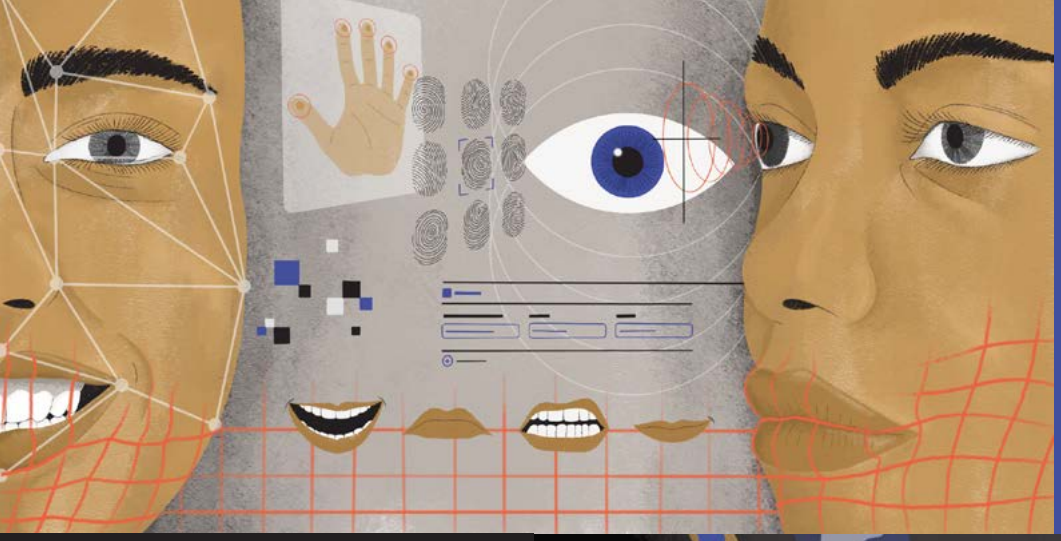
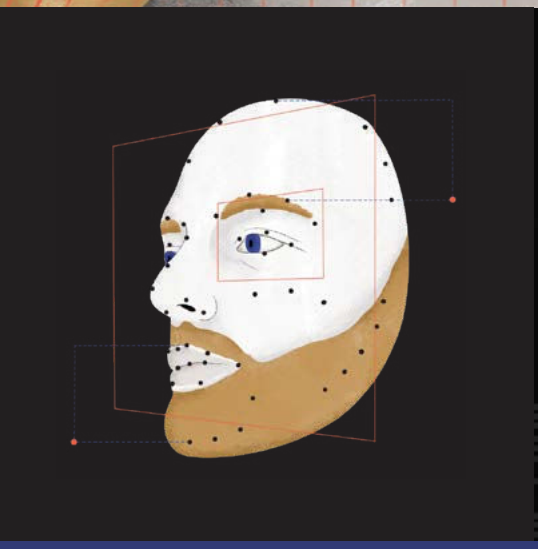




Eyes on the Watchers: Challenging the Rise of Police Facial Recognition

Principles to reduce the human rights harms of FRT

INCLO

Contents

Introduction

This project by the International Network of Civil Liberties Organizations (INCLO) focuses on the use of facial recognition technology (FRT) by police.

Our project builds on the 2021 INCLO report *In Focus: Facial Recognition Stories and Rights Harms From Around the World*.[1] That report was a compilation of stories demonstrating the then emerging harmful effects of FRT that can be used to map, analyse and attempt to establish the identity of a face in a photograph or video, thereby giving users the capability to track or surveil a person in real time or retrospectively without their knowledge or consent.[2] It outlined how FRT, a powerful but flawed technology, impacts citizens' rights and daily lives across 13 countries in the Americas, Africa, Europe, Asia and Australia. It looked at how FRT poses risks by enabling surveillance that can track individuals during protests, religious events, medical visits and everyday activities, and how FRT can misidentify people – especially people of colour – for crimes they did not commit. Our report made a strong case for an open, public, democratic debate about the use of this technology.

Three years later, the use of this transformative technology is increasingly normalized and ubiquitous. The current US$5 billion FRT industry is estimated to grow to US$50 billion by 2030.[3] A growing number of state and private actors[4]

---

1 *In Focus: Facial Recognition Tech Stories And Rights Harms From Around The World*, International Network of Civil Liberties Organizations, 2021, https://inclo.net/publications/in-focus-facial-recognition-tech-stories-and-rights-harms-from-around-the-world/.

2 Akbari, A, "Facial Recognition Technologies 101: Technical Insights" in *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, 2024, pp. 29–43, https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technologies-101/8B3039F97B11F43B78E52BBEB73E8479.

3 Matulionyte R & Zalnieriute M, "Facial Recognition Technology in Context: Technical and Legal Challenges" in *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, 2024, https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technology-in-context/A4F5E2C52EF9CFD27E8F04D0DD60074D.

4 Lyons, J, *NFL to begin using face scanning tech across all of its stadiums*, The Register, 2 August 2024, https://www.theregister.com/2024/08/06/nfl_face_scanning_tech/. See also Baker, T, *Home Office eyeing expansion of "Orwellian" facial recognition*, Sky News, 30 August 2023, https://news.sky.com/story/facial-recognition-technology-labelled-orwellian-as-government-eyes-wider-use-by-police-and-security-agencies-12950942.

across the globe are moving to introduce[5] or expand[6] the use of FRT. As legislators are passing laws for FRT use with inadequate guardrails for fundamental rights,[7] courts are increasingly tasked with understanding and adjudicating on the risks.[8] This is the context within which we return to this subject with urgency.

