Snapshot Series
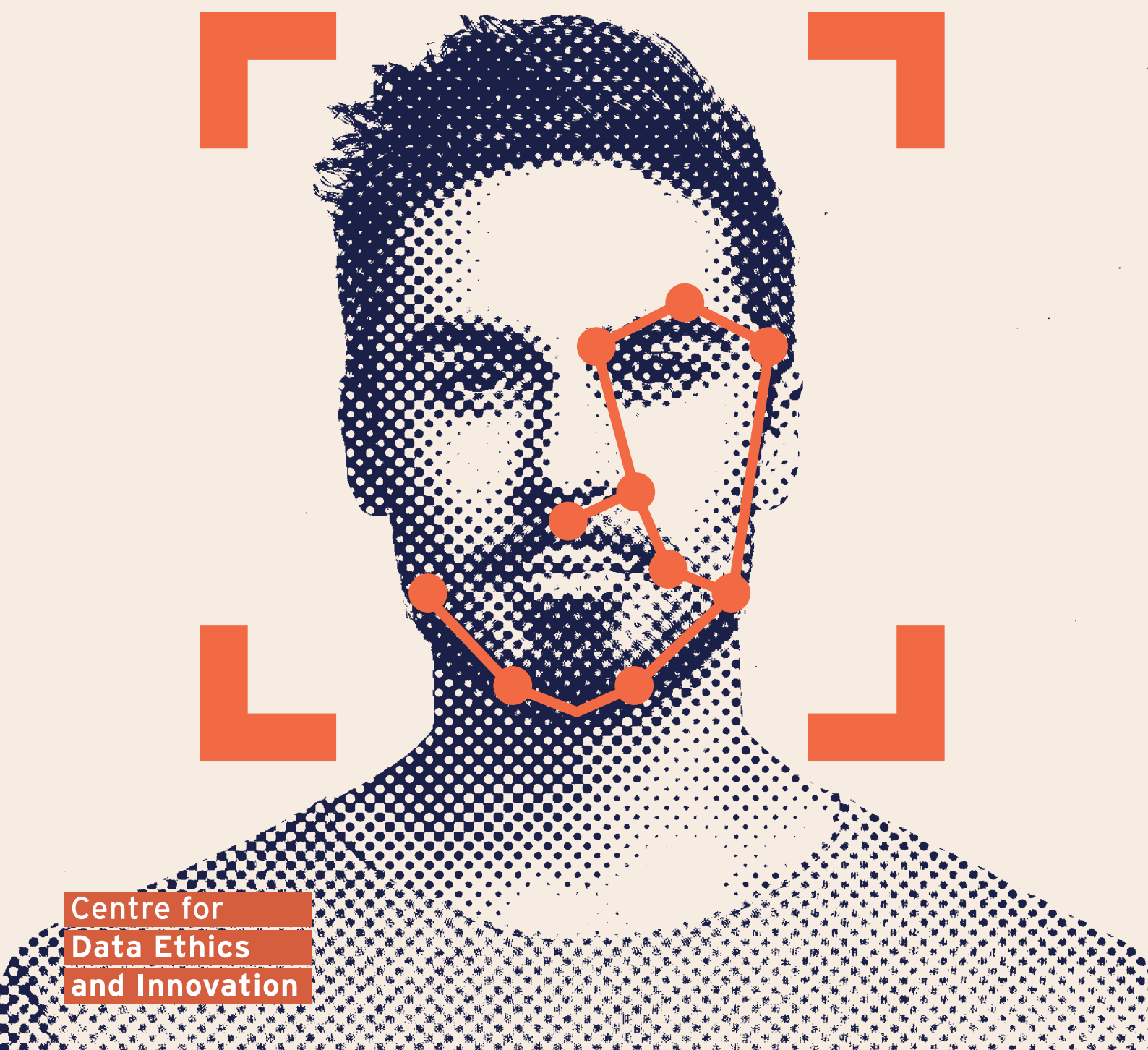
Facial Recognition Technology

May 2020

Centre for
Data Ethics
and Innovation

Contents

About this CDEI Snapshot Paper

The Centre for Data Ethics and Innovation (CDEI) is an independent expert committee, led by a board of specialists, set up and tasked by the UK government to investigate and advise on how we maximise the benefits of AI and data-driven technology.

Our goal is to create the conditions in which ethical innovation can thrive: an environment in which the public are confident their values are reflected in the way data-driven technology is developed and deployed; where we can trust that decisions informed by algorithms are fair; and where risks posed by innovation are identified and addressed.

The paper distinguishes between proven fact and speculation, and illustrates how FRT can have markedly different implications for society depending on the type of system and the reasons for its use.

In developing this Snapshot Paper we spoke with the following people and organisations:

- **Andrew McStay** (Professor of Digital Life, Bangor University)
- **Margaret Mitchell** (Senior Research Engineer, Google)
- **Michael Veale** (Lecturer in Digital Rights and Regulation, University College London)
- **Karl Ricanek** (Professor of Computer Science, University of North Carolina)
- **Hassan Ugail** (Professor of Visual Computing, University of Bradford)
- **Peter Fussey** (Professor of Sociology, University of Essex)
- **Alexander Babuta** (Research Fellow, Royal United Services Institute (RUSI))
- **Marion Oswald** (Founder, Centre for Information Rights, RUSI & University of Winchester)
- **Lilian Edwards** (Professor of Law, Innovation and Society, University of Newcastle)
- **Rowland Manthorpe** (Technology correspondent, Sky News)
- **Ruth Boardman** (Partner, Bird & Bird)
- **Julie Dawson** (Director of Regulatory & Policy, Yoti)
- **Johanna Morley** (Technology Lead for Facial Recognition, Metropolitan Police Service)
- **Lindsey Chiswick** (Head of Intelligence and Covert Policing, Metropolitan Police Service)
- **Matt Jukes** (Chief Constable, South Wales Police)
- **Tony Porter** (Surveillance Camera Commissioner)
- **Paul Wiles** (Biometrics Commissioner)
- **Anne Russell** (Information Commissioner's Office)
- **Peter Brown** (Information Commissioner's Office)
- **Carl Wiper** (Information Commissioner's Office)
- **Jonathan Langley** (Information Commissioner's Office)
- **Griff Ferris** (Big Brother Watch)
- **Jacob Ohrvik-Stott** (Doteveryone)
- **Hannah Couchman** (Advocacy and Policy Officer, Liberty)
- **Lynette Webb** (Google)
- **David Frank** (Microsoft)
- **Dave Sumner** (Facewatch)
- **Nelson Wootton** (Facewatch)
- **Suzanne Shale** (London Policing Ethics Panel)
- **Nina Hallowell** (Biometrics & Forensics Ethics Group)
- **Home Office**
- **Department for Digital, Media, Culture, and Sport**

Summary

1. **Facial Recognition Technology (FRT) refers to algorithms which estimate the degree of similarity between two faces.** FRT can be used to verify someone's identity (e.g. to unlock an electronic device) or to identify individuals (e.g. scanning a group of people to see if anyone is on a watchlist).

