Government
Office for Science

Biometrics: a guide

Contents

Foreword

All manner of businesses and public services depend on being able to identify people conveniently, accurately, securely, and with appropriate safeguards. Biometrics – automatic recognition of people from physical attributes like their face, voice, iris or fingerprints – has been around for a while but is now developing and spreading rapidly, driven by advances in sensors and algorithms. The use of biometrics on mobile devices has, in particular, attracted a lot of public and media interest.

The nuances of how biometrics works are highly technical: accuracy rates vary hugely by system, conditions and context. The technology is indeed getting better all the time, but there are some inherent limitations. Along with the opportunities, there are some risks and possible mitigations.

Our aim for this report is to demystify biometrics and alternative forms of identification, so that policymakers and the public can take informed views on their uses, now and in the future.

Dr Patrick Vallance
Government Chief Scientific Adviser

Introduction

Biometrics is where statistical methods meet biological data. In modern terminology, as used here, its purpose is specifically to find or confirm the identity of individuals from intrinsic traits.

Accurate identification is fundamental to physical security, information security, financial transactions, contracts and employment, public services, criminal justice, national security and more. The range and frequency of instances where identity must be verified is increasing, with, for example, air passenger numbers forecast to double in the next 20 years.[1] Identity fraud is also increasing year on year.[2] Older systems of identification, such as manual passport checks and computer passwords, are therefore under considerable strain.

Scientific biometrics emerged around 1880, more or less simultaneously in several places. One motivation was to provide secure authentication for employment contracts, especially in the colonial context.[3] But even more significant was the drive to identify repeat offenders who were passing through the criminal justice system – people who were liable to change their names and superficial appearance.

Figure 1: iris scanning in *Minority Report*, Dreamworks, 2002

The two technologies that emerged first were anthropometry (body measurements) and fingerprinting. The latter was more successful because of its ease of capture. Applications of fingerprinting have widened from authenticating documents and recording prisoners to forensic analysis of crime scenes, workplace access and device access. More than 1 billion smartphones with fingerprint scanners are expected to be made in 2018.[4]

Despite its very widespread use, fingerprinting does have weaknesses, and there are numerous alternatives. These include matching of iris pattern, hand shape or the vasculature of fingers or the retina. Generating particular interest now are facial recognition and voice recognition. These can operate remotely and unobtrusively, utilising existing infrastructure such as CCTV and telephones.

Biometrics, either alone or in concert with other technologies, presents huge opportunities for consumers, businesses and government to make identity verification cheaper, more convenient and less vulnerable to fraud. Trends indicate that existing applications will expand and new ones will emerge, meaning that biometrics will become increasingly ubiquitous and powerful.

Indeed, improvements in hardware and software mean biometric technologies that until recently were the domain of science fiction, such as the personally targeted advertising based on iris scans in the 2002 film *Minority Report*, are now entirely possible. (Figure 1.) This raises popular interest in biometrics but also leads

to questions about privacy and where the limits of acceptable use lie. Those issues are international: the current leading face recognition algorithms were developed in Russia and China,[5] while regulatory frameworks everywhere have generally lagged behind the development and deployment of the technology.

The aims of this report are:

- To explain the methods and vocabulary of biometric systems for the benefit of people who are using or considering deploying them.
- To examine current biometric technologies in terms of their capabilities and suitability versus alternatives for the identification requirements of governments, institutions, companies and individuals.
- To consider the drivers, risks and wider developments that are likely to influence the future of biometrics and its applications.

Identification and authentication

An important first principle is that identification is not a single, common process. The terminology of identification is confusing and often used inconsistently. People can be identified with or without their consent, with or without their active cooperation, and with or without them first claiming who they are. The word "authentication" is a generic term for proving the origin or truth of something and can be applied to any of these.

The consensual, cooperative end of that spectrum is generally associated with access control. This is a wide suite of applications, which essentially ensure that an individual has secure and private access to their home, car, workplace, money, data, democratic and travel rights, online identities, hazardous machinery and more. Access can be controlled with physical objects such as keys, cards or tokens, with secret knowledge such as a password or PIN, or with biometrics. A combination of those is multi-factor authentication, the classic "something you have, something you know, something you are".[6] The main difference between those is that objects and knowledge can be shared, legitimately or illicitly, and must be remembered and looked after. Biometrics cannot be lost or forgotten, or readily shared or changed.

The non-consensual, non-cooperative end of the spectrum tends to be associated with powers of the state, relating to criminal justice and national security. Although forensic science and biometrics are closely related and use many of the same sources of data, they are not the same discipline.[7] Forensic science happens after an event, usually involves manual recovery of data, and its results have to be communicated verbally to a courtroom audience. Biometrics is usually applied before the event and can be completely automated. Non-cooperative biometric applications are generally surveillance-based, very often using facial recognition.


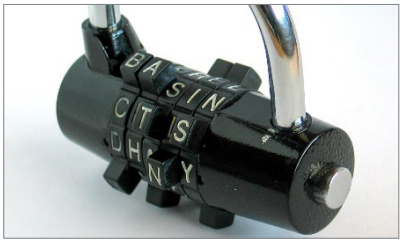

Figure 2: object-based, knowledge-based and biometric patterns

Pattern matching

There are several types of evidence that can be used to find or confirm identity. They include process of elimination and the stated or documented opinion of a third party. But the most important type is direct evidence, which means pattern matching.

The cuts of a mechanical key are a pattern. Passwords are patterns of letters and numbers. Biometric modalities are ingrained patterns within the human body. (Figure 2.) To be useful for identifying an individual, these patterns must be distinguishing and repeatable. For some applications, pattern consistency over long periods is preferable. Fingerprints are formed semi-randomly in the womb, so even identical twins have non-identical fingerprints, and while they stretch over time their fundamental shapes never change, other than through injury. Iris patterns are similar, as are configurations of small blood vessels, for example in the retina or fingers.

Soft biometrics is a wider category of patterns, which may not be unique or permanent but can still be useful for identification. These include physical characteristics like height, body shape or eye colour; affectations like clothing, jewellery, tattoos or facial hair; or behavioural biometrics, which are patterns in learned actions such as gait, handwriting (including signature) or typing.

Samples and references

To make a firm pattern-based identification, a biometric sample from the subject needs to be compared with a biometric reference from when the subject was enrolled in the system. Neither humans nor machines do this by an exact overlay because samples can vary, from causes including angle, lighting or pressure, depending on modality.

The critical challenge is to distinguish between intra-class variation – differences between samples from the same person – and inter-class variation, which is differences between samples from different people. The key is to focus on distinctive features, those where there is considerable inter-class variation. For fingerprints, minutiae – the points where ridges end, meet or split – yield considerable inter-class variation while being very consistent for the same individual. In the 1890s, Sir Francis Galton established that minutiae do not change over time and estimated the probability of two identical fingerprint images coming from different people as 1 in 64 billion.[8] Modern modelling suggests he was, if anything, overly cautious.[9] Different systems and jurisdictions vary in what they

consider the minimum number of minutiae for a guaranteed match. Most are set between seven and seventeen,[10] although for forensic purposes the UK has abandoned a minimum number in favour of a qualitative statistical assessment.

In an automatic system, an algorithm will extract the distinguishing features from biometric samples, then convert them into a numeric code. (Figure 3.) A stored record of these extracted features is also called a template.

The similarity between a sample and a reference is measured as a comparison score. This either passes or falls short of the threshold that has been set for determining whether the two match.

Biometric verification is where the sample is compared with only one person's reference. This is how smartphone authentication works, with the sample and reference usually never leaving the device. It is also how ePassport gates work at the UK border. These match an arriving passenger's face image with the digital image stored in the chip of their ePassport, automating and speeding up the immigration process for low-risk passengers while enabling staff to be re-deployed to higher risk areas. Operating in the UK since 2008, there are now around 254 gates, across 22 air and rail entry points, with numbers continuing to rise.[11] Another example is voice recognition for telephone banking, which was introduced in 2016 and is now used by several of the main retail banks.

Biometric identification is where the system checks the sample against every reference in the database. A green result is where a single reference is above the threshold. An amber result is where multiple references are above the threshold, which will probably require human intervention. A red result is where none are. Identification is harder to get right, but it enables access control without the user having to supply a credential upfront, making it particularly useful for situations where high security must be combined with very convenient access. For example, managing a kindergarten or chemical store within a university campus. Iris scanning is particularly popular in those contexts because it is hands-free, hygienic and accurate.[12]

This "one-to-many" matching is also the method most used for non-consensual and/or non-cooperative identification. Police forces worldwide now keep databases of fingerprints, DNA and faces from convicted criminals, and many have automated systems that can determine in real time if there is a match to a person they have stopped. For surveillance, there might be quite a small database, called a watchlist, but large numbers of people are scanned against it. Watchlists are often of criminals or suspects, but may equally be of missing or vulnerable people, or VIP customers.[13] The nature of the watchlist of course also affects what action is taken when a match is made.

Figure 3: an example of feature extraction from a fingerprint. The raw image is turned into a thinned binary plot, then ends and splits in lines are detected from changes in pixel colour. The set of points is then transformed into a geometric map, which can be stored numerically.

Errors and thresholds

Biometric matching is probabilistic, and the placing of that threshold is critical. A false positive means a sample is matched against the wrong reference, and the proportion of false positives by attempt is called the *False Accept Rate* (FAR). A false negative is a failure to match a sample against the correct reference, and the proportion of those is called the *False Reject Rate* (FRR).