Here, we repeat our call for a thorough re-evaluation and reconsideration of FRT's application in law enforcement. This call is underscored by FRT's potential misuse, the growing interconnectedness of state surveillance systems and its ongoing impact on individual freedoms. Given the growing deployment of FRT across INCLO member states, we have returned to this subject and developed a set of principles grounded in our documented explanation of the technology, its applications, and its harms and risks, together with human rights standards and legal analysis.

Our principles are focused on the use of FRT by police for the purpose of identification; they provide a foundation for understanding the risks of FRT and serve as a tool for assessment and advocacy. We believe they are valuable to civil society, policy makers, legislators, the public, media, courts and law enforcement.

The risks of FRT in a policing context cannot currently be safeguarded by legislation and the technology cannot be safely deployed; therefore, police should be banned from using FRT. Our principles do not promote the use of policing FRT, but rather map existing minimum accountability and harm-mitigation standards. They serve as a tool to build consensus around the significant problems posed by FRT and the need for significant restrictions and bans.

We advocate for adopting even higher standards tailored to the specific circumstances of each jurisdiction to ensure the protection of human rights and the integrity of law enforcement practices.

---

5 Desmarais, A, *Ireland's new police facial recognition bill has "fundamental defects," experts say*, Euronews, 1 March 2024, https://www.euronews.com/next/2024/03/01/irish-police-facial-recognition-bill-has-fundamental-defects-experts-say#:~:text=The%20Irish%20Parliament%20passed%20the,to%20this%20law%20in%20December.

6 Sabbagh, D, "Starmer's live facial recognition plan would usher in national ID, campaigners say", *The Guardian*, 2 August 2024, https://www.theguardian.com/technology/article/2024/aug/02/starmer-live-facial-recognition-plan-would-usher-in-national-id-campaigners-warn.

7 Volpicelli, G, *EU set to allow draconian use of facial recognition tech, say lawmakers*, Politico, 16 January 2024, https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns/.

8 *Glukhin v Russia*, App. No(s),11519/20,https://hudoc.echr.coe.int/eng?i=001-225655; see also *New Jersey Appellate Division One of First Courts in Country to Rule on Constitutional Rights Related to FRTs*, ACLU, June 2023, https://www.aclu-nj.org/en/press-releases/new-jersey-appellate-division-one-first-courts-country-rule-constitutional-rights.

About INCLO

INCLO is a network of 15 independent national human rights and civil liberties organizations working to promote fundamental rights and freedoms. We support and reinforce our member organizations' work in their respective countries and foster bilateral and multilateral collaborations within the network. INCLO is composed of multi-issue multi-constituency human rights organizations that are domestic in focus and independent of their governments. These organizations defend the rights of all persons on their national soil through a mix of litigation, legislative campaigning, public education and grassroots advocacy.

INCLO's 15 member organizations are the American Civil Liberties Union (ACLU); the Association for Civil Rights in Israel (ACRI); the Canadian Civil Liberties Association (CCLA); the Centro de Estudios Legales y Sociales (CELS) in Argentina; Dejusticia in Colombia; the Egyptian Initiative for Personal Rights (EIPR); the Human Rights Law Network (HRLN) in India; Human Rights Law Centre (HRLC) in Australia, the Hungarian Civil Liberties Union (HCLU); the International Human Rights Group Agora (Agora) in Russia; the Irish Council for Civil Liberties (ICCL); the Kenya Human Rights Commission (KHRC); KontraS in Indonesia, the Legal Resources Centre (LRC) in South Africa; and Liberty in the United Kingdom.

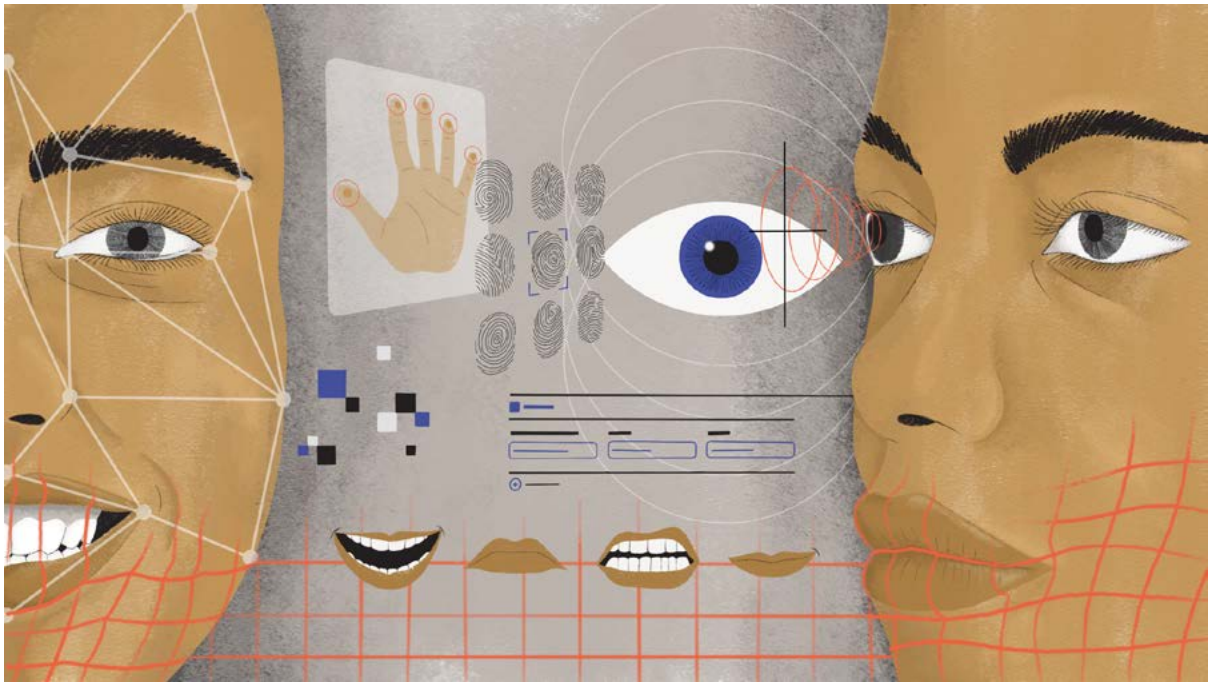


Illustration by Alina Najlis - © 2024 INCLO

What is FRT?

FRT is a form of biometric[9] artificial intelligence[10] that police use to attempt to identify or characterize a person on the basis of their facial features.[11] Our principles refer to systems using FRT as organized and structured sets of interrelated software, hardware, procedures, datasets and human resources that are deployed – that is, set up and implemented – as a unit. In other words, while the software's main component involves detecting a facial image and attempting to identify it, it works within a structure, and in conjunction with other hardware and software operated by humans who interpret the outputs produced.

9 "Biometrics" refers to the measurement of physical characteristics or personal behaviour. Under the understanding that these are unique, and therefore could be used to identify a person, biometrics refers in computer science to the field of authenticating the identity by automatically carrying out these measurements and calculations. Some examples of body parts used for such purposes are face, fingerprints, DNA or the iris.

10 For the purposes of this project, we refer to the definition of an "artificial intelligence system" under Article 3 (1) of the European Union Artificial Intelligence Act: "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments", together with Recital 12 of the Act, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

11 For more information on the history and development of facial recognition, see Raviv, S, *The Secret History of Facial Recognition*, Wired, 21 January 2020, https://www.wired.com/story/secret-history-facial-recognition/.

What is FRT used for?

The following are some of the main uses of facial recognition:[12]

VERIFICATION

The goal of FRT-based verification is to confirm the identity of a person through the comparison of a single image captured at that moment against a single stored image. For that reason, FRT verification can also be referred to as "one-to-one matching" or "one-to-one comparison". Examples of this include a person attempting to unlock their smartphone with their face, or when a person's photograph taken at an airport checkpoint is compared with their passport photograph.

IDENTIFICATION

The goal of FRT-based identification is to determine the identity of an unknown individual whose face is captured on a picture or video by comparing the image of the unknown person against a reference database of images of known people. It can also be referred to as "one-to-many identification". This is the traditional use of FRT-based surveillance systems, upon which these principles are focused. Examples include police attempting to identify a person by comparing the image of a person taken from a closed-circuit television (CCTV) still or social media against driver's licence, voter registration or passport holder databases, or comparing the image of a person caught on CCTV against a watchlist of known individuals in a real-time, or live, manner.

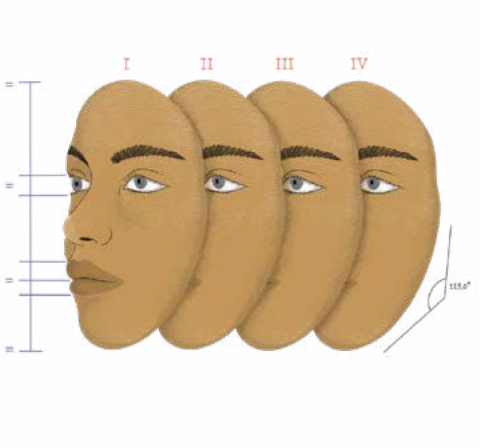
FACIAL ATTRIBUTE CLASSIFICATION, ESTIMATION AND DETECTION

The goal of attribute classification is to obtain information about features that are then used to attempt to measure (such as estimating age) or categorize (such as identifying gender). It can also involve checking whether certain features are present or not (such as detecting if someone is wearing glasses). An example of this use is the categorization of large numbers of people into smaller clusters for

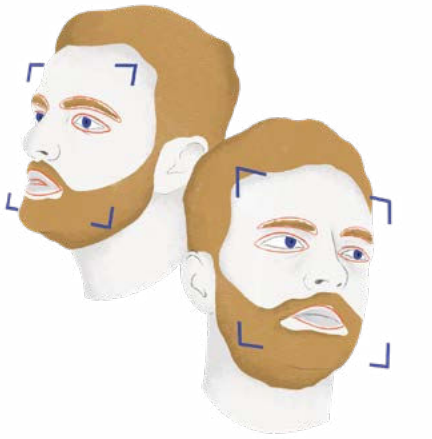
12 See Buolamwini, J et al., *Facial Recognition Technologies: A Primer*, May 2020, https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf.

VERIFICATION

IDENTIFICATION



FACIAL ATTRIBUTE CLASSIFICATION, ESTIMATION AND DETECTION



FACIAL EMOTION RECOGNITION

marketing purposes,[13] a practice which raises serious concerns about profiling, privacy and data protection.

FACIAL EMOTION RECOGNITION

The goal of facial emotion recognition is to attempt to infer a person's feelings or emotions based on their facial expressions. For example, the US retail giant Walmart previously used facial recognition to attempt to identify unsatisfied

13 Kuligowski, K, *Facial Recognition Advertising: The New Way to Target Ads to Customers*, Business News Daily, 20 October 2023, https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html.

customers.[14] The accuracy and scientific grounding[15] of this hugely controversial "pseudoscientific"[16] use of facial recognition is highly contested.[17]

Technical notes to accompany these principles

Generally speaking, this use of FRT involves the following steps. However, it should be noted that this set of steps is a simplified version of a very complex process and sequence of actions involving various factors:[18]

STEPS OF FACIAL RECOGNITION

1. **FACE DETECTION:** Localization of a face or faces in an image or video and, if any, return of the coordinates of the boxes bounding each of them.
2. **FACE ALIGNMENT:** Modification of the face input (such as scaling or cropping), based on its geometric features, to adapt it to a canonical form in order to allow it to be compared against a database or watchlist of facial images.
3. **FACE REPRESENTATION:** Transformation of the pixels in the image into inputs that are useful for computer comparison. This may be a set of templates or, depending on the technique, features or shapes.
4. **FACE MATCHING:** Comparison of the input obtained in the previous step against the reference database to assess, with a probability score, the verification, identification or categorization of the face.

---

14 Peterson, H, *Walmart is developing a robot that identifies unhappy shoppers*, Business Insider, 19 July 2017, https://www.businessinsider.com/walmart-is-developing-a-robot-that-identifies-unhappy-shoppers-2017-7.

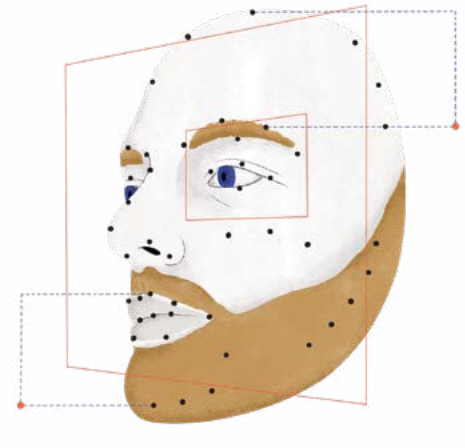
15 Stanley, J, *Experts Say "Emotion Recognition" Lacks Scientific Foundation*, American Civil Liberties Union, 18 July 2019, https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific and Romero, A, *AI Emotion Recognition is a Pseudoscientific Multi-billion Dollar Industry*, The Algorithmic Bridge, 12 July 2022, https://www.thealgorithmicbridge.com/p/ai-emotion-recognition-is-a-pseudoscientific.

16 Hern, A, "Information commissioner warns firms over 'emotional analysis' technologies", *The Guardian*, 25 October 2022, https://www.theguardian.com/technology/2022/oct/25/information-commissioner-warns-firms-over-emotional-analysis-technologies.

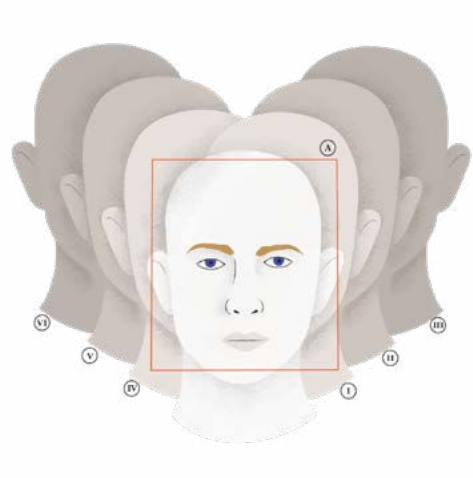
17 Barrett, LF, Adolphs, R, Marsella, S, Martinez, AM & Pollak, SD (2019), "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements", *Psychological Science in the Public Interest*, 20(1), 1–68. https://doi.org/10.1177/1529100619832930.

18 Sáez Trigueros, D, Meng, L & Hartnett, M, *Face Recognition: From Traditional to Deep Learning Methods*, 2018, https://arxiv.org/pdf/1811.00116.

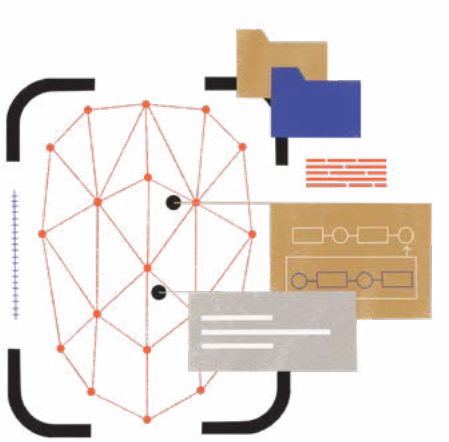
FACE DETECTION



FACE ALIGNMENT



FACE REPRESENTATION



FACE MATCHING

Probe image

The unidentified facial image of a particular individual whom the police wish to identify is often referred to as the ‘probe image’. Probe images can vary widely in terms of angle, format, quality, and pixelation. This variability can result in a range of issues.

The key point here is that, in reality, facial imagery comes from many different sources and involves, at the very least, people holding many different poses, people being captured in very different lighting conditions, and faces being obscured by varying degrees due to the position of the camera, clothing or sunglasses, etc.

FACTORS WHICH CAN AFFECT THE RELIABILITY OF A FACIAL RECOGNITION SYSTEM IN RELATION TO PROBE IMAGES:

1. **POSE:** The position of the face in the probe image affects the attempted matching process.
2. **ILLUMINATION:** The ambient lighting may affect the texture patterns detected in a face, including the possibility of highlighting or playing down certain traits or altering the shape of the face.
3. **EXPRESSION:** Mainly impacting facial emotion recognition, the configuration of the large collection of muscles we have in our faces may also affect identification and verification.
4. **OCCLUSIONS:** The use of accessories or other ways to cover part of the face, such as clothing, masks or hands, can result in part of the facial information not being available for facial recognition purposes. This may also affect the information that can be captured by altering, for example, the symmetry of a face.
5. **IMPRECISELY LOCALIZED FACES:** Whereas the factors above refer to the environment where the person is, this one points towards the flaws of systems when conducting facial detection or when delineating facial features from a picture or video, making it difficult to determine where a face or a feature starts or ends.

Reference database or watchlist

The unidentified probe image is compared against a set of identified images (**reference databases or watchlists**) in an attempt to find a "match". A significant factor in the system's performance will therefore be the quality of the images in these sets and the accuracy of the information contained in the database against which probe images are compared. This means that a match depends not only on the quality of the probe image, but also on the accuracy of the details contained in the reference database or watchlist as to the targets' identities. For example, outdated lists of fugitives in a reference database may lead to wrongful arrests.

Training dataset

Other than the probe images and the database images, there is a third set of images that needs to be considered and is accounted for in these principles: the **dataset**. This is the set of images that are fed into the system during its training phase, before the system's deployment and use by the police. This training phase aims to teach the system to recognize patterns (in this case facial features) on the basis of thousands of images of people's faces. This stage also aims at increasing the system's robustness to overcome aforementioned challenging conditions that can affect the reliability of the system, such as images with partially covered or obscured faces.

Understanding the training process and the datasets involved in this training is key to understanding the source of some of the harms associated with FRT systems. The very nature of training datasets may be the source of the bias reflected by FRT systems[19] via the following causes:

DATASET BIASES

- *Capture bias:* related to the origin of the pictures. Affected by both the device used and the collector's preferences, and related to factors that affect reliability mentioned above such as lighting or position of the face.
- *Category or label bias:* related to ambiguity and vagueness in our visual semantics and deriving both from similar images being put in different categories and, on the other hand, diverse images falling into the same category.
- *Negative bias:* related to the part of the visual information left out of the dataset due to a focus on particular features.

19 Tommasi, T, Patricia, N, Caputo, B & Tuytelaars, T (2015). *A Deeper Look at Dataset Bias*. ArXiv, abs/1505.01257.: https://arxiv.org/ftp/arxiv/papers/1505/1505.01257.pdf.

FUNCTIONING IN REAL LIFE[20]

Facial recognition systems operate in real-life scenarios and do not reflect laboratory conditions. Flaws in the datasets, reference databases/watchlists and probe images result in limited accuracy, which can lead to huge fundamental rights violations. **Accuracy figures put forward by vendors of these systems and supporters of FRT are also very often based on pristine laboratory conditions and scenarios** involving the comparison of high-quality, clean images with perfect lighting, where people's faces were perfectly captured in images used for visa applications and mugshots, with very similar clean, high-quality and controlled images. However, advocates fail to mention the following shortcomings:

- Limited technical literacy of police forces as final users:

  As with other digital technologies, and more so with AI-based tools, a careful understanding of how a system works, including its failings and limitations, is paramount to mitigate risks and harms. When considering a deployment, training and procedures are key elements of the system.

- Distorted performance metrics and figures:

  As contested tools, these systems will be accompanied by metrics and figures to try to legitimize their use by either police forces or vendors of the systems. These figures and metrics should be robustly interrogated and questioned by the public, media and civil society, taking into consideration at least two issues: 1) some metrics and figures may be the result of ideal or laboratory-scenario testing as opposed to real-life settings, and 2) some metrics and figures may be in respect of a specific use case of FRT which may not be relevant to, or reflective of, the proposed use case under consideration by a police force or state passing legislation for FRT use.

  In the interests of democracy and transparency, citizens and residents of a state must know what tools are used to monitor them. For a hugely controversial technological tool such as FRT, there must be robust public scrutiny regarding how the tool's accuracy figures are measured and the conditions within which the tool is tested.

- Multiplicity of actors leading to a chain of cumulative flaws:

20 See Akbari, A, "Facial Recognition Technologies 101. Technical insights" in *The Cambridge Handbook of Facial Recognition in the Modern State*, March 2024, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/8B3039F97B11F43B78E52BBEB73E8479/9781009321198c3_29-43.pdf/facial_recognition_technologies_101.pdf.

Many different actors are involved in the development and deployment of facial recognition systems, at different points in time and with diverse interests that may affect the system's final performance. Some of those actors, such as academics developing an algorithm, may be unaware of its future use.

Some other actors involved in these systems may not have the public interest as a priority. For example, data brokers (whose business is collecting personal data to sell it, or its use, to third parties) could provide training datasets, a tech provider could implement an algorithm in a commercial tool or a contractor could offer an "integral solution" (that includes parts acquired from third parties).

Finally, the policy makers who may play a role in the design of a system, the data controllers responsible for the image databases used and the police authorities who are the final users of the systems are some of the other human actors involved in the development and deployment of facial recognition systems. They may lack the technical training to understand the implications of the system they are trying to regulate.

Having a deep understanding of the diverse actors involved in the development and deployment of facial recognition systems, from their creation to their use, is of significant value for understanding why the use of FRT by police is so problematic for the protection of fundamental rights. Such knowledge is also valuable for better understanding where and why issues regarding transparency and accuracy arise.

Types of FRT

For the purposes of these principles, we use the following definitions:

1. Real-time or live facial recognition:

    a. Real-time or live facial recognition involves comparing a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert for police or the user. Such systems involve capturing people's biometric facial data in a live video feed, comparison against a watchlist and possible identification, all of which occur instantaneously, near-instantaneously or without a significant delay. Examples:

        i. The use of live FRT by London's Metropolitan Police in the UK.[21]

        ii. The use of live FRT by US retail chain Rite Aid.[22]

        iii. The use of live FRT by authorities in Moscow, Russia.[23]

---

21 Metropolitan Police Service live facial recognition policy document, https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf.

22 Bhuiyan R, "Rite Aid facial recognition misidentified Black, Latino and Asian people as 'likely' shoplifters", *The Guardian*, 20 December 2023, https://www.theguardian.com/technology/2023/dec/20/rite-aid-shoplifting-facial-recognition-ftc-settlement.

23 Vincent, J, *Moscow rolls out live facial recognition system with an app to alert police*, The Verge, 30 January 2020, https://www.theverge.com/2020/1/30/21115119/moscow-live-facial-recognition-roll-out-ntechlab-deployment.

2. Retrospective remote facial biometric identification:

    a. Retrospective facial recognition involves comparing images of faces of unknown people against a reference image database of known people in order to attempt to identify the former. For each search the system returns a list of potential candidates accompanied by similarity scores. There is no guarantee that the person whose identity is being sought will be in the reference database or that, if the "true match" *is* in the reference database, they will be given the highest similarity score on the candidate list; nor is there any guarantee that the person running the FRT search will choose the correct candidate if they do appear in the candidate list. Examples:

        i. The use of FRT to track down a demonstrator in Moscow.[24]

        ii. The use of FRT which led to the misidentification and wrongful arrests in the USA of Robert Williams,[25] Michael Oliver,[26] Nijer Parks,[27] Randal Reid,[28] Alonzo Sawyer,[29] Porcha Woodruff[30] and Harvey Eugene Murphy, Jnr.[31]

        iii. The use of FRT in Argentina when Guillermo Ibarrola was misidentified and wrongfully arrested, detained and accused of carrying out an armed robbery in a city he had never visited, 600 kilometres from his home city of Buenos Aires.[32]

3. Operator-initiated facial biometric identification system:

---

24 *Glukhin v Russia*, App. No(s),11519/20,https://hudoc.echr.coe.int/eng?i=001-225655

25 Williams, R, *I Did Nothing Wrong. I Was Arrested Anyway*, American Civil Liberties Union, 15 July 2021, https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

26 Stokes, E, *Wrongful arrest exposes racial bias in facial recognition technology*, CBS News, November 2020, https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/.

27 Bryan, K et al., "Government Users of Facial Recognition Software Sued by Plaintiff Alleging Wrongful Imprisonment Over Case of Mistaken Identity", *The National Law Review*, January 2021, https://natlawreview.com/article/government-users-facial-recognition-software-sued-plaintiff-alleging-wrongful.

28 Hill, K & Mac, R, "'Thousands of Dollars for Something I Didn't Do'", *The New York Times*, 31 March 2023, https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

29 Johnson, K, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, Wired, 28 February 2023, https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

30 Hill, K, "Eight months pregnant and arrested after false facial recognition match", *The New York Times*, 6 August 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

31 Robledo, A, "Texas man says facial recognition led to his false arrest, imprisonment, rape in jail", USA Today, 24 January 2024, https://eu.usatoday.com/story/news/nation/2024/01/24/sunglass-hut-robbery-facial-recognition-arrest/72343044007/.

32 Naundorf, K, *The Twisted Eye in the Sky Over Buenos Aires*, Wired, 13 September 2023, https://www.wired.com/story/buenos-aires-facial-recognition-scandal/.

a. Operator-initiated facial recognition is a near real-time use of FRT, where an officer takes a photograph of a person on a mobile device and uses that image for an immediate search against a reference image database. Similar to retrospective FRT, each search will return a candidate list with a similarity score. Examples:

    i. The use of the Blue Wolf facial recognition system by Israeli authorities against Palestinians.[33]

    ii. Use of operator-initiated FRT by South Wales Police.[34]

33 Robins-Early, N, "How Israel uses facial-recognition systems in Gaza and beyond", *The Guardian*, 19 April 2024, https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians.

34 Facial Recognition Technology, South Wales Police, https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/.

Policing FRT: the rights, risks and harms

Real and potential impact on human rights

To hinge the decision of whether a police force should use an FRT system on its purported "accuracy" is, wilfully or unwittingly, to misunderstand the contextual complexity of this biometric technology and its potential far-reaching implications for fundamental human rights.

Even if *all* policing FRT systems were accurate 100 percent of the time, the risks for people's fundamental human rights would multiply significantly. FRT systems risk stripping people of their anonymity, reducing them to walking licence plates[35] and tilting the power dynamic inherent in police–civilian interactions further towards police.

To ensure this powerful surveillance technology is not misused, abused or normalized, the entire lifetime of an FRT system, its connection to other surveillance systems, the use, storage and destruction of facial biometric identifiers and the technical and organizational safeguards in place (or not) to

35 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, European Data Protection Board, adopted 26 April 2023, p.15, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

protect those identifiers all have to be considered when one contemplates the potential human rights risks associated with FRT.

In the interests of democracy and the right to a fair trial, we must know which surveillance tools may lead to us being arrested or accused. As such, consideration must also be given to mechanisms for transparency and oversight of each component of FRT and of each step in the use of FRT by police, the independence and efficacy – or lack thereof – of such mechanisms and the question of how to hold accountable the ever-changing policing FRT systems and the developers, manufacturers and users of those systems.

> *Even if all policing FRT systems were accurate 100 percent of the time, the risks for people's fundamental human rights would multiply significantly. FRT systems risk stripping people of their anonymity, reducing them to walking licence plates and tilting the power dynamic inherent in police–civilian interactions further towards police.*

Fundamental rights at risk with police use of FRT

The following rights are engaged by police use of FRT. The level of impact on these rights depends, like every individual use case of an FRT system by police (whether retrospective, live or operator-initiated) on many factors. These include the architecture of the system – including its subsystems and the algorithms at the heart of it, the dataset the algorithms have been trained on and the purpose of the FRT use – whom the technology is used against and the consequences of its use.

None of the following fundamental rights are absolute and it is acknowledged that states may interfere with fundamental rights in the pursuit of legitimate public interest objectives, provided the interferences are proportionate, are limited to what is necessary in a democratic society and are the least intrusive methods. A balance must be struck between ensuring that a state has effective and legitimate tools at its disposal in order to fulfil its functions and the protection of fundamental rights and freedoms. It should also be noted that when we consider the use of FRT by police, different jurisdictions respect and uphold the following

rights differently and to differing degrees, giving further context to the human rights implications of FRT use.

I. RIGHT TO DIGNITY

As stated by the Universal Declaration of Human Rights, all humans are born free and equal in dignity and rights.[36] By virtue of being human, all people deserve respect.

A person's facial biometric data is permanently and irrevocably linked to their identity. The processing of biometric data under *all* circumstances constitutes a serious interference in itself with several rights, including privacy, regardless of the outcome of the identification attempt (incorrect or correct).[37] This intrusiveness is one of the reasons a person's biometric data is given extra legal protection in certain states.[38]

This serious interference is linked with the right to dignity, to be valued, respected and treated ethically and not as a commodity.[39] Should a person feel they are under surveillance – constant or otherwise – as a consequence of FRT, they may change their behaviour in order to avoid locations, social scenarios or cultural events where FRT is deployed, thereby severely impacting their ability to live a dignified life.[40]

As the European Data Protection Board warns, "Human dignity requires that individuals are not treated as mere objects. FRT calculates existential and highly personal characteristics, the facial features, into a machine-readable form with

---

36 Article 1, Universal Declaration of Human Rights, https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

37 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, European Data Protection Board, adopted 26 April 2023, p.5, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

38 Article 4(14) of the EU General Data Protection Regulation defines "biometric data" as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Under Article 9 of the GDPR the processing of biometric data is prohibited, save for certain circumstances. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Also see Biometric Information Privacy Act, Illinois State Legislature, 2008, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

39 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, European Data Protection Board, adopted 26 April 2023, p.15, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

40 *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, European Union Agency for Fundamental Rights, 2020, p.20, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

the purpose of using it as a human license plate or ID card, thereby objectifying the face."

II RIGHT TO PRIVACY

The right to privacy is an expression of human dignity and is linked to the protection of autonomy and personal identity.[41] It includes a reasonable expectation of privacy while in public and is recognized as a "gateway" right, given it enables the realization of other rights.

Should a policing FRT system enable members of the public to be identified in public spaces, and/or their movements, interests and associations to be tracked, either in real time or in retrospect, they are at risk of losing not only their privacy rights but also the associated rights built upon privacy. These include the right to protest, to freely associate with others and to express one's sexuality, religious belief and/or political affiliation.

The manner in which FRT engages the right to privacy can be exacerbated when the FRT system is used live from a distance or in retrospect, without the person's consent, active involvement or knowledge. This is a point of critical importance when we consider the use of FRT by police, as some uses of FRT could amount to covert and/or sustained mass surveillance. In addition, the fact that FRT watchlists and reference databases, and the scanning of multiple people in real time or retrospect, unavoidably involve the processing of facial data belonging to people who have nothing to do with certain crimes, but potentially remain in a virtual line-up,[42] underscores how FRT seriously interferes with people's right to privacy.

III RIGHTS TO FREEDOM OF EXPRESSION, FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

The rights to freedom of opinion and expression are indispensable conditions for the full development of the person, provide for the exchange and development of opinions in society and, together, constitute the foundation stone of every free and democratic society.[43] The fundamental human right of peaceful assembly

41 *A/HRC/55/46: Legal safeguards for personal data protection and privacy in the digital age*, Office of the High Commissioner of Human Rights, 18 January 2024, https://www.ohchr.org/en/documents/thematic-reports/ahrc5546-legal-safeguards-personal-data-protection-and-privacy-digital.

42 Garvie, C, Bedoya, A & Frankle, J, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology, October 2016, https://www.perpetuallineup.org/risk-framework.

43 UN Human Rights Committee, General comment No.34, CCPR/C/GC/34, para.2., https://documents.un.org/doc/undoc/gen/g11/453/31/pdf/g1145331.pdf.

and association enables and protects individuals' ability to express themselves individually and collectively.[44]

If a police force uses FRT, in a live, operator-initiated or retrospective manner, to monitor and/or seek to identify people who are freely gathering, attending a protest in a public space or congregating in a place of worship, the technology could potentially reveal the political leanings of individuals and/or their religious beliefs. Even if police were seeking to find a specific individual at a protest whom they have included on a watchlist via a legal mechanism, some uses of FRT could result in every person attending the demonstration – the majority of whom would be of no interest to police – having their biometric data processed, and possibly stored, in real time or in retrospect without their knowledge, active involvement or consent.

The mere knowledge that police are using FRT in such a way severely affects people's reasonable expectation of being anonymous in a public space, and could result in a chilling effect on citizens' ability or decision to gather, express their opinions, freely exchange information and engage in behaviour that is necessary and vital for a healthy democracy, thereby impairing political participation.[45] Experts have warned that the long-term chilling effects of FRT on democratic societies have not been fully examined by the courts or the police.[46]

IV RIGHT TO PROTECTION OF PERSONAL DATA

Everyone has the right to the protection of their personal data. Police use of intrusive technologies, such as FRT, can pose significant risks to data protection rights, as it involves processing sensitive personal data and can lead to discriminatory and biased outcomes for individuals. It also raises questions concerning consent.

Just because a person is aware they have been photographed or recorded by CCTV in a public space, this does not mean that they have agreed to make

44 UN Human Rights Committee, General comment No.37, CCPR/C/GC/37, para.1, https://documents.un.org/doc/undoc/gen/g20/232/15/pdf/g2023215.pdf.

45 Murray, D et al., "The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe", *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, pp. 397–412, https://doi.org/10.1093/jhuman/huad020.

46 Murray, D, "Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework", *Modern Law Review*, December 2023, https://doi.org/10.1111/1468-2230.12862.

their biometric data public and/or consented to this data being extracted from an image, processed to create a biometric template and stored or used for identification purposes by police in real time or at some point in the future. Different states have varied, and in some cases no, legal safeguards for the retrieval of biometric data and the use, retention and/or destruction of the same.

Depending on the use case of FRT, its interference with the right to protection of personal data would be heightened considerably if a person is subjected to any manner of "profiling" or automated processing. Such processing might see a person's biometric facial data used to evaluate certain of their personal aspects and/or to analyse or erroneously predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

V RIGHT TO EQUALITY AND NON-DISCRIMINATION

Everyone is equal before the law and entitled without any discrimination to equal protection of the law.[47]

When used to try to identify a person, different policing uses of FRT systems composed of different algorithms and trained on different datasets amid differing conditions can result in different error rates. But while error rates will vary depending on the multiple factors which can affect the performance of an FRT system, these errors do not affect all individuals equally. Studies on FRTs have clearly demonstrated racial and gender biases,[48] meaning women and people of

47 Article 7, Universal Declaration of Human Rights, https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

48 Buolamwini, J & Gebru, T, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. See also Buolamwini, J, *Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces*, Medium, 25 January 2019, https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

See also Deborah Raji, I & Buolamwini, J, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products", *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, https://dl.acm.org/doi/10.1145/3306618.3314244. See also Cook, C, Howard, J, Sirotin, Y, Tipton, J & Vemury, A, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2019, https://ieeexplore.ieee.org/document/8636231. See also *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, 19 December 2019. NIST wrote: "How accurately do face recognition software tools identify people of varied sex, age and racial background? According to a new study by the National Institute of Standards and Technology (NIST), the answer depends on the algorithm at the heart of the system, the application that uses it and the data it's fed – but the majority of face recognition algorithms exhibit demographic differentials. A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another." https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

colour are more likely to be misidentified by FRT and, therefore, potentially more likely to be wrongfully accused by police who use FRT than light-skinned men.

In addition, some authorities are more likely to apply FRT to marginalized communities which are already over-surveilled, over-policed and over-incarcerated,[49] meaning FRT can be used as a tool to create or deepen structural inequalities and discrimination. These biases are deeply compounded by law enforcement authorities who fail to even acknowledge that, let alone take steps to understand why, these technological biases occur, or fail to ask robust questions about the technology they purchase and deploy relevant to the demographic of people they are using it against. Misunderstandings about so-called "accuracy" figures[50] further exacerbate these issues, which threaten people's right to equal protection against discrimination.

VI RIGHTS OF PEOPLE WITH DISABILITIES

The former UN Special Rapporteur on the rights of persons with disabilities has previously documented that some FRT algorithms have inherent biases against people with disabilities and especially people with conditions such as Down syndrome, achondroplasia, cleft lip or palate, or other conditions that result in facial differences.

He reported that these issues have resulted in some people with disabilities being "judged untrustworthy" because their face did not conform to the standard programmed in the respective FRT system. The special rapporteur has called on states to consider imposing a moratorium on the sale and use of FRTs until a full audit of the effects of FRT involving representative organizations of people with disabilities can be carried out.[51]

---

49 Amnesty International, *Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid*, 2 May 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

50 Gerchick, M & Cagle, M, *When it Comes to Facial Recognition, There is No Such Thing as a Magic Number*, American Civil Liberties Union, 7 February 2024, https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number.

51 *Report of the Special Rapporteur on the rights of persons with disabilities on Artificial Intelligence and the rights of persons with disabilities*, December 2021, https://www.ohchr.org/en/calls-for-input/2021/report-special-rapporteur-rights-persons-disabilities-artificial-intelligence.

VII RIGHT TO PRESUMPTION OF INNOCENCE

A fundamental element of fair trials and the rule of law is that every human being is innocent until proven guilty.[52]

The use of FRT by a law enforcement authority requires them to run a biometric template against a reference database of biometric templates, if used retrospectively, or to run biometric templates taken from a live video feed and compare them to a "watchlist" of biometric templates if used live. These processes, by their nature, effectively necessitate the generation of multiple false matches. What this means is that ultimately, because of these systems, innocent people will always end up on lists used by law enforcement when they seek to find and/or identify a suspect or person of interest.

When a person is included in a reference database, in some cases simply because they own a driver's licence or passport,[53] or on a watchlist, because of a usually unknown or entirely opaque[54] set of criteria established by a law enforcement authority, this inclusion of their biometric facial data means that they will be subject to searches by police who are seeking either to find or to identify a person of interest. This effectively means that every person in a database or on a watchlist is treated as a potential criminal suspect or person of interest, thereby intruding on their right to presumption of innocence. It means many people who have nothing to do with a specific crime being investigated, for which an FRT search is carried out, could erroneously face potentially grave consequences, as has happened in the case of misidentifications.

It is becoming increasