PRIVACY INTERNATIONAL

Submission to the Scottish Parliament's Justice Sub-Committee on Policing's inquiry into facial recognition policing

November 2019

PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

1 November 2019

Privacy International's submission to the Scottish Parliament's Justice Sub-Committee on Policing inquiry into facial recognition policing

Privacy International welcomes the Scottish Parliament's Justice Sub-Committee on Policing call for evidence in relation to the use of Facial Recognition Technology (hereinafter, FRT) by Police Scotland.[1]

Privacy International (PI) is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

PI employs technologists, investigators, policy experts, and lawyers, who work together to understand emerging technology and to consider how existing legal definitions and frameworks map onto such technology. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

The rapid advances in the field of artificial intelligence and machine learning, and the deployment of new technologies that seek to analyse, identify, profile and predict, by police, have and will continue to have a seismic impact on the way society is policed.

The implications come not solely from privacy and data protection perspectives, but from the ethical question for a democratic society of permitting the roll out of such intrusive technology.

> A person's face is a precious and fragile element her identity and sense of uniqueness. It will change in appearance over time and she might choose to obscure or to cosmetically change it – that is her basic freedom. Turning the human face into another object for measurement and categorisation by automated processes

[1] Police Scotland, Policing 2026: Our 10 year strategy for policing in Scotland (June 2019) https://www.scotland.police.uk/assets/pdf/138327/386688/policing-2026-strategy.pdf.

controlled by powerful companies and governments touches the right to human dignity – even without the threat of being used as a tool for oppression by an authoritarian state.

Moreover, it tends to be tested on the poorest and most vulnerable in society, ethnic minorities, migrants and children.[2]

The Surveillance Camera Commissioner in England and Wales notes that *"[w]e are seeing the increasing use of automatic facial recognition (AFR), unmanned aerial vehicles (UAVs), automatic number plate recognition (ANPR) and body worn video cameras (BWVs)*".[3] It has been reported that in the past 3 years, police in different parts of the UK have used or tested FRT in more than 50 instances to monitor peaceful protests, music concerts, sport events, carnivals, festivals and public gatherings, and shopping centres.[4]

FRT refers to the automatic processing of "*digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorisation of those individuals*".[5]

The intrusiveness of FRT and the dangers associated with its potential abuse by the police call for robust safeguards and oversight governing its authorisation and use.

Verification, authentication and identification

This submission focuses on the fundamental rights issues the use of FRT for identification purposes raises. This includes but is not exclusively related to the use of automated facial recognition. i.e. we are referring to both live and static use of facial recognition technology. Our submission on FRT for identification purposes is however distinct from FRT used for the purposes of verification or authentication.

---

[2] EDPS, Facial Recognition: A solution in search of a problem? (28 October 2019) https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

[3] Surveillance Camera Commissioner, Annual Report 2017/18 (January 2019), page 5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772440/CCS207_CCS1218140748-001_SCC_AR_2017-18_Web_Accessible.pdf.

[4] See, for example, Mark Townsend, Police to use facial-recognition cameras at Cenotaph service (The Guardian, 12 November 2017) https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph, Rebecca Hill, South Wales cops crow about facial recognition arrests on social media (The Register, 5 February 2018) https://www.theregister.co.uk/2018/02/05/south_wales_police_facial_recognition_arrests/, James Vincent, UK police are testing facial recognition on Christmas shoppers in London this week (The Verge, 18 December 2018) https://www.theverge.com/2018/12/18/18146083/facial-recognition-police-london-uk-met-christmas-shopping. For a list of events and dates where South Wales and Metropolitan Police have used live facial recognition, see https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/#list-swp.

[5] Article 29 WP, Opinion 02/2012 on facial recognition in online and mobile services (WP 192, 22 March 2012), page 2.

An example of verification and authentication is the use of FRT to allow individuals to unlock their devices, authorise payments or sign up for services. This process relies on the facial image of a single individual being compared to an existing image that individuals have already provided and verifying that it is them requesting access (i.e. one to one matching).