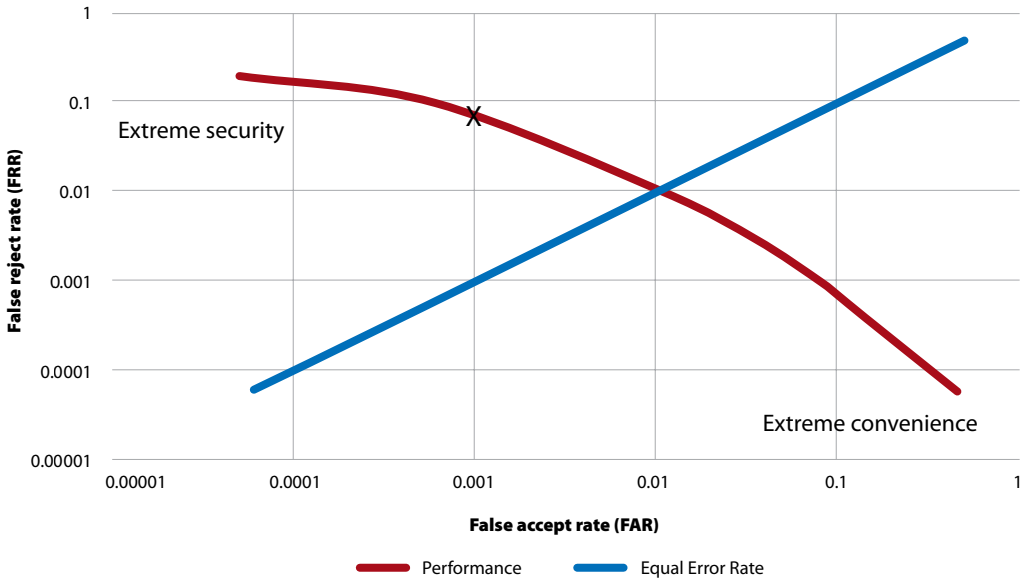

Figure 4: indicative graph showing performance of a single biometric system, on a logarithmic scale. The system can be set anywhere along the red line, by adjusting its threshold. The X marks a sensible threshold for a standard access control application.

A high threshold means a low FAR but a higher FRR. A low threshold means a low FRR but a higher FAR. The point where those are balanced is the *Equal Error Rate* (EER). This is not used to set how the thresholds should be applied but it provides a way of comparing between approaches. A higher EER means a less accurate overall performance.

For access control applications, the right threshold is ideally where the FAR approaches zero, but that might result in a high enough FRR to cause unacceptable irritation to legitimate users. So one would set a high threshold for access to a site of national security importance but a lower threshold for access to a gym or business lounge. (Figure 4.) A false positive does not necessarily mean there is an imposter: the system could have confused two legitimate users. That could result, for example, in passengers in an automated airport being denied access to their flight or sent to the wrong one.

For surveillance applications, the right threshold is ideally where the FRR approaches zero, but that might mean the FAR is so high it causes chaos for the people responding to the alerts. So one would set a low threshold if looking for a terrorist or a missing child, but a higher threshold if using the system as a background deterrent to shoplifters. There is therefore a basic trade-off between accuracy and usability.

There are two other error rates. *Failure to Acquire* (FTA) is where the image acquired by the device is, for whatever reason, not of sufficient quality to create a template. *Failure to Enrol* (FTE) is similar, but the failure is in creating an original reference. It is quoted separately because the threshold is often set higher for enrolment.

Accuracy by modality

Errors in biometric tests can come from inherent or technological sources. Inherent sources, such as medical issues with the individual subject or clusters of template repetition (e.g. babies have relatively similar faces), are hard to change. Errors from technological limitations have much more potential for reduction, from improved sensors, more sophisticated algorithms and better training data.

Comparing modalities by EER requires heavy caveating, noting that the EER is almost never the threshold actually deployed or tested. Also, different algorithms

for the same modality can show very different performance, which varies still further between testing in ideal, laboratory conditions and testing in the field.

All that said, of the modalities in common use today, iris scanning is generally agreed to be the most accurate, with an EER around 0.001%-0.002%.[14] That implies one false accept and one false reject from 100,000 samples. Issues in deployment are that iris requires strong cooperation and can be affected by conditions like drooping eyelids.

Fingerprinting for access control has an EER around 0.5%-3.0%,[15] although with a suitably adjusted threshold its FAR is sufficient to identify an individual from a database of millions. Yet it often has a significant FTA rate: dirt and moisture distort the image, while older people, especially those who have done manual labour for many years, may have very worn fingertips.

Voice recognition has an EER around 5-10%.[16] The voice does change noticeably over time, along with temporary changes such as during illness, as well as natural or affected variations in pitch, speed, accent and so on. The FTA again is a problem, especially in situations with background noise. These are offset by the convenience of voice, and the potential for specifying the content of what is said.