2. **FRT is used across a range of contexts, from personal devices, to social media, to policing.** The technology can be used retrospectively or live, and it can be fully automated or used to assist humans. The extent to which an FRT system is helpful or detrimental to society depends on the context, as well as the accuracy and biases of the specific algorithm deployed. Each use must be assessed according to its own merits and risks.

3. **Whilst FRT can provide additional security when accessing devices and places**, and increased efficiency in a number of settings, its increasing prevalence has concerned civil society groups and political leaders. Objections centre on the potential for some uses of FRT, particularly when live FRT is used in public settings, to i) undermine individual privacy; ii) entrench bias and unequally distributed consequences, especially where systems have different accuracy rates for different demographic groups; and iii) bestow private and public organisations with disproportionate power to surveil the population, potentially leading to worrying consequences for rights such as freedom of expression and association.

4. **Several police forces have undertaken trials of live FRT systems** to identify persons of interest and the Metropolitan Police are now deploying the technology operationally. These and other deployments of FRT for the purposes of law enforcement are regulated by the Data Protection Act, Human Rights Act, Equality Act, and the Protection of Freedoms Act, amongst other legislation. Contrary to popular belief, the use of FRT in policing is not unregulated.

5. **Until recently, the legality of FRT use by the police had yet to be formally tested.** In the summer of 2019, however, civil liberties group Liberty took South Wales Police (SWP) to court on the basis that their use of live FRT on members of the public had breached the Human Rights Act, the Data Protection Act, and the Equality Act. The high court ruled that there is a clear and sufficient legal framework to ensure the appropriate and non-arbitrary use of live facial recognition, and that SWP used live facial recognition in a way that abided by this legal framework.

6. **Despite the ruling on the legality of FRT's use, some civil society groups believe the current safeguards are insufficient to protect people's privacy and freedoms, while others believe this technology should not be used by the police at all.** As such, Liberty has been granted an appeal of the high court's decision, and the case will be heard by the Court of Appeal in June 2020. Elsewhere, the Information Commissioner's Office (ICO) has called for a new code of practice to give specific guidance to police forces on how to deploy FRT and ensure consistent interpretations of this decision.

7. **FRT has also seen increasing use in the private sector, where it is being applied to identify known shoplifters or people engaged in antisocial behaviour in stores,** as well as to anonymously track the movements of customers for marketing purposes. Data Protection legislation is the only major regulation that sets limitations on the use of FRT in this context, and there is no exact interpretation of the conditions it sets.

8. **Regulators, politicians and civil society groups will continue to scrutinise the governance regime for FRT in the months ahead.** In doing so, they should seek to answer several outstanding questions, among them how to meaningfully involve the public in deciding whether this technology should be used, and what for; whether oversight in the private sector needs to be strengthened; and if and how the governance of FRT should factor in developments in other forms of biometric recognition technologies.

9. **Over the coming months, the CDEI will continue to examine the impact of FRT on society.** We are particularly interested in exploring how FRT is being used in the private sector, and whether the UK's current arrangement of laws and oversight bodies is equipped to minimise the harms posed by this technology.

10. **In the meantime, with regards to the use of live FRT in law enforcement, the CDEI expects police forces to be appropriately transparent about how they use this technology,** including where it is deployed, the basis by which people are included on watchlists, and how deployments are signed off. We support calls for greater consistency in how live FRT is used by different forces, including having minimum safeguards in place before each rollout is confirmed.

What is Facial Recognition Technology (FRT)?

01

What is FRT?

Facial recognition technology refers to algorithmic systems (and the associated hardware) that can analyse a person's face to make claim of an identity. It is a form of biometric technology: much like a fingerprint scan finds patterns in fingerprints, facial recognition technology finds patterns in the measurements of a face to create a 'template' of a face, then looks for similarities between two templates. It is also a statistical system, in that it estimates this similarity with a certain degree of error.

Two main types of facial recognition are used to make a claim of identity: [1]

1. Facial Verification

(One-to-one matching): These systems try to determine whether a face matches with a single facial template, often saved on a device. Many phones and laptops are now embedded with verification technology, allowing users to log on to their devices more securely. Facial verification can also be used to facilitate secure entry into buildings, to match against a passport at an e-gate border crossing, or to prove one's identity to access public services online.

2. Facial Identification

(One-to-many matching): These systems try to determine whether a face matches with any facial template in a database of individuals. These databases can be of any size, sometimes running into millions of images. Facial identification technology is used in varied settings, including by Facebook to suggest friends to tag in photos, and by the police and private security to locate people of interest in a crowd.[2] This also includes use-cases where a name is not attached to the template, but an individual is still uniquely identified and tracked, for instance analysing customer movements around a retail store.

1. "Information technology — Vocabulary — Part 37: Biometrics". International Organization for Standardization. 2017.
2. At least three police forces in the UK have trialled the use of live facial recognition systems, the Metropolitan Police, South Wales Police and Leicestershire Police. Police use of retrospective facial identification analysis, for example to analyse crime scene footage, is widespread.
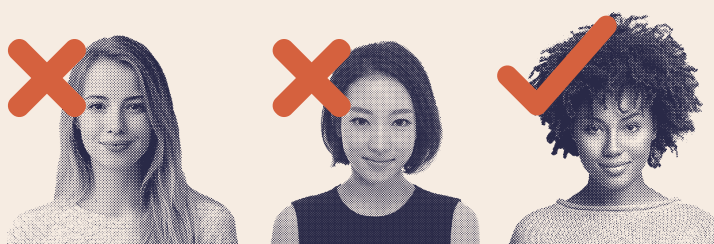
1.
Facial
Verification

Match

No match

2.

Facial

Identification

What are 'Biometrics'?

Biometrics enable the recognition of individuals based on their biological and behavioural characteristics.[3] Facial images are one form of biometric data. Others include DNA, fingerprints, irises, and voice.[4] The field of biometrics is growing as new technologies are able to measure subtle biological differences between individuals. For example, a person's gait or the shape of the veins in their hands are also ways in which to identify someone.

Deployments of FRT can be retrospective, analysing previously collected images, or live, processing faces in real time. Systems also differ in their degree of automation, either being automated and acting directly on the output of the algorithm, or instead assisting human arbitration. Most forms of facial verification (one-to-one) systems are fully automated, with a match being sufficient to result in an action (e.g. to unlock a phone). Facial identification systems are more likely to assist, with someone deciding whether and how to act on a result (e.g. an operator deciding whether to follow up on an FRT match that indicates someone is a person of interest).

Alongside facial verification and facial identification are systems that categorise people and infer characteristics about them. Facial analytics systems are designed to reveal the demographic traits of a subject, including their gender, age, race, health or body mass index. The technology works by examining the features of a face, for instance the shape of the eyes and the colour of the hair, which may be correlated with particular demographic groups. Affective computing, meanwhile, attempts to infer someone's emotional state by analysing their facial expressions, along with their tone of voice, posture, and other physiological features. Each type of FRT brings with it new opportunities as well as ethical and legal challenges.

The focus of this Snapshot is the use of facial verification and facial identification technology, as these are the most widely deployed technologies, present similar risks, and have attracted the greatest public concern. Future CDEI research may explore the unique implications of facial analytics and affective computing in more depth.

---

3. "Information technology — Vocabulary — Part 37: Biometrics". International Organization for Standardization. 2017.
4. "What are Biometrics?". Kaspersky. 2019.

02

How does FRT work?

The implications of FRT become clearer when looking at how the technology is developed and deployed in practice. This means looking at how the system is designed, how and where facial image databases are collated, and the way in which human operators engage with a system's results (if it is not fully automated).

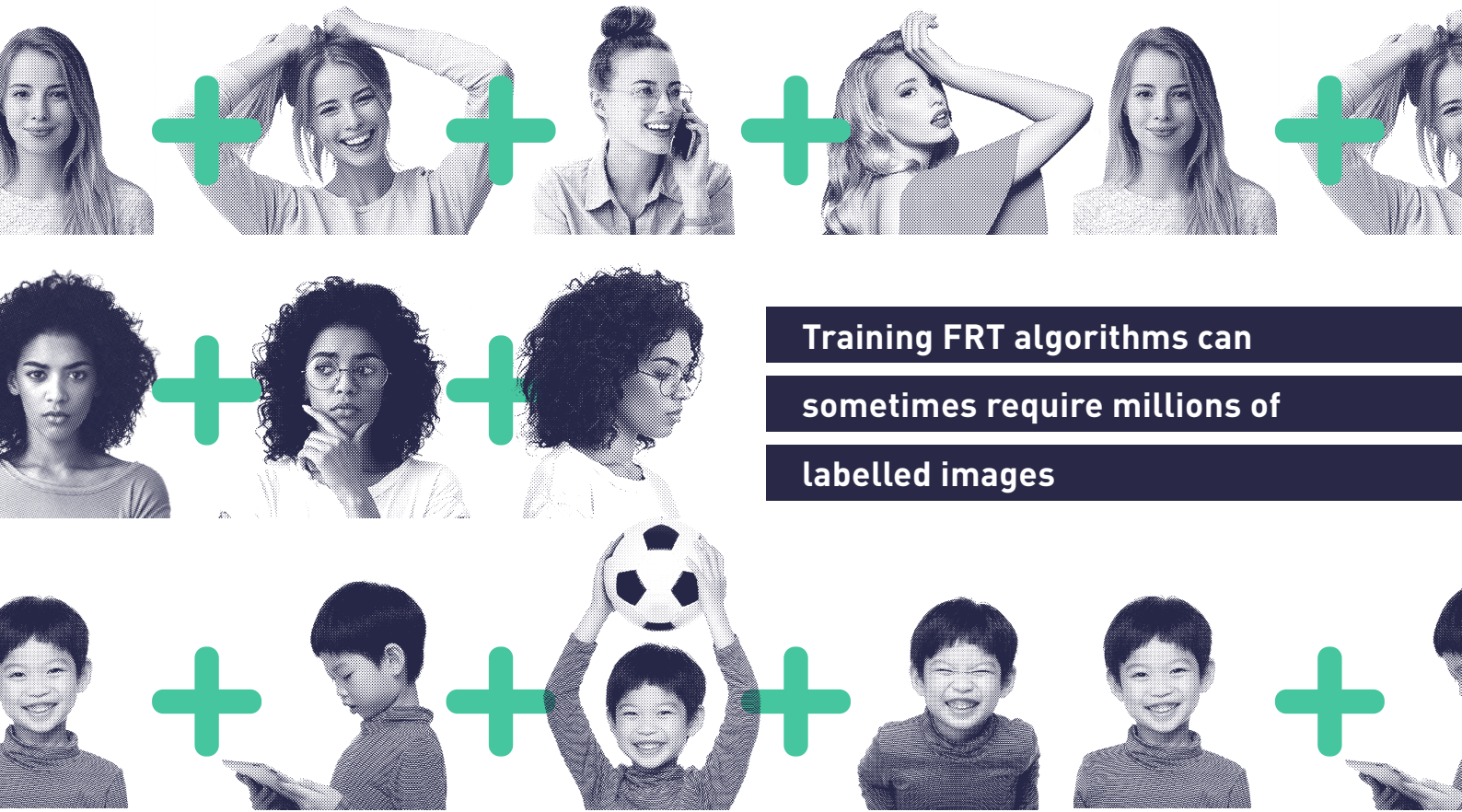The lifecycle of the application and use of FRT can involve four main stages:

1. Development

2. Deployment

3. Result

4. Execution

What follows is a description of one approach to building FRT systems using modern machine learning technology.

1. Development

Training FRT algorithms can sometimes require millions of labelled images

Most FRT software has two key functions: i) to identify the presence of a human face in an image, and ii) to map the key features within that face, which allows comparisons to be made.

FRT software can find the features that are most useful in distinguishing between faces based on a number of approaches. These include defined rules (e.g. patterns of light and dark around a person's nose or eyes), or from training on a large number of other facial images. A finished FRT system can recognise similarities between faces, even when they are viewed in different conditions, but training FRT algorithms can sometimes require millions of labelled images and a great deal of computational time. Google used a dataset of 200 million facial images over four weeks to train an FRT system in 2016 (although large training datasets may not always result in more accurate

systems if they are homogeneous). [5] If using FRT in conditions which cannot be easily controlled, e.g. using CCTV camera footage, it becomes even more important than usual that training sets feature a range of faces shown at different angles and exposed with different lighting conditions.

Most organisations using trained FRT will not conduct the training themselves, and will instead purchase a pre-trained algorithm from a company with sufficient scale to do this work. This may limit transparency into how these algorithms are designed and the data they are trained on. Large technology firms develop a number of the most popular products and provide their functionality to smaller firms via APIs (Application Programming Interfaces, which are a set of shared tools to build software applications). These products include Amazon's Rekognition, Microsoft's Azure Face and NEC's NeoFace.

[5.] Schoff, Florian., Kalenichenko, Dmitry., and Philbin, James. "FaceNet: A Unified Embedding for Face Recognition and Clustering". 2015

2. Deployment

Once developed, FRT can be deployed in real world settings to verify or identify individuals as they feature in new image data, either in the form of digital photographs or video footage. Users of FRT systems should test and trial their models to ensure they are fit for purpose before deploying them.

Step one of the FRT process involves detecting when a face is present and then cropping this segment of the image in order to remove as much background 'noise' as possible. This is done to ensure the FRT software only analyses relevant pixels in an image.

The FRT software will then analyse the face and create an array of numbers – also known as a 'template' – that represent its features and their position in relation to one another. With facial verification, the finished template is then compared with the template generated from another facial image, which is often stored locally, for instance in a biometric passport or on a phone. For identification, the template is compared with all templates in a database to find the closest matches.