What is meant by facial recognition technology used in identification

In the context of policing, identification can be understood as the capturing of facial images within a specific range, through cameras placed in fixed or moving positions, which are subsequently processed in real (live) or static time (at a later point) with FRT software.[6] This processing results in the creation of digital signatures of identified faces, which are then analysed against a database ('Watchlist'), which contains facial images, in order to determine if there is a match.[7]

It is vital that Police Scotland clarify how they define FRT, whether they identify some or all of their activities as falling under identification or otherwise and what are the sources of the images[8]. They must also explicitly state how facial images are used to allow the committee to investigate whether there are aspects of their work which Police Scotland do not identify as FRT, but which society would identify as such.

For example, we are aware that the police in England and Wales use the term 'facial matching' to refer to the taking of one image or a set of images (probe images) and seeing if there is a match with another image that is on a database. They distinguish this from 'facial recognition' which they define as the taking of an image and seeing if it is a match with images captured either in the live environment or live captured images that are checked at a later period. Facial matching purportedly works on information that has been obtained following a series of interactions with the police and other law enforcement organisations e.g. custody image or a CCTV image of a suspect.

We note that in the Information Commissioner's Office ("ICO") report into how the police use facial recognition technology in public places, the ICO refer to live facial recognition (LFR) technology as that which "*involves the real time automated processing of digital images containing the faces of individuals, for the purposes of identification, authentication or verification, or categorisation of those individuals*".[9] Later the ICO notes other uses of

[6] See, for example, Bethan Davies, Martin Innes and Andrew Dawson, An evaluation of South Wales Police's use of Automated Facial Recognition (September 2018) https://www.statewatch.org/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf.

[7] Privacy International, The police are increasingly using facial recognition cameras in public to spy on us (20 February 2019) https://privacyinternational.org/long-read/2726/police-are-increasingly-using-facial-recognition-cameras-public-spy-us.

[8] As noted in the ICO report, "*[b]oth the DPIAs from SWP and the MPS leave enough room for a range of sources for watchlist images. This could include social media images*", ICO investigation into how the police use facial recognition technology in public places (31 October 2019) https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf.

[9] Ibid, page 3.

facial recognition technology for law enforcement purposes include "*the retrospective identification of individuals from older (that is, not live) CCTV footage or from still images. This use is referred to by South Wales Police as 'AFR Identity'. Another use is similar to 'AFR Identity' approach but uses mobile devices rather than CCTV style cameras*".[10]

Serious risk to society

Whilst it is anticipated that Police Scotland will seek to make a strong case for the use of FRT, it should not be forgotten that this relatively new technology poses a serious risk to society in ways that are known but also ways that may not at present be anticipated. Privacy International believes that the deployment of this technology should be approached with great caution and it should be seriously considered whether the use of FRT is permissible at all in light of the safeguards imposed by the Human Rights Act 1998, the EU Charter of Fundamental Rights as well as the Data Protection Act 2018, in particular Part 3 which applies to the processing of personal data for law enforcement.

The United Nations Special Rapporteur on freedom of opinion and expression, David Kaye, has called for a moratorium of the sale and use of live facial recognition (LFR) technology.[11] His report highlighted instances where LFR has been used as a means to repress particular groups, such as its use to monitor and carry out surveillance on Uighur Muslims in China.[12]

We wish to draw the Sub-Committees attention to the following points.

Points of Clarification

First, Privacy International underlines that the use of FRT by the police for identification purposes is significantly intrusive and constitutes a grave interference with individuals' rights. It is worth noting that in the recent judgment on the use of Automated Facial Recognition by the South Wales Police, the High Court, sitting at Cardiff, stated that this technology "*goes much further than the simple taking of a photograph. The digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information. The fact that this happens when the Claimant is in a public space is not a sufficient response"*.[13]

The use of this technology would consequently trigger the applicability of not only international and European human rights law, but also the relevant domestic data protection legislation, since it involves the processing of special-category/sensitive category of personal data, i.e. biometric data.[14]

---

[10] Ibid, page 11.
[11] UN, Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35, 28 May 2019), para 66ff.
[12] Ibid, para 12.
[13] Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019), para 54.
[14] See Article 9 Regulation (EU) 2016/679 of the European Parliament and of the Council of

The latter would oblige the police to adhere to the data protection principles enshrined in Part 3 of the Data Protection Act 2018, namely lawfulness and fairness of processing, purpose limitation, data accuracy, data minimisation, storage limitation, data security.