Accuracy of face recognition is very variable. It can compete with human perception in certain circumstances, although the variables on both sides are very extensive. Recent best EER figures are around 0.2%,[17] but that is in static, optimum conditions and with ideal references. The EER for low-resolution surveillance footage, as obtained for example from a drone flying over a crowd, easily exceeds 10% and can be as high as 50%.[18] Even that assumes the references are still of high quality: comparing live faces with low quality printed images, for example a suspected fake ID, has in experimental testing shown error rates of 50% at best, and very high susceptibly to error with siblings and lookalikes.[19] (Figure 5.) As biometric templates are essentially hard-wired passwords, biometric matching from poor-quality sample data is like matching a password from one or two letters.

Figure 5: matching a low-quality CCTV image to a pencil sketch in *Mission Impossible: Rogue Nation*, 2015, Paramount Pictures. In real life, matching from data of this quality has extremely high error rates.

As biometric templates are essentially hard-wired passwords, biometric matching from poor-quality sample data is indeed like matching a password from one or two letters.

People are best at identifying the type of face they see most often, which usually means their own ethnicity. Facial recognition algorithms can similarly become biased if their training datasets are not diverse. Recent research on face classification algorithms from IBM, Microsoft and the Chinese company Megvii shows all to be most accurate with light-skinned men and least accurate with dark-skinned women.[20] Companies involved have responded to say they are working hard to minimise bias in facial recognition, their strategies including ensuring

fairness in training databases and developing bias-detection algorithms.[21] Some have suggested that programmers can unintentionally encode their own biases into software: although more research is needed to establish the true extent of this, diversity in the coding profession can only be a good thing.

Existing research suggests, however, that no algorithm will ever perform ideally for everyone: there will be a few users who are prone to being misidentified, which may make them targets for impersonation or indeed unusually able to impersonate others.[22]

Algorithms and templates

For reasons of computing capability, the first automated biometric systems to appear were the ones that produce small templates. The smallest come from hand geometry systems, an access control device that debuted in the early 1970s.[23] Hand geometry is still probably the best modality in dark and dirty environments such as construction sites. The problem is that there is limited inter-class variation between templates, so it won't work among large populations.

Retinal scanning, which uses infra-red light to scan the pattern of blood vessels in the retina, also produces a small template and was developed commensurately early. In fiction, it appeared in the 1982 film *Star Trek: Wrath of Khan*. Two years later there was a real product on the market (the *Eyedentification 7.5*). Retina is arguably still the most accurate modality.[24] But it is slow, invasive, requires a lot of cooperation from the user, and can be affected by conditions like cataracts, so has since almost entirely disappeared from commercial use.

Iris recognition also scans the eye but takes a standard digital image, augmented with some near infra-red light to brighten dark irises. It uses much more sophisticated algorithms, which were developed in the 1990s. A matrix of data points turns the capture into a compressed image of a given resolution. A statistical test is then done for how much the sample must be changed to morph it into the reference.

Face recognition is an even more advanced problem. There is a lot of intra-class variation – from fashion, ageing etc., as well as capture conditions – while sometimes the inter-class variation is small, including between siblings (especially twins), among the very young and sometimes the very old.

Humans are much better at recognising faces than recognising inanimate objects, but how exactly they do it is still not well understood. It is thought to be a holistic process, involving multiple, diverse areas of the brain. There is a bell curve of ability: people who are exceptionally good at it have sometimes been labelled "super-recognisers", while at the other extreme are people who are severely face-blind, a condition called prosopagnosia. Super-recognisers often outperform machine algorithms in tests, although a machine never gets tired and does not suffer from confirmation bias.

Automatic face recognition uses a chain of algorithms. There are many variations and options, but here is an exemplar of how it can work from surveillance footage.[25] (Figure 6.) The image is first converted to a greyscale map, with changes in gradient then compared with a trained map of the average face, so as to detect

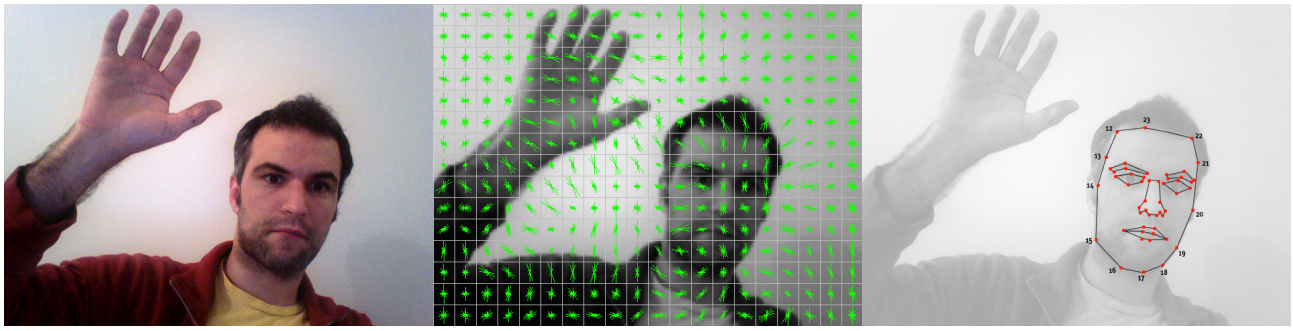

Figure 6: the techniques for turning faces into biometric templates are similar to those for other modalities. A histogram of orientated gradients (centre) detects binary changes in pixel colour, while a landmark map (right) picks out the distinctive points. Photos (left and centre): Greg Borenstein (http://creativecommons.org/licenses/by-nc-sa/2.0).

faces within the image. Another algorithm matches a set of "landmark" points that exist on every face, in order to detect orientation. Each face is then transformed in non-distorting ways, so as to centre the eyes and mouth.

Faces are then analysed by a deep neural network algorithm, which has been trained to find the set of measurements that maximise inter-class variation but minimise intra-class variation. This aspect, called embedding, has become far more sophisticated since 2015. Note that the algorithm never reveals what these measurements represent. As with other modalities, the final step is to check for reference templates that exceed the set threshold.

Attacks on biometric systems

The difficulty of changing one's biometrics is useful for law enforcement applications: criminals such as the 1930's gangster John Dillinger have attempted to burn or sand off their fingerprints, but the resulting scars simply mark one out as a high-value fugitive. Similarly, one can hide one's face from a camera, but that might attract the attention of human operators. The potential value of one's own biometrics also means there is considerable public concern around protecting biometric data from theft. Mitigation against these threats is a fast-evolving field of research.

Cyberattack is the first threat to biometrics and other types of authentication. Passwords are normally attacked via theft of the reference database. Plain text in that database is protected from instant compromise by hashing and salting. Hashing is irreversible encryption, while salting is the addition of random data that prevents an attacker from scanning for known hashes. However, as a desktop computer using its GPU can check around 2 billion hashes per second,[26] it is still vital to choose passwords that are long and not guessable from any dictionary or open source data.

Biometric references, which are more complex than memorable passwords, can also be salted and hashed, making a "cancellable biometric" that could be regenerated if compromised. Note that storing the template on the device is in some ways more secure and private than storing it on a remote database, but equally means the device could be used as a closed sandbox for testing attacks.

Human factors are the next possible line of attack. The most disturbing way to obtain a victim's biometrics is via mutilation, which didn't take long to be imagined

in fiction: in the 1993 film *Demolition Man*, a retinal scanner is fooled with a gouged-out eye. In reality, eye modalities and several others will only work if the tissue is live. Liveness testing for fingerprints can be built into scanners quite easily, albeit with a slight increase in the FRR.

Alternatively, an attacker might coerce their target into using a scanner. This is difficult to stop automatically: detection of stress is one thing, but accurate attribution of its cause is well beyond current technology. The most plausible solution would be for the scanner to recognise a secret distress signal,[27] similar to the real one but triggering a different response.

Presentation attacks

Presentation attacks, also known as spoofing, involve obtaining the victim's biometrics in some way, for example by taking a high-resolution photo of their face, fingertip or iris, or recording their voice, and then using that to create a copy image (2D or 3D), which may be turned into a mask or overlay for an imposter to use. Right back in 1971, the film *Diamonds are Forever* showed James Bond fooling a (crude) fingerprint scanner with latex overlays, as well as using a voice impersonation device: ideas that were apparently beyond the CIA's own thinking at the time.[28]

The huge expansion of smartphone biometrics has made spoofing an item of considerable news interest.[29] Spoofing exploits a threshold that has been set to trade some accuracy for convenience. The acquisition aspect of a presentation attack cannot, in general, be prevented: it is legal to photograph people who are in a public place. Possible defences come at the presentation stage and overlap with liveness testing. They involve analysis of optical, electrical, ultrasonic or temperature properties of the material being scanned, to differentiate live human tissue from an artificial overlay.

Attacks can also be enacted at the enrolment stage if there is a possibility of presenting an imposter's sample, or indeed a morph of multiple images.

Regulation

Over 120 countries now have some form of data privacy law, with another 30 having such laws in the legislative pipeline.[30] But laws that talk about biometrics specifically and in detail are rare. This leads to some discrepancies: for example, Germany is well known for having strict privacy laws but is introducing facial surveillance in railway stations.[31]

One jurisdiction that does have a strong biometrics law is Illinois, which passed its Biometric Information Privacy Act (BIPA) in 2008. At this time many companies were piloting biometric employee monitoring systems in Chicago, and there were concerns about what was happening to the data. BIPA essentially forbids commercial use of biometrics without informed, written consent, or for resulting data to be handed to law enforcement bodies without a warrant. Private legal action may be brought against companies in breach. Ten years on, the number of cases has suddenly mushroomed, with 32 class-action lawsuits brought in two months in late 2017.[32] Some of these stretch beyond Illinois, beyond the modalities originally mentioned, and beyond the employer-employee relationship.[33] This,

arguably, serves as a warning of the difficulties in getting the right balance when regulating biometric use. Texas and Washington State have enacted similar but weaker laws, which do not allow private legal action.