Detect a face

7 8 5 1
2 7 6 5
3 3 4 2
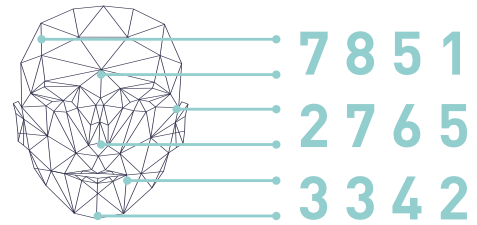
Analyse the face and create a numbers-based template

Compare with target templates in a database, to find the closest matches

3. Result

The third stage sees the system present its result. Given that no FRT software is completely accurate, results are framed in terms of a 'similarity score' between the two facial image templates. Higher numbers imply that the faces are more similar, but it is hard to interpret anything beyond that fact as the calculations are often unique to the system and proprietary.

When looking for binary match/no-match decisions, it is up to the organisation deploying FRT software to determine an acceptable 'similarity threshold' – the lowest score that is counted as a positive match. Setting this threshold is a critical decision. In circumstances where false positives (that is, wrong identifications) can be tolerated, for example where people are suggested for tags in Facebook photos, the threshold can be set relatively low. However, when the stakes are high, for instance when FRT is used to give people secure access to their bank account, one might expect the similarity threshold to be set at the upper end of the scale, strictly preventing unauthorised access while accepting the risk that a customer may not be able to get in themselves.

Given that no FRT software is completely accurate, results are framed in terms of a 'similarity score' between the two facial image templates.

4. Execution

Except for fully automated FRT systems (e.g. those used to unlock devices on a mobile phone), any matches made by the software will be passed on to a human operator, who will then make the final decision on whether to act on the result.

This could be, for example, a security guard deciding whether to intervene with a potential shoplifter. The quality of the operator's judgement will depend on the level of training they receive, their skill in questioning a person about their identity, and the time they have at their disposal to do so (e.g. to talk with the person if they are in their immediate vicinity). Judgements will also depend on the innate ability of individual operators, as well as the specific conditions they are working in. It is important to note that human operators may also have innate biases and are likely to be better at distinguishing and recognising faces from their own ethnic background than from other backgrounds.[6]

6. Meissner, Christian A., Brigham, John C., "Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review." Psychology, Public Policy, and Law, 2001

What do we mean by an accurate system?

Simply talking about 'accuracy' can be problematic when evaluating the effectiveness of FRT systems, especially when matches are expected to be rare. If 99% of people are not on a watchlist, a system could achieve an accuracy of 99% simply by matching no-one, while never finding any of the 1% of people it sets out to. To evaluate a system, we therefore need to know both the proportion of people the technology should have matched but missed (false negatives) and the proportion of people it matched but shouldn't have (false positives).

While a good FRT system will have low errors for both, there is always a trade-off between these two aims in any system. The decision of how to balance these errors can be made by raising or lowering the similarity threshold, and will depend on the context.

A/ False negatives (should have matched but missed)

False negative

B/ False positives (matched but shouldn't have)

False positive

Where is FRT being used today?

03

Where is FRT being used today?

FRT has proven popular with public and private sector organisations alike. Some police forces, property developers and retailers are now using the technology, while some banks and tech firms have already embedded it within their products and services. In a short space of time, FRT is now visible across many areas of our lives.

Use of Facial Verification Systems

The most common use of facial verification is within personal devices, where the technology is used to unlock mobile phones, tablets, and laptops without the need to type in a password. In the banking sector, facial verification systems are helping to authenticate people against the identification they provide when setting up an account (e.g. with providers like Monzo and Revolut). Border control is another area where FRT is being used. Most major UK airports have now installed 'eGates' that use 1:1 facial verification systems to help with passport checks.[7]

Use of Facial Identification Systems

Facial identification systems are most visible on social media, such as on Facebook or Google Photos, where they automatically identify the same face across multiple images, and in the case of Facebook suggest linking this face to a profile. The police similarly use facial identification retrospectively, for instance on still images taken from CCTV or social media, to identify someone who they believe is a suspect against their custody image database or with images acquired from elsewhere.

7. UK Border Force. "Guide to faster travel through the UK border". GOV.UK. May, 2019.

8. Davies, B., Innes, Martin., and Dawson, Andrew. "An evaluation of South Wales Police's use of automated facial recognition". Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University. September 2018.

9. Metropolitan Police. "Standard operating procedure (SOP) of the overt deployment of live facial recognition (LFR) technology".

Most of the public commentary and controversy, however, has focused on the use of live facial identification in public places. The most high profile deployment in the UK has been in policing, where three UK forces (South Wales Police, Leicestershire Police and the Metropolitan Police Service) have trialled and used live forms of FRT to locate individuals in crowds in real time. South Wales Police (SWP), for instance, have used the technology near football matches and music concerts, public demonstrations, and during a royal tour. [8] In January 2020, the Metropolitan Police Service (MPS) announced they would be deploying FRT operationally to "[target] those wanted for imprisonable offences, with a focus on serious crime, with a particular regard to knife and gun crime, child sexual exploitation and terrorism." [9] Their Standard Operating Procedure lists examples for who could be included on a watchlist, including wanted people, missing people, and other people of interest to the police. [10]

This use of live facial identification extends into private security, with many commercial firms reportedly using it to safeguard their premises. Property developer Argent, for example, recently used FRT on its 67-acre site in Kings Cross, which is home to a university, several major employers, and a large transport hub, whilst a private site in Canary Wharf is seeking to use FRT for a similar purpose. [11] FRT is also being used by individual retail shops to flag the presence of known shoplifters. [12] Facewatch, a supplier of facial identification systems, manages a shared watchlist of individuals that are deemed suspicious, sourced from and deployed across 15 household name retailers. It says that it expects to install 5,000 FRT-enabled cameras across private premises by 2022. [13] This use cannot be easily disentangled from the use by law enforcement as they may share watchlists, as in the King's Cross example where the MPS provided images to Argent. [14]

In the retail sector, meanwhile, facial identification systems are being used by some shopping centres to track the movements of customers – information that can be aggregated and then used for marketing purposes and to inform the design of buildings and shop fittings. The UK FRT company Springboard promises retailers a detailed understanding of customer behaviour, including information about the average time they spend queuing, dwelling, and travelling in store. [15] Some companies, such as Panasonic, let retailers tie these movements to an individual's account, enabling them to track repeat customers. [16]

The most high profile deployment in the UK has been in policing, where three UK forces have trialled live forms of FRT to locate individuals in crowds in real time.

10. Murgia, Madhumita. "London's King's Cross uses facial recognition in security cameras". The Financial Times. August 2019; and Kleinman, Zoe. "King's Cross developer defends use of facial recognition". BBC News. August 2019.

11. Chivers, Tom. "Facial recognition... coming to a supermarket near you". The Guardian. August 2019.

12. Devlin, Hannah. "'We are hurtling towards a surveillance state': the rise of facial recognition technology." The Guardian. October 2019.

13. Kelion, Leo. "Met Police gave images for King's Cross facial recognition scans". BBC. September 2019.

14. See https://www.spring-board.info/technology for more details.

15. See Panasonic Business's "FacePRO™ Facial Recognition System with Deep Learning Technology".

16. See Panasonic Business's "FacePRO™ Facial Recognition System with Deep Learning Technology".

What are the main benefits and risks of FRT?

04

What are the main benefits and risks of FRT?

FRT has proven controversial. Some believe it will make our streets safer, our bank accounts more secure, and our public services more efficient and accessible.

Yet others see the technology as a tool of mass surveillance that will erode privacy and undermine human rights. These disagreements mirror a wider debate in society about the trade-offs between privacy and public security, which has been ongoing since the introduction of the first surveillance technologies. The following section summarises the claims made about FRT by its proponents and critics. Note that many of these refer to hazards rather than proven harms, and that an effective governance regime may be able to manage the risks posed by FRT.

Benefits

Security

FRT could strengthen access security in a number of settings, making sure that online bank accounts, personal devices such as phones and laptops, and private premises are only accessible to those with permission.

- Faces have the advantage of being easier to analyse from a distance and can often rely on existing camera technology. As such, they are particularly useful for the security of public spaces, as the objective is often to identify someone from a distance without their active participation.

- It should be noted that whilst the best FRT systems can perform in the accuracy range of professional facial examiners, optimal facial identification is best achieved when humans are involved in the process.[17]

Efficiency

FRT systems, given the right conditions, can instantaneously verify an individual's identity or spot people in a crowd, saving human labour and increasing efficiency across a number of services.

- US flight operator Delta Airways claim their new FRT system will shorten the boarding time for a plane of 270 passengers by around 9 minutes.[18] For an airport like Heathrow, which has 1,300 flights a day, the time saved could be as much as 195 hours over every 24 hour period. These savings in turn could allow workers to focus on tasks that make better use of their skill sets, including those that machines still struggle to automate.

- Efficiency savings can also be passed on to users or customers, for example, with FRT allowing people to open a bank account more easily.

Scale

By increasing the speed of individual identity checks, FRT makes new forms of security infrastructure possible.

- This is especially true in the context of facial identification in policing, where it would not be feasible for humans to check a face or a crowd against a database of thousands of people without digital assistance.

- Unlike human reviewers, algorithmic systems do not suffer from fatigue, nor are they distracted - two limitations that can slow down decision-making and result in substandard judgements by humans alone.

---

17. Raddatz, Kate. "Facial Recognition Coming To Delta Gates At MSP". CBS Minnesota. June, 2019.
18. Users may have given permission for their data to be used in such a way, but they may not realise they had done so. Few users of social media or photo sharing platforms read the often very long Terms & Conditions that describe how these platforms can use their personal data.

Risks

Risks to individual privacy

Threats to privacy can occur at different stages of the life cycle of an FRT system, from training through to execution.

- The volume of facial images often required to train these systems has seen technology companies resort to gathering large quantities of photographs from the internet, sometimes without the informed consent of the people featured within them. [19] In March 2019, for example, IBM was criticised for using close to a million photos from Flickr to train its FRT software, many of which will feature individuals who would be concerned that their facial images had been used in such a way. [20] More directly, a contractor for Google was found to be paying black people $5 to collect images of their face to improve the accuracy of their system, targeting homeless people and students in particular, without informing them what it would be used for. [21]

- The deployment of live facial identification systems in public places may interfere with the privacy of anyone in that place, since the systems scan the faces of every individual who passes through the vicinity where footage is collected – without explicit consent, and potentially without their knowledge if they have not been sufficiently notified. It is important to note however, that in most cases only the facial data of individuals who are flagged as a match is retained beyond the initial facial scan.

- Live FRT also poses a risk to privacy in the sense that it allows people's whereabouts to be revealed as they pass by cameras. The use of live FRT in commercial settings, for example, would enable retailers and others to know when particular individuals enter their premises, thereby diminishing people's ability to move about anonymously. The significance of this risk depends on how this information is stored and whether operators are likely to misuse the data (e.g. for the purposes of tracking individuals).

Inaccuracy and bias

FRT systems have become increasingly accurate in recent years, with the best algorithms getting 20 times better between 2014 and 2018. [22] Nevertheless, they will always be prone to a degree of error and some critics believe they are not yet ready for deployment in sensitive contexts.

- Bias is not an inevitable feature of these algorithms, however at present the majority of FRT systems have different accuracy rates dependent on ethnicity, sex and age, with performance often worse when recognising Black and Asian people, as well as women. [23] This could partly be the result of a lack of representative training data. [24] Differential accuracy can create additional barriers or disincentives for underrepresented groups when accessing key services. When assessing bias in FRT systems, it is important to be mindful of the bias that may be present in conventional identity-checking procedures (i.e. in human-only identity checks).

> **...at present the majority of FRT systems have different accuracy rates dependent on ethnicity, sex and age**

- Any bias or inaccuracy takes on greater significance in the context of policing. The Metropolitan Police Service (MPS) have configured their system to achieve a false positive rate of less than 1 in 1000 passers-by. However, due to the large number of people scanned compared to the watchlist, a substantial proportion of matches may still be inaccurate and lead to false interventions. An independent review of the MPS trials between 2018 and 2019, showed that of the 42 matches

---

19. Users may have given permission for their data to be used in such a way, but they may not realise they had done so. Few users of social media or photo sharing platforms read the often very long Terms & Conditions that describe how these platforms can use their personal data.

20. BBC. "IBM used Flickr photos for facial-recognition project". BBC News. March, 2019.

21. Carrie Wong, Julia. "Google reportedly targeted people with 'dark skin' to improve facial recognition." The Guardian. October 2019.

22. Boutin, Chad. "NIST Evaluation Shows Advance in Face Recognition Software's Capabilities. National Institute for Standards in Technology". National Institute of Standards and Technology. November 2018.

23. Grother, Patrick., Ngan, Mei., and Hanaoka, Kayee. "NISTIR 8280 - Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects". National Institute of Standards and Technology. December, 2019.

24. A hypothesis supported by the absence of bias against East Asian people by algorithms produced in China

produced by the software, 16 were rejected by the human operator as not credible, 4 people were lost in the crowd, 14 were wrongly stopped, while 8 were correctly stopped. [25] South Wales Police (SWP) published statistics showing 96 matches from their trials in 2019, with 56 rejected by the operator, 13 people not stopped, 4 falsely stopped, and 23 correctly stopped. [26]

- The distribution of false positives and incorrect interventions will depend on the demographic make-up of the watchlist, as well as that of the people scanned, even when the underlying algorithm has no in-built bias.

- Live FRT also has limitations when people do not want to be identified, as these systems can be deliberately evaded. Special types of clothing and sunglasses have been shown to fool some systems, raising some doubts about the ability of FRT to identify wanted individuals when used overtly.

Power imbalance

As FRT becomes more accurate, it could place a disproportionate amount of power in the hands of its operators.

- The extent of this power will depend on who is targeted on watchlists, and where and when FRT operators are deploying the technology. As the ICO noted in their recent opinion, a police force using a watchlist of a handful of terrorist suspects at a high-profile public event will present a different order of concern to them keeping a watchlist of thousands of petty criminals and deploying the technology routinely. The creation and maintenance of watchlists by private organisations deserves particular attention, as there are no commonly agreed rules to govern who can and cannot be included.

- Concern has been expressed that use of live FRT in public spaces, especially at demonstrations such as the use by SWP at protests of the Cardiff Arms Fair, might have a chilling effect on our democracy. People may be discouraged from voicing discontent if they believe, for example, that their presence could be identified at demonstrations.

The degree of risk that FRT poses to society will depend on the type of system being used and the manner of its deployment. FRT systems are not universally beneficial or harmful, and the acceptance of the technology in one context does not mean it will be accepted in another. The Ada Lovelace Institute's 2019 survey of the UK public, for example, found that while 29 percent are uncomfortable with police forces using FRT systems, this number increases to 67 percent when thinking about its use in schools and 61 percent when thinking about its use on public transport. [27] One reasonable conclusion to draw from the limited body of evidence available today is that FRT presents greater hazards when used to identify individuals than to verify them, particularly when that identification is live and occurs in public settings.

25. Fussey, P., and Murray, D. "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology." Essex Human Rights Centre. 2019.
26. Information Commissioner's Office. "Lawful basis for processing".
27. European Data Protection Board. "Guidelines 3/2019 on processing of personal data through video devices". July, 2019

What laws and regulations govern the use of FRT?

05

What laws and regulations govern the use of FRT?

The last chapter detailed several hazards posed by FRT systems. Many of these hazards, however, can be contained through an effective governance regime. Some groups argue that FRT is insufficiently governed to diminish the chance of harm, with few boundaries on how it can be applied in either the public or private realms. A House of Commons Science and Technology Committee report, for example, warned that FRT suffers from a "regulatory lacuna". [28] Yet while there is no one specific law detailing the conditions under which FRT can be used, it is still governed by several UK laws and regulators.

does not receive the explicit consent of every individual whose data is processed, they must show that collecting facial data is necessary for reasons of substantial public interest. Additionally, private organisations cannot process data about criminal offences except in narrowly defined circumstances (such as when necessary for legal proceedings).

The ICO is currently investigating whether the use of a facial identification system by a property developer in Kings Cross for security purposes breached the DPA. [31] A central concern is that the surveillance occurred without the knowledge of people walking through the vicinity, and the investigation will, amongst considerations such as fairness and transparency, look at whether this deployment was necessary to achieve a substantial public interest and whether any criminal offence data was used.

Private Sector Use

The Data Protection Act 2018 (DPA) (which implements the EU's General Data Protection Regulation (GDPR) and Law Enforcement Directive) is applicable to all uses of FRT, both private and public, and is enforced and regulated by the Information Commissioner's Office (ICO).

Under data protection legislation, organisations must use data in a lawful, fair, and transparent way. To be lawful in the case of private organisations means they have a lawful basis for collecting and processing data.[29] In scenarios where FRT is used for private security purposes, the relevant basis is often the legitimate interests of the data controller which must be weighed on a case-by-case basis against the rights of individuals [30] (for other possible lawful bases, see the ICO's guidance). As facial templates are biometric data that can identify individuals, they are also considered special category data and users of FRT must therefore meet additional requirements beyond those governing the deployment of general video surveillance technology. When the organisation

Police use

Part 3 of the Data Protection Act 2018 implements the Law Enforcement Directive governing police use of data. While the police have broad powers under their common law obligation to detect and prevent crime, they must only collect and process biometric data when it is strictly necessary and proportionate to achieve a law enforcement purpose. In their recent Opinion on police use of FRT, the ICO called for a new binding code of practice to give clearer guidance on what can be considered a strictly necessary deployment of FRT, including guidelines for targeted watchlists and locations.[32]

> **While there is no one specific law detailing the conditions under which FRT can be used, it is still governed by several UK laws and regulators.**

---

28. European Data Protection Board. "Guidelines 3/2019 on processing of personal data through video devices". July, 2019

29. Denham, Elizabeth. "Statement: Live facial recognition technology in King's Cross". Information Commissioner's Office. August, 2019.

30. ICO. "The use of live facial recognition technology by law enforcement in public places". October, 2019

31. Equality and Human Rights Commission. "Public Sector Equality Duty". April, 2019

32. Home Office. "Surveillance Camera Code of Practice". Presented to Parliament Pursuant to Section 30 (1) (a) of the Protection of Freedoms Act 2012. June, 2013.

Alongside the DPA, police use of FRT is governed by the Human Rights Act 1998, the Equality Act 2010, the Protection of Freedoms Act 2012, and the Regulation of Investigatory Powers Act 2000. The Human Rights Act lists a number of fundamental rights that must be protected by public bodies. In his recent assessment of the live FRT system used by the Metropolitan Police Force, Professor Peter Fussey suggested that at least four rights are of particular interest: the right to privacy (Article 8), the right to freedom of expression (Article 10), the right to protest and freedom of association (Article 11), and freedom from discrimination (Article 14). The Equality Act adds additional regulations on public bodies through the Public Sector Equality Duty, which obliges them to positively promote equality for people and groups with protected characteristics. [33]

Police use of FRT is also regulated by the Protection of Freedoms Act, which created the Surveillance Camera Code of Practice and the Surveillance Camera Commissioner to encourage compliance with the code.

Police use of FRT is also regulated by the Protection of Freedoms Act, which created the Surveillance Camera Code of Practice and the Surveillance Camera Commissioner to encourage compliance with the code. [34] This sets out 12 principles for public authorities to follow as they deploy surveillance cameras or use information gathered from them, including providing transparency, accountability, and meeting technical standards. The Surveillance Camera Commissioner released guidance for police forces to ensure they are paying regard to the code in their deployments of FRT. [35] The Protection of Freedoms Act also created the role of Biometrics Commissioner, however this role does not regulate FRT as it is specifically limited to governing police collection, use, and retention of DNA and fingerprints.

33. Equality and Human Rights Commission. "Public Sector Equality Duty". April, 2019

34. Home Office. "Surveillance Camera Code of Practice". Presented to Parliament Pursuant to Section 30 (1) (a) of the Protection of Freedoms Act 2012. June, 2013.

35. Surveillance Camera Commissioner. "The police use of automated facial recognition technology with surveillance camera systems. Section 33 Protection of Freedoms Act 2012." March 2019.

36. IPCO, Annual Report 2017

If FRT is used covertly by law enforcement in public places (that is, when it is deployed so that the people scanned are unaware that it is taking place), then the Surveillance Camera Code does not apply and instead this use is governed as 'directed surveillance' under the Regulation of Investigatory Powers Act (RIPA). It must therefore be authorised by a RIPA Authorising Officer, who is a senior officer within the police force, to ensure it is proportionate and necessary, and this process is documented. The Investigatory Powers Commissioner (IPCO) regulates this use through inspections of forces and their decisions, and the Investigatory Powers Tribunal is a judicial body which investigates and makes legal judgments based on complaints. [36] There is no publicly available information on whether this technology is being used covertly by any police forces.

Legal Challenges

Until recently, the legality of FRT use by the police had yet to be formally tested. In the summer of 2019, however, civil liberties group Liberty took South Wales Police (SWP) to court on the basis that their use of live FRT on members of the public had breached the Human Rights Act, the Data Protection Act, and the Equality Act.

The High Court judged in favour of the police force. It ruled that there is a clear and sufficient legal framework to ensure the appropriate and non-arbitrary use of live facial recognition, and that SWP used live FRT in a way that abided by this legal framework. Focusing on the Human Rights Act, the court ruled that although the technology interfered with the right to privacy, this specific interference was justified as there were sufficient legal safeguards including the Surveillance Camera Code and SWP's specific internal policies. It was also found that this particular use of live FRT was limited and proportionate for a legitimate aim. For similar reasons, the collection of biometric data was found lawful under the Data Protection Act. Regarding the Public Sector Equality Duty, the court felt there was no reason to believe beforehand that the software would have a discriminatory impact, that SWP have always included a human in the loop as a failsafe, and they continue to monitor and investigate any biased outcomes. Liberty has been granted an appeal of this decision, and the case will be heard by the Court of Appeal in June.

Discussion

For private sector use-cases, the exact restrictions that the DPA places on FRT may require clarification: the requirements of the law have not been tested in court and the definition of "substantial public interest" remains open to interpretation. The ICO's upcoming opinion on the King's Cross case should provide welcome clarity.

In policing, the SWP court case clarified that there is a clear and sufficient legal framework for the use of live FRT, suggesting that there is a legal basis for other police forces to use it if the same safeguards exist. However, the ruling does not mean that every deployment of live FRT by a police force will necessarily be legal (for example, under the Data Protection Act, police forces will still need to demonstrate that their use of the technology is strictly necessary). The ICO recommends there be a binding code of practice so that all police forces can better interpret the law and abide by it when they use live FRT systems, for instance through guidelines on the make-up of watchlists. This could potentially build on SWP's internal guidance documentation, which the court ruled acted as an important safeguard.

Despite the ruling, some bodies have questioned whether existing regulation of police use-cases goes far enough. The Surveillance Camera Commissioner has argued that these new surveillance capabilities enabled by FRT may require changes to regulation that would put overt police deployments of FRT under similarly strict controls as those enforced for covert surveillance by the Investigatory Powers Commissioner. [37] In March 2020, the Scottish Parliament passed a bill to create a Scottish Biometrics Commissioner, who would cover next generation biometric technologies such as FRT and the governance of facial data. [38]

---

37. Tony Porter. "The State of Surveillance". Surveillance Camera Commissioner's Office. July, 2019.
38. Scottish Government. "Biometrics Commissioner". Scottish Government. May, 2019.

What's next for the governance of FRT?

06

What's next for the governance of FRT?

It is likely that regulators, civil society groups and political leaders will continue to scrutinise the governance of FRT over the coming months. In doing so, they will ask not just whether existing laws are clear, but whether they are being enforced, and indeed whether they are sufficient. It is not for this paper to present the CDEI's final opinion on this debate. However, it is clear that several questions should be front of mind in any future investigations, among them:

1. How should the public be engaged in deciding whether or not we should use FRT, and under what conditions?

Polling by the London Policing Ethics Panel, the Ada Lovelace institute, and the ICO, suggests that a majority of the public are comfortable with FRT being used by police in criminal investigations, more so than for commercial purposes.[39] However, survey results can be limited, and may hide stark divisions in public opinion. While some in society will be happy to trade off privacy for security, others will be opposed to having their faces scanned in crowds and public spaces in real-time, under any circumstances.[40] Given the importance of accounting for the rights of minority groups and of balancing expert opinion with public opinion, policymakers and civil society groups must carefully consider to what extent, and how, the public should be involved in deciding the conditions under which FRT should be deployed. Initial work in this area is being undertaken by the Ada Lovelace Institute in the form of their Citizens' Biometrics Council to "support a deeper understanding of public perspectives and values on biometrics".[41]

2. Is there a case for a new law regulating FRT use by the police?

The use of FRT is already governed by multiple laws, namely the Data Protection Act, the Human Rights Act, the Equality Act, and the Protection of Freedoms Act. However, some have argued that these laws are insufficient to govern the unique risks posed by FRT and similar emerging surveillance technology due to potentially broad interpretations of these laws, and have therefore called for new standalone legislation regulating the use of this technology.[42]

Several civil society groups, for example, have expressed their desire for a law that would either outlaw or temporarily prohibit the live deployment of facial identification systems in public places, while others, such as the Surveillance Camera Commissioner, have raised the possibility of legislation enforcing strict authorisation for its use, similar to covert surveillance. The South Wales Police vs. Bridges judgement disagreed with this approach, commenting that it was "neither necessary nor practical for legislation to define the precise circumstances under which [the FRT system in question] may be used".

39. London Policing Ethics Panel. "Interim Report on Live Facial Recognition". July, 2018; Information; Ada Lovelace Institute. "Beyond face value: public attitudes to facial recognition technology". September, 2019; Commissioner's Office. "ICO investigation into how the police use facial recognition technology in public places". October 2019.
40. Carlo, Silkie., Kruekeberg, Jennifer., and Ferris, Griff. "Face Off: The Lawless Growth of Facial Recognition in UK Policing". Big Brother Watch. May, 2018.
41. Ada Lovelace Institute. "Citizens' Biometrics Council".
42. Fussey, P., and Murray, D. "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology." Essex Human Rights Centre. 2019.

Effective governance requires more than the formulation of laws, guidance and oversight bodies; it also requires industry to agree common standards and mitigate hazards of its own accord.
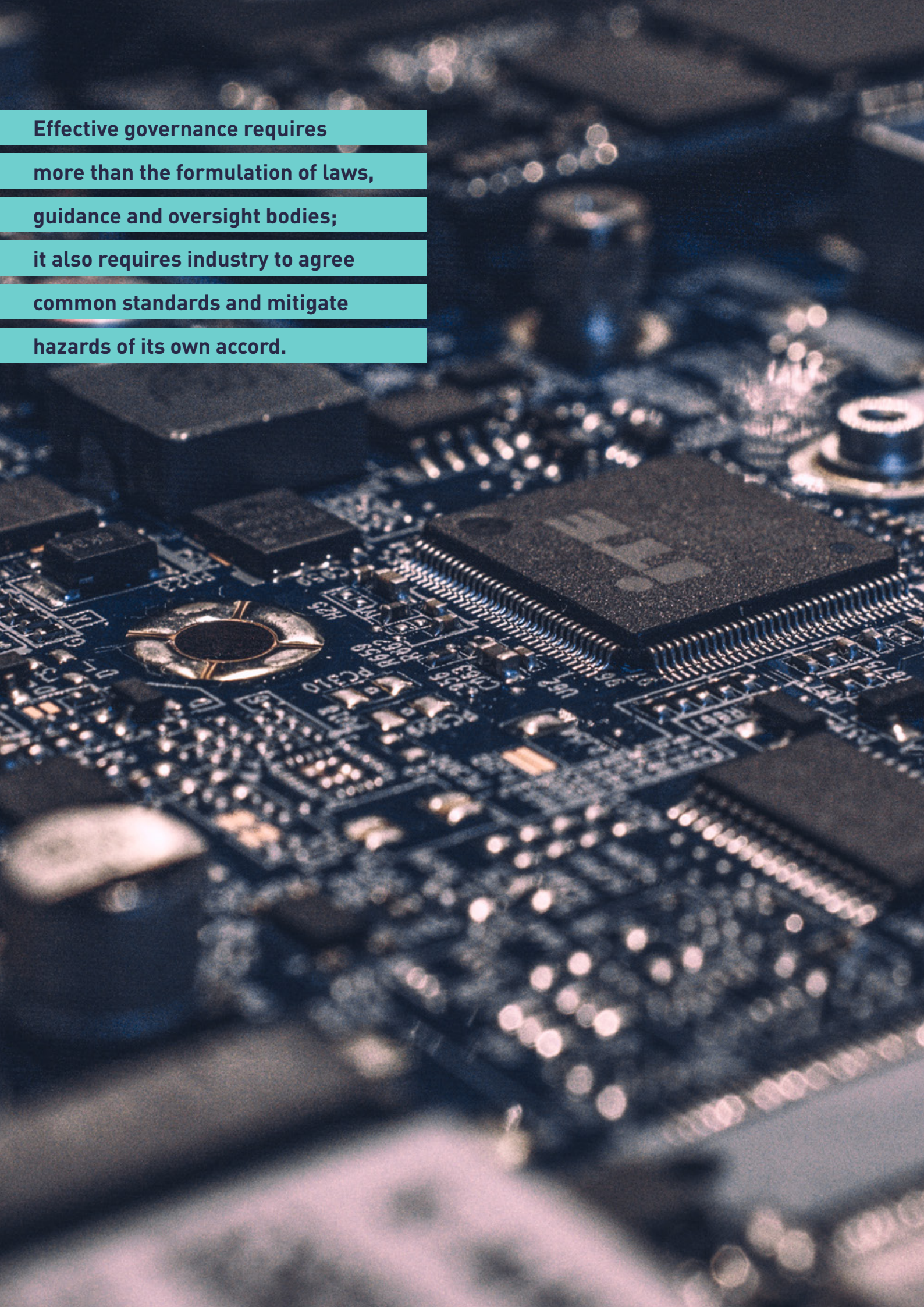
3. Should the powers of the oversight commissioners be reviewed and clarified?

The Surveillance Camera Commissioner (SCC) promotes compliance by police and local authorities with the Surveillance Camera Code, which includes specific references to FRT. A 2019 High Court judgement noted that the SCC provides an important safeguard against the misuse of live FRT in policing. The Information Commissioner's Office, meanwhile, is responsible for overseeing compliance with data protection legislation by all bodies across the public and private sectors, and has regulatory powers. Both have issued guidance on the use of FRT, with the ICO launching investigations into police and private sector use of live facial recognition. The current oversight arrangements can be confusing for the public, civil society groups, and the AI and ethics community, many of whom are unclear as to who is responsible for issuing guidance and enforcing adherence to regulation. Policymakers may wish to review the current regulatory arrangements to ensure there is a clear and straightforward division of responsibility, and that those charged with overseeing FRT have the powers to do so effectively across all settings and sectors. At present, for example, the Surveillance Camera Commissioner has no official remit to promote best practice among commercial firms, meaning oversight of FRT in the private sector is not as strong as it could be. Any attempt to simplify the governance of this technology should be careful to retain the best elements of existing arrangements.

4. How should private sector use of FRT be regulated?

The regulatory regime governing the use of FRT in the private sector is less extensive than the one for law enforcement agencies. That does not necessarily mean it is lacking, however there has been little in the way of policy or judicial reviews to give reassurance to the public. The ICO's investigation into the use of FRT at King's Cross will provide welcome guidance on how private companies can use this technology in relation to the DPA, however it will only go so far in commenting on the suitability of the wider legislative framework. More consideration should be given to this question, in particular whether the DPA is sufficient and how this and any other regulation might be enforced. This in turn may require more research into how private firms are using FRT day-to-day (e.g. how retail stores are compiling and maintaining watchlists) and into any 'crossover' between public and private use (e.g. private sector organisations using facial images from police forces).

5. What role is there for industry self-regulation?

Effective governance requires more than the formulation of laws, guidance and oversight bodies; it also requires industry to agree common standards and mitigate hazards of its own accord. While self-regulation is not a complete solution, bottom-up interventions are easier to assemble and more adaptable than top-down governance. There may also be some risks, such as inaccuracy and bias, where the industry's incentives are well aligned with the public interest. Before implementing any new measures, policymakers and regulators should seek to understand the steps industry is willing to take to address the concerns outlined in this report.

It is important that these and related questions are answered before live FRT is used even more widely and potentially becomes normalised in public life. Several organisations are already contributing to this effort, including the Ada Lovelace Institute, which, as mentioned above, has launched a Citizens' Biometric Council to better understand public attitudes and an independent legal review of Biometrics as a whole. Several technology companies have also made steps towards self-regulation, such as Microsoft, who have developed their own technical standards for training and using FRT systems, and Amazon, which has provided guidance to police forces on conditions for responsible use of the technology. [43]

In the months ahead, the CDEI will look closely at the use of FRT in the private sector, which has had relatively little attention in comparison to the use of FRT in law enforcement. The AI and ethics community would benefit from a clearer understanding of where and how the technology is being used in this domain, the extent to which it is governed, and whether there are grounds to strengthen regulatory oversight, looking at whether lessons might be learned from overseas.

In the meantime the CDEI expects police forces to be appropriately transparent about how they use live FRT in law enforcement, including where it is deployed, the basis by which people are included on watchlists, and how deployments are signed off. We support calls for greater consistency in how FRT is used by different forces, including having minimum safeguards in place before each rollout is confirmed.

To find out more about this project, contact the Centre for Data Ethics & Innovation at cdei@cdei.gov.uk.

43. Punke, Michael. "Some Thoughts on Facial Recognition Legislation." Amazon Web Services Machine Learning Blog. February 2019.

Centre for
Data Ethics
and Innovation