System Briefing, 2018
[58] European Commission, Security Union: Commission Welcomes Adoption of Entry/Exit System for Stronger and Smarter EU Borders, 2017
[59] European Scrutiny Select Committee, Managing the Schengen External Borders, 2017
[60] About Forensics, Harry Jackson, accessed 11/04/18
[61] Parliamentary Office of Science and Technology, Forensic Language Analysis POSTnote, 2015
[62] UK Parliament, Data Protection Bill [HL] 2017-19, accessed 11/04/18
[63] UK Parliament, Data Protection Bill Explanatory Notes, 2018
[64] Information Commissioner's Office, Guide to the General Data Protection Regulation, 2018
[65] House of Commons Library, Commons Library Analysis of the Data Protection Bill [HL] 2017-19, 2018
[66] Human Rights Act 1998
[67] European Court of Human Rights, Case of S. and Marper v. The United Kingdom ECHR 1581, 2008
[68] High Court of Justice, RMC and FJ v. Commissioner of Police of the Metropolis EWHC 1681, 2012
[69] Police and Criminal Evidence Act 1984
[70] House of Commons Library, Retention of Fingerprints and DNA data, 2015
[71] Biometrics Commissioner, About Us, accessed 29/06/18
[72] Surveillance Camera Commissioner, About Us, accessed 29/06/18
[73] National DNA Database Strategy Board, accessed 24/06/18
[74] Forensic Science Regulator, Codes of Practice and Conduct Fingerprint Comparison – Forensic Science Regulator, 2017
[75] Parliamentary Office of Science and Technology, National DNA Database POSTnote, 2006
[76] Forensic Science Regulator, Guidance: Allele Frequency Databases and Reporting Guidance for the DNA (Short Tandem Repeat) Profiling, 2014
[77] Sense about Science, Making Sense of Forensic Genetics, 2017
[78] Law Gazette, DNA – An Unstoppable March?, accessed 11/04/18
[79] Forensic Science Regulator, About Us, accessed 25/04/18
[80] Forensic Science Regulator, Codes of Practice and Conduct, 2017
[81] UK Parliament, MPs Debate Motion Relating to Prüm Decisions, accessed 11/04/18
[82] Home Office, Government Sets Out Case for Joining Prüm, accessed 11/04/18
[83] House of Lords European Union Committee, Brexit: Future UK-EU Security and Police Cooperation, 2016
[84] European Parliament, The Implications of the United Kingdom's Withdrawal from the European Union for the Area of Freedom, Security and Justice, 2017
[85] Gov.UK, Home Office Biometrics (HOB) - Biometric Technical Services, accessed 11/04/18
[86] UK Authority, Home Office to Consolidate Biometrics Systems, accessed 11/04/18
[87] National DNA Database Ethics Group, Annual Report of the Ethics Group 2016, 2017
[88] Biometrics and Forensics Ethics Group, About Us, accessed 29/06/18
[89] Home Office, Review of the Use and Retention of Custody Images, 2017
[90] NEC, Face Recognition, accessed 11/04/16
[91] Home Office, Letter from Baroness Williams, Minister of State for Countering Extremism, 28th March 2018
[92] Metropolitan Police, Statement from Police Commander for Notting Hill Carnival 2016, accessed 11/04/18
[93] Metropolitan Police, Met's Message Ahead of Notting Hill Carnival 2017, accessed 11/04/18
[94] BBC News, Wales Police Technology has 'Ethical Responsibility too', accessed 11/04/16
[95] Wales Online, Facial Recognition Software is Being Used to Catch Shoplifters This Christmas in a Welsh City, accessed 20/04/18
[96] South Wales Police, AFR Trial Results, 2018, accessed 24/06/18
[97] eGov Innovation, Singapore Gov't Completes Safety and Security Trials with NEC, accessed 11/04/18
[98] Bloomberg, China Uses Facial Recognition to Fence In Villagers in Far West, accessed 11/04/18
[99] Biometrics and Forensics Ethics Group, Ethical Advice on the Home Office Review of the Use and Retention of Custody Images, 2017

[100] AOL News, 'Custody Image' Deletion Request Figures Revealed, accessed 11/04/18
[101] House of Commons, CCTV: Written Question - 8098, 2017
[102] Home Office, Surveillance Camera Code of Practice, 2013
[103] Information Commissioner's Office, In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information, Version 1.2
[104] Biometrics Commissioner, About Us, accessed 25/06/18
[105] Biometrics Commissioner, Metropolitan Police's use of Facial Recognition Technology at the Notting Hill Carnival, 2017
[106] House of Lords, Short Debate - Security and Policing: Facial Recognition Technology, 2018
[107] Jain et al, Biometric Template Security - Eurasip Journal on Advances in Signal Processing, 2008
[108] Patel et al, Cancelable Biometrics: A review, 2015
[109] Ars Technica, Galaxy S8 Face Recognition Already Defeated with a Simple Picture, accessed 11/04/18
[110] Nogueira et al, Fingerprint Liveness Detection Using Convolutional Neural Networks, 2016
[111] Information Commissioner's Office, Privacy by Design, accessed 11/04/18
[112] Biometrics and Forensics Ethics Group, Ethical Principles, 2018
[113] Biometrics Institute, Written Evidence submitted to House of Commons Science and Technology Select Committee – Current and Future Uses of Biometrics (BIO0003), 2014
[114] Irish Council for Bioethics, Biometrics: Enhancing Security or Invading Privacy?, 2009
[115] Malcolm Crompton, Biometrics and Privacy: The End of the World as we Know it, or the White Knight of Privacy?, 2009
[116] Big Brother Watch, Briefing for Short Debate on the use of Facial Recognition Technology in Security and Policing in the House of Lords, 1st March 2018, 2018
[117] Gemalto, Aadhaar: Facts and Trends 2017-2018, accessed 11/04/18
[118] Livemint, No Supreme Court Stay on Mandatory Aadhaar Linking for now, accessed 11/04/18
[119] Commons Science and Technology Select Committee, Oral Evidence to Current and Future Uses of Biometric Data and Technologies Inquiry HC734, 2014
[120] National Physical Laboratory, Comparing Biometric Systems, accessed 20/04/18
[121] NIST - Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms NIST Interagency Report 8009
[122] Kalaiselvi et al, Face Recognition System Under Varying Lighting Conditions, 2013
[123] NIST, Face In Video Evaluation (FIVE) - Face Recognition of Non-Cooperative Subjects, 2017
[124] Home Office, Forensic Science Strategy, 2016
[125] Klare et al, Face Recognition Performance: Role of Demographic Information (2012)
[126] Phillips et al, An Other-Race Effect for Face Recognition Algorithms, 2010
[127] IMPRINTS, Written Evidence Submitted to House of Commons Science and Technology Select Committee – Current and Future Uses of Biometrics (BIO0005), 2014
[128] Experian, UK Now Ready for Biometric Banking, accessed 11/04/18
[129] Visa, European Consumers Ready to use Biometrics for Securing Payments, accessed 11/04/18