Second, Privacy International highlights that legislative frameworks governing the use of FTR must satisfy the "*in accordance with the law*" requirement imposed by human rights law.[15] Specifically, the use of FRT by the police must not only meet strict accessibility, foreseeability and quality of law requirements, but should also be accompanied by safeguards in order to prevent abuse of this rather intrusive power. These should at the very minimum include:

- precise/explicit framework on how the technology is used and for what purposes by the police, which should be approved by Parliament, and be accessible to the public;
- transparency around the criteria for inclusion on the watchlist, including with respect to the seriousness of the underlying offence;
- existence of individualised reasonable suspicion and concrete or specific threat that would justify deploying this technology;
- as well as independent judicial or administrative authorisation.

We note that MP's in the House of Commons Science and Technology Committee have called for the police use of Live Facial Recognition to be suspended, until further legislative framework is applied to the technology.[16]

We are not aware of independent reports on the use of FRT in Scotland. We note the value that independent ethics committees have brought in relation to raising pertinent questions about the deployment of new surveillance technologies by police forces in England and Wales. We bring to the Committee's attention to the July 2019 Independent Report into London MPS FRT trial which concluded:

> [T]he implicit legal authorisation claimed by the MPS for the use of LFR appears inadequate when compared with the 'in accordance with the law' requirement established under human rights law. The absence of publicly available guidance clearly circumscribing its circumstances of use – thereby facilitating foreseeability – reinforces this point. Without explicit legal authorisation in domestic law it is highly possible that police deployment of LFR technology – as a particularly invasive surveillance technology directly affecting a number of human rights protections, including those relevant to

---

27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Article 10 Data Protection Act 2018.

[15] See Privacy International, Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data to tackle terrorism (June 2019) https://privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf, pages 3-4.

[16] UK House of Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session 2017–19 (HC 1970, 18 July 2019) https://www.publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003

democratic participation – may be held unlawful if challenged before the courts.[17]

Additionally, the Report indicated that, although the first live FRT trial was conducted as early as August 2016, "*no detailed information was available to the public prior to 15 July 2018 at the earliest*", contrary to the requirements of the Surveillance Camera Commissioner's Code of Practice.[18] If deployed as a covert means of surveillance, FRT will leave individuals unaware of the fact that sensitive biometric data of them have been captured, stored or processed, in general.[19] As a result, this would render their data protection or other rights meaningless. Both the Court of Justice of the European Union and the European Court of Human Rights have highlighted the obligation of authorities to notify ex post the individuals affected by surveillance measures so that they can effectively exercise their rights, including their right to a legal remedy.[20]

Third, human rights law requires that measures that interfere with fundamental rights adhere to necessity and proportionality, meaning that any interferences with fundamental rights need to be limited to what is strictly necessary and proportionate to the aim sought.[21] This consequently requires the police firstly, to prove a concrete, specific and immediate threat to national security or public safety that would justify deploying this kind of technology (necessity). Secondly, they must demonstrate that the use of FRT would override any fundamental rights implications (proportionality).

Necessity considerations require that the police be able to prove that deploying FRT would be the least restrictive means of achieving similar identification results, compared to other available policing techniques. In August 2019, the Swedish Data Protection Authority issued a fine against a school that used facial recognition technology to monitor attendance. In its decision, the Swedish Data Protection Authority found that the use of the technology constituted "*an intrusion on [students'] integrity and that attendance can be monitored in other ways that are less privacy violating than facial recognition*".[22] In discussions around necessity, concerns relating

[17] Pete Fussey and Daragh Murray, Independent Report on the London Metropolitan Police Service's Trial of Live FRT (University of Essex Human Rights Centre, July 2019), page 9.
[18] Ibid, page 63.
[19] See, for example, Lizzie Dearden, Police accused of deploying facial recognition 'by stealth' in London (Independent, 27 July 2018) https://www.independent.co.uk/news/uk/crime/facial-recognition-uk-police-london-trial-data-human-rights-legal-action-met-a8466876.html.
[20] See, for example, CJEU, Joined Cases C–203/15 and C–698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson [2016] ECR I–970, para 121; ECtHR, Zakharov v. Russia (App. No. 47143/06, 4 December 2015), paras 233-234.
[21] See, in particular, Convention for the Protection of Human Rights and Fundamental Freedoms, Articles 8-11, which require interferences to be "necessary in a democratic society", as well as Charter of Fundamental Rights of the European Union, Article 52(1) ("Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others").
[22] European Data Protection Board, Facial recognition in school renders Sweden's first GDPR fine (22 August 2019) https://edpb.europa.eu/news/national-news/2019/facial-

to the accuracy of the technology, as identified above, further undermine the case for the use of FRT.

Regarding any proportionality or balancing assessments carried out by the police, Privacy International suggests extreme caution. Any balancing between the benefits of FRT and the human rights harms will be incapable of adequately incorporating the extent of the latter due to FRT's chilling effects. For example, authorities would likely not be in a position to assess the exact number of people who have chosen not to attend a public event, sacrificing their freedom of expression and assembly rights over legitimate concerns relating to abuse of their biometric data by the police. It should be noted that, under the freedom to hold opinions, a necessary condition for the exercise of freedom of expression,[23] individuals also enjoy protection against negative consequences in cases where particular opinions are attributed to them following previous public expressions as well as the right not to be compelled to communicate their opinions.[24]

According to a recent survey conducted by the Ada Lovelace Institute, more than 60% of the respondents were uncomfortable with the idea that FRT could be used in public spaces, with a majority "*connecting their discomfort with the prospect that it will normalise surveillance*".[25] As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated, "I*i]n environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the rights to freedom of expression, association, religious belief, culture and so forth*".[26]

Fourth, FRT that is deployed in public spaces for the purposes of policing does not only interfere with individuals' privacy and data protection rights. It can also seriously affect the exercise of rights to freedom of thought, conscience and religion, freedom of expression and freedom of assembly and association.[27] In its submission on Article 21 of the International Covenant on Civil and Political Rights to the UN Human Rights Committee,

---

recognition-school-renders-swedens-first-gdpr-fine.

[23] The Council of Europe Committee of Ministers has stated that "*any restrictions to this right will be inconsistent with the nature of a democratic society*", Report of the Committee of Ministers, in Theory and Practice of the European Convention on Human Rights, Van Dijk and Van Hoof, Kluwer, 1990, page 413.

[24] See, for example, ECtHR, Vogt v. Germany, App. No. 17851/91, 26 September 1995.

[25] Ada Lovelace Institute, Beyond face value: public attitudes to FRT(September 2019) https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf. See also Mattha Busby, People at King's Cross site express unease about facial recognition (The Guardian, 13 August 2019) https://www.theguardian.com/technology/2019/aug/13/people-at-kings-cross-site-express-unease-about-facial-recognition.

[26] UN, Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35, 28 May 2019), para 21.

[27] As the European Data Protection Supervisor has also highlighted, the use of FRT "*is fundamentally an ethical question for a democratic society*", since it can "*obviously chill individual freedom of expression and association*", EDPS, Facial Recognition: A solution in search of a problem? (28 October 2019) https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

Privacy International highlighted how new surveillance technologies can also affect the exercise of the right to freedom of peaceful assembly, by also having "*a chilling effect on individuals*".[28] Due to this chilling effect, it is extremely difficult or impossible for authorities wishing to make use of this technology to precisely measure the negative effects for the exercise of the aforementioned rights, and to thus justify its use.[29]

Fifth, FRT relies on probabilistic reasoning, and as such, inevitably produces varying levels of false positive and false negatives. In addition, many commercially available facial recognition systems have been found to have different error rates, depending on people's race and gender.[30] In his 2019 Report the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression mentioned that FRT "*seeks to capture and detect the facial characteristics of a person, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics, which are often the basis for unlawful discrimination*".[31]

In a test conducted by the ACLU in July 2018, facial recognition software incorrectly "*matched 28 members of Congress, identifying them as other people who have been arrested for a crime*".[32] As the Article 29 Data Protection Working Party mentions in its Opinion 3/2012 on developments in biometric technologies, differences in the quality of captured images as well as pose and illumination variations "*remain a big challenge for facial recognition, highly affecting the accuracy*".[33] According to research carried out by Big Brother Watch, FRT used by police in the UK has proven to be extremely inaccurate. Specifically, Metropolitan Police's and South Wales Police's matches have wrongly identified people up to 98% of the time, i.e. more than 2,500 people in total.[34]

The combination of FRT with other forms of surveillance policing, such as body worn cameras, poses unprecedented threats. In July 2019, Axon Enterprise Inc. announced that the company would refrain from equipping police body-worn cameras with FRT as the latter is "*not currently reliable enough to ethically justify its use on body-worn cameras*" and that such use should not occur "*until the technology performs with far greater*

---

[28] https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf, page 10.
[29] Privacy International, Protecting Civic Spaces (1 May 2019) https://privacyinternational.org/long-read/2852/protecting-civic-spaces.
[30] Karen Hao, AI is sending people to jail—and getting it wrong (MIT Technology Review, 21 January 2019) https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/.
[31] UN, Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/41/35, 28 May 2019), para 12.
[32] ACLU, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots (26 July 2018) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[33] Article 29 WP, Opinion 3/2012 on developments in biometric technologies (WP 193, 27 April 2012), page 22.
[34] Big Brother Watch, Face Off: The lawless growth of facial recognition in UK policing (May 2018) pages 3-4.

accuracy and performs equally well across races, ethnicities, genders, and other identity groups".[35]

Concerns relating to the integration of face recognition with other policing equipment go beyond issues of accuracy. As people move through public spaces or interact with police, they do not anticipate or expect that their faces will be converted into a biometric map, so that their facial features can be recorded, catalogued, and analysed, without their awareness or consent.[36] Based on these concerns, in October 2019, California enacted a law that temporarily prohibits law enforcement from adding face and other biometric surveillance technology to officer-worn body cameras for use against the public.[37] Such integration further risks chilling people's willingness to engage with law enforcement officers or to report crimes if they believe that their biometrics will be captured by the officers' body-worn cameras. For example, it could chill the ability of victims of human trafficking or those with uncertain immigration status to report offences if they are unwilling to approach officers for fear their biometrics will be captured and analysed.

Sixth, the use of live or real time FRT fundamentally violates human dignity and freedom. Human rights law requires that limitations placed on individuals' rights should not significantly impair their core or essence.[38] In a similar vein, the European Court of Human Rights has held that "*the very essence of the Convention is respect for human dignity and human freedom*"[39] and that restrictions imposed upon rights should not unacceptably weaken the protection afforded by them.[40] Echoing such concerns, in May 2019, San Francisco's Board of Supervisors issued an ordinance, which outlaws the use of facial-recognition technology by police and other government departments.[41]

Seventh, Privacy International notes the serious security concerns surrounding the processing of sensitive personal data captured by FRT as

---

[35] First Report of the Axon AI & Policing Technology Ethics Board (June 2019), pages 28ff.
[36] Privacy International, Real-time facial recognition should never be coupled with body-worn cameras (7 July 2019) https://privacyinternational.org/news-analysis/3028/real-time-facial-recognition-should-never-be-coupled-body-worn-cameras.
[37] The Body Camera Accountability Act (AB 1215) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.
[38] The U.N. Special Rapporteur for Counterterrorism has emphasized that "*in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right*", U.N., Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism (A/69/397, 23 September 2014), para 51.See also Charter of Fundamental Rights of the European Union, Article 52(1) ("Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others").
[39] ECtHR, Christine Goodwin v. the United Kingdom, App. No. 28957/95, 11 July 2002, para 90.
[40] ECtHR, S. and Marper v. the United Kingdom, App. Nos. 30562/04 and 30566/04, 4 December 2008, para 112.
[41] https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A, pages 2 ff.

well as the risks associated with the involvement of private actors in policing. In August 2019, privacy researchers revealed that fingerprints, facial images and other personal data of more than a million people were discovered on a publicly accessible database for a company used, among others, by the Metropolitan Police.[42]

Similarly, in October 2019, it was revealed that a property developer was using facial recognition software around the King's Cross site for two years from 2016 without any apparent central oversight from either the Metropolitan police or the office of the mayor.[43] A police report later revealed that images of seven people were passed on by local police for use in the system in an agreement that was struck in secret,[44] triggering an investigation by the ICO.[45]

Such incidents raise serious questions regarding the involvement of private actors in the use of invasive surveillance technologies. Privacy International questions whether private actors should be conducting policing functions. We are concerned whether such actors are in a position to comply with the provisions of Part 3 of the Data Protection Act 2018 or adhere to strict confidentiality and security requirements regarding the processing of biometric data and also provide individuals with adequate safeguards against potential abuse.

Going Forward

In all, Privacy International is deeply concerned that the use of FRT by the police, including Police Scotland, raises significant problems for fundamental rights and individual freedoms. So far, this technology has offered law enforcement new opportunities to experiment with or engage in novel forms of surveillance, in an arbitrary or unlawful fashion, which lacks transparency and proper justification, and fails to satisfy both international and European human rights law standards.[46]

Due to the impermissibly intrusive nature of this technology, Privacy International submits that live or real-time FRT should never be deployed. Moreover, police should not be allowed to make use of this technology

---

[42] Josh Taylor, Major breach found in biometrics system used by banks, UK police and defence firms (The Guardian, 14 August 2019) https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[43] Dan Sabbagh, Facial recognition row: police gave King's Cross owner images of seven people (The Guardian, 4 October 2019) https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people.

[44] https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf.

[45] ICO, Statement: Live FRT in King's Cross (15 August 2019) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/.

[46] Privacy International, Our response to the Westminster Hall Debate on Facial Recognition (30 April 2019) https://www.privacyinternational.org/advocacy/2835/our-response-westminster-hall-debate-facial-recognition.

without justification that relies on concrete and specific threats to national security or public safety, as well as in absence of legal safeguards, such as publicly available legal frameworks, existence of reasonable suspicion, independent authorisation, ex post notification. Such requirements effectively mean the situations in which such technology can be used in accordance with law are so few so as to render any further testing or expenditure of resources on FRT disproportionate.

Privacy International recommends the Justice Sub-Committee on policing:

- Take a position that this technology is of such an intrusive nature as to pose unprecedented threats not only to privacy and data protection, but also to other rights that enable democratic participation.

- Consider in detail whether:
    - There is evidence that Police Scotland need the technology at all; whether there are less intrusive means to achieve the same goal; whether it is a solution for a problem that does not exist.
    - There can ever be a valid legal basis for the application of such technology given that it relies on the large-scale processing of sensitive data.
    - The likely direction of travel if FRT is deployed by Police Scotland and other government agencies and continues to be deployed more widely both in the government and private sector.

- Advise the Scottish Government to take steps to prevent the testing, trialling and deployment by law enforcement, other government agencies and private actors of live or real time FRT.

- Advise the Scottish Government that no facial recognition technology be used under any circumstances unless:
    - There is sufficient clarity from Police Scotland on their definitions and understanding of what does and does not fall under 'automated facial recognition technology' and 'facial recognition technology'.
    - There is sufficient clarity from Police Scotland on the various ways that images, in particular facial images are collected, processed and stored. This includes how data is used by those who collect it, who has access and to whom it is shared, how long it is retained, how a profile is formed, who is responsible for any automated decision-making.
    - There is sufficient clarity from Police Scotland as to the various ways that images are processed which may or may not fall under the definition of facial recognition technology.
    - There is clear articulation of the lawful basis for processing and the legislative basis relied upon by Police Scotland for the use of this technology.

- A statutory code of practice and national guidelines are established.
- There is clear articulation about the necessity of using FRT for policing purposes and how its use will be proportionate to the objectives of deployment. In addition, it should explain how the use of FRT is more effective than alternative measures.
- Ensure independent review and scrutiny takes place as to whether the use of FRT in Scotland does or could meet human rights and data protection safeguards including data minimisation and data protection by design.
- Ensure scrutiny as to the accuracy of FRT, the consequences for individuals being falsely identified, the risk of bias, false positive or false negatives.
- Police Scotland have carried out and published relevant impact assessments including data protection impact assessments; human rights impact assessments; equality impact assessments and others deemed relevant.
- Specific assessment to the risks to the rights and freedoms of individuals and an explanation of how these risks will be mitigated
- Clear articulation of how technology bias has been eliminated and why Police Scotland is satisfied this is the case
- A transparent, informed and detailed consultation has taken place engaging both the public and civil society.
- Detailed consideration is given not only to the privacy and data protection implications and other legal considerations but also the ethical implications for democratic society of deployment of this technology.

It is only at the point the bare minimum actions above are taken that it is possible to take an informed approach as to whether FRT should ever be deployed. As the European Court of Human Rights has underlined, a state that claims a "*pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard*".[47]

[47] ECtHR, S. and Marper v. the United Kingdom, App. Nos. 30562/04 and 30566/04, 4 December 2008, para 112.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471