In the UK, there is the Protection of Freedoms Act 2012, which regulates two specific uses of biometrics. Enacting a judgment made by the European Court of Human Rights and following widespread concern,[34] it prevents indefinite police retention of DNA and fingerprints from people who have not been convicted of a crime. It also stipulates that schools operating biometric systems can only enrol children with the consent of both child and parent. The part for schools applies to all modalities, but the police part only applies to DNA and fingerprints (plus shoeprints). Oversight of the Act's implementation is provided by the Biometrics Commissioner. The Home Office's forthcoming Biometrics Strategy is expected to consider a new oversight mechanism for police use of facial images and automatic facial recognition technology.

The EU General Data Protection Regulation, effective from May 25th 2018, grounds biometrics under the processing of personal data. "Lawful grounds" for processing include explicit consent, but also vital, legal, legitimate and public interests.[35] Yet it puts a stronger obligation than before on organisations to consider whether they actually need the data, and if so how records will be kept appropriately secure. A generally useful rule of thumb is that data used for authentication purposes should be less sensitive than the data they are protecting.[36]

Acceptability and rights

There are understandable concerns about how biometric databases are generated, stored and applied, especially, but not exclusively, relating to uses by the state. The challenge to policymakers is to ensure the right balance between the rights of individuals and the wider public (or legitimate commercial) interest.

Figure 7: Aadhaar enrolment campaign, 2014. Photo: Ravishyam Bangalore (http://creativecommons.org/licenses/by-sa/4.0).

Concerns about potential abuse of biometric systems are revealed in the public reception to civil identity schemes. US social security numbers were deliberately set up not to be used for identification, although that has since changed.[37] In the UK, the introduction of biometric ID cards was a long-running debate, reaching the piloting phase before they were abandoned in 2010. India has introduced a system of virtual, biometric ID cards called Aadhaar, with over one billion people now enrolled. (Figure 7.) However, the constitutional basis of this scheme and its relationship with an established inalienable right to privacy are now being extensively argued in the courts.[38]

The Russian app Findface, launched in 2016, allows individuals to match people on the street with their profiles on the social media app *Vkontakte*, with error rates that are significant but not overwhelming. Findface has been used to uncover the true identities of people who have legitimate personal or professional reasons for concealing them.[39] Western social media companies have so far been much more restricted in their use of face data, in part because of pressure from regulators. Faces themselves cannot be kept secret, so the protection against unlimited matching on databases comes from either self-regulation or enforced regulation.

Drivers of development

The idea of an identity verification system that is accessible to everyone and has multiple applications is certainly far from new. In the Ancient world they used seals for these purposes, developing sophisticated bureaucracy around them.[40] In the 19th century handwriting and signatures were the norm. People were indeed quick to recognise the potential of electronic signatures made from thousands of miles away, as they were ruled legally valid as early as 1869.[41] The signature is a behavioural biometric, and while we now have the technology to authenticate pen pressure and angle to a high degree of accuracy, the electronic pads used to sign for deliveries offer a poor tactile experience. It may be that future improvements in e-paper and pens will bring writing-based authentication back into fashion.[42]

Figure 8: RFID implantable microchip, compared with a grain of rice. A next generation, less intrusive version of this technology is a plausible rival to biometric authentication.

In the late 20th century cards predominated, either magnetic swipe or the more advanced gold-chipped smart cards. Unlike keys, these allow subtle gradations of authorisation: only permitting access for a limited period, at certain times, or only if the card is loaded with money, which is why they are used so extensively in hotels and public transport. But for high-security applications, neither cards nor passwords are considered secure enough on their own, which means multi-factor authentication – compounding security but also compounding the inconveniences for the user.

Although smartphones are now ubiquitous, with even low-end models now having advanced capabilities to capture and process optical and other data, authentication to access the phone is more common than using the phone for authentication. Smartphone-based passports have been suggested but not yet implemented, [43] while smart locks are available but so far are a niche product.[44] Smartphones have numerous issues with reliability and constantly broadcast their location, which may be useful or a vulnerability depending on circumstances.

Radio Frequency Identification (RFID) tags can be passive or active. Alone or in combination with a smart chip, they enable the transfer of small amounts of data over a short distance. Forms of these are used in ePassports and Oyster cards. RFID tags are extensively implanted in animals, and may equally be implanted in humans, for example in the web between thumb and forefinger. (Figure 8.) The intrusiveness has largely limited human uptake to enthusiastic amateurs ("biohackers"), with a particular subculture in Sweden.[45] But an RFID tag allows convenient and graded access control, without the wide-area surveillance potential of smartphones or facial recognition. GPS transponders will not currently fit on an RFID tag, and a tag can be removed. It is quite possible that future technology will allow less intrusive RFID implants, such as a temporary tattoo,[46] which with sufficient security protection could become the most significant competitor to biometric authentication.

Horizon scan

"Frictionless verification" is often claimed to be the goal of authentication development, i.e. legitimate users don't even notice the process, but it is very hard for an imposter to get through.

At airports, the next step on from e-gates at immigration is to make the entire airport experience seamless, so that passengers show their passport only at check-in, and then bag drop, security, immigration, lounge access and boarding are all handled by gates using real-time face recognition. Schiphol airport in Amsterdam is currently piloting this, and there are similar plans for Australia's international airports.[47] (Figure 9.) This is thought to be the only viable solution to increasing passenger numbers, without making proportional increases to staff numbers and floor space. Issues that have emerged so far are the need to control light – face recognition accuracy drops off sharply in shadow or strong sunlight – and the fact that a small percentage error rate will still scale up to a significant net number of people affected by system errors.

Figure 9: face recognition at Schiphol airport. Photo: Newsroom KLM

It is highly likely that the next developments in biometric authentication will focus on raising security against different types of attack and on removing as much friction as possible. Those two goals often conflict: iris recognition is accurate, but the need for correct positioning necessarily adds friction, while using it for surveillance over distance could result in some people receiving risky doses of near-infra red light.[48] These factors mean facial recognition is likely to grow as the most widely applicable modality, with further improvements coming in the cameras and algorithms used for spotting and identifying faces from distance and in poor conditions. Notably, it is easier to get access to recordings of faces and voices, and so develop open source algorithms, than it is to access fingerprint or iris databases. Human/machine combinations may also prove more powerful than either on their own.

Multimodality means checking more than one biometric pattern, ideally within the same scan, for example face plus iris or fingerprint plus finger veins. This makes spoofing far more difficult and allows people who are excluded from one modality for medical reasons still to use the system. DNA is the only modality that applies to absolutely everyone, but it cannot yet be matched in real time, and subjects could provide samples from another person, making it problematic for access control.

Fusion is the general term for combining multiple sources of data, which may be multimodal, or the same modality scanned by different sensors, assessed by

different algorithms, or snapshotted at different moments in time. If fusion is on a disjunctive (an "or" test in logic terms) basis, for meeting two or more thresholds, it can dramatically reduce the FRR and FTA rates, but at the cost of a slightly higher FAR. If it is on a conjunctive ("and") basis, it can make the FAR tiny, but at a cost to the FRR. More sophisticated fusion algorithms try to get the best of both, but any fusion also adds cost in acquisition and processing resources.

Fusion is therefore the most promising strategy for virtually eliminating user inequalities and presentation attacks, but there is not a single fusion process that suits every deployment.[49]

Since the 1990s, there has been talk of unconventional modalities replacing the classic ones.[50] These include gait, typing speed, screen angle, electrocardiogram (ECG) rhythms, or odour. All of these provide evidence, but they are limited in terms of uniqueness, permanence, or sampling time. Gait, for example, is easily affected by factors like weight change (especially pregnancy), injury, or when carrying heavy bags.[51] The more internal modalities also raise the ethical issue of what happens when the data show a medical abnormality that might require treatment.

It is, however, the case that behavioural data – at the most basic level meaning time and approximate location, but potentially including soft biometrics or emotion detection – can be used to do an initial risk scoring of the interaction, enabling security measures to be scaled up or down as appropriate. These algorithms will inevitably become increasingly sophisticated, although the current capability of actual behavioural prediction is very limited. [52]

Conclusion

Before any authentication or identification solution is developed, it is right to ask whether biometrics is the best option, before getting into the details of modalities and thresholds. The answer is often, though not always, yes. When designed well and deployed with appropriate regulation, biometric technologies can solve many policy, commercial and individual problems.

It is important, however, to consider thoroughly the various drivers around cost, accuracy, friction, resistance to attack, public acceptability and legal compliance, before narrowing down to the best option. The consequences of getting that wrong could be significant, as there is clearly strong and increasing public interest in biometrics.

It is indeed hard to overestimate the importance of biometrics to society. The need to demonstrate identity is just so central and so diverse. Biometric systems are not perfect – no such system is. But they represent the best-known solution to a set of major and growing issues. As such, the future of biometric and authentication technologies looks to be innovative and dynamic.

Acknowledgements

The preparation of this report was led by Marcus Besley, Government Office for Science.

The Government Office for Science would like to thank all those who provided expert input to this report, including:

Dr Tony Mansfield, National Physical Laboratory.

Professor Sarah Stevenage, University of Southampton.

From the Home Office – Professor John Aston, Alex MacDonald, Sanaya Thethy, Quentin Revell and Carrie Golding.

Endnotes

1 http://www.iata.org/pressroom/pr/Pages/2017-10-24-01.aspx

2 https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels

3 Sir William J. Herschel, *The Origin of Finger-printing*, OUP, 1916, p19

4 https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/

5 https://americansecuritytoday.com/russian-chinese-firms-win-nistiarpa-face-recog-contest/

6 https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

7 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4580999/

8 Sir Francis Galton, *Finger Prints*, Macmillan, 1892, p110

9 http://biometrics.cse.msu.edu/Presentations/AnilJain_UniquenessOfFingerprints_NAS05.pdf

10 Stan Li and Anil Jain, *Encyclopedia of Biometrics*, Springer, 2009, p532

11 Home Office figures, May 2018

12 https://findbiometrics.com/interview-with-james-hammond-associate-vice-president-for-information-technology-winthrop-university/

13 http://www.nec.com/en/global/techrep/journal/g16/n01/160108.html

14 http://www.cse.nd.edu/BTAS_07/John_Daugman_BTAS.pdf

15 https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/PublishedAlgs.aspx

16 http://www.cs.joensuu.fi/~sahid/Sahidullah_fil/IEEE-INDICON15-Comparison.pdf

17 http://www.biometricupdate.com/201709/applied-recognition-achieves-new-benchmark-for-face-recognition-accuracy

18 http://www.pbs.org/wgbh/nova/next/tech/the-limits-of-facial-recognition/

19 Research by Dr Tony Mansfield and Aruna Shanoy, National Physical Laboratory, 2018

20 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" in *Proceeds of Machine Learning Research 81:1-15*, 2018

21 https://www.ibm.com/blogs/research/2018/02/mitigating-bias-ai-models/

22 Neil Yager and Ted Dunstone, "The Biometric Menagerie" in *IEEE Transactions on Pattern Analysis and Machine Intelligence,* Vol. 32, No. 2, February 2010

23 David Sidlauskas and Samir Tamer, "Hand Geometry Recognition" in *Handbook of Biometrics*, Springer, 2008, p91

24 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3758647/

25 Adapted from https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78

26 https://en.wikipedia.org/wiki/Password_cracking

27 Matthew and Anderson, *Developing Coercion Detection Solutions for Biometric Security*, SIA Computing Conference 2016

28 "Bond Fingerprint Technology" - https://www.youtube.com/watch?v=yP5ku2IJgAY

29 https://www.wired.com/story/hackers-say-broke-face-id-security/

30 Graham Greenleaf, *Global Data Privacy Laws 2017*, University of New South Wales, 2017

31 http://www.dw.com/en/germanys-facial-recognition-pilot-program-divides-public/a-40228816

32 https://www.mwe.com/en/thought-leadership/publications/2017/11/surge-in-lawsuits-under-illinois-biometrics-law

33 https://www.bakermckenzie.com/en/insight/publications/2017/10/illinois-biometric-information-privacy-act/

34 https://www.theguardian.com/politics/2009/may/07/dna-database-plans-condemned

35 https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection

36 https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data/

37 http://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html

38 http://www.thehindu.com/news/national/constitutional-validity-of-aadhaar-the-arguments-in-supreme-court-so-far/article22752084.ece

39 https://mashable.com/2017/07/28/russia-facial-recognition-emotion-ntechlab-findface

40 Stephen Bertman, *Handbook to Life in Ancient Mesopotamia*, OUP, 2005, p235

41 *Howley v. Whipple*, Supreme Court of New Hampshire, 48 NH 487

42 https://futurewrite.com/presentations/rich-miner.pdf

43 https://www.theguardian.com/money/2017/sep/09/secure-smartphone-app-replace-fraud-prone-paper-passports

44 https://www.techlicious.com/guide/5-futuristic-smart-locks-for-your-home/

45 https://www.usatoday.com/story/tech/talkingtech/2017/07/25/do-microchip-implants-pose-health-risks-ask-swedes-and-pets/507408001/

46 https://www.theverge.com/circuitbreaker/2016/8/13/12460542/mit-microsoft-research-gold-leaf-smart-temporary-tattoo

47 https://www.airport-technology.com/features/featurea-world-first-australias-plan-for-advanced-biometric-airport-checks-5808560/

48 Mario Savastano, "Noncooperative Biometrics: Cross-Jurisdictional Concerns" in *Human Recognition in Unconstrained Environments*, Elsevier, 2017, p219

49 Tabassi, Quinn, Grother, "When to Fuse Two Biometrics" NIST, 2006

50 https://www.wired.com/1997/07/biometrics-2/

51 For more detail, see *Forensic gait analysis: a primer for courts*, The Royal Society, 2017

52 See https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition

This publication available from www.gov.uk/go-science

Contact us if you have any enquiries about this publication, including requests for alternative formats, at:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
Email: contact@go-science.gsi.gov.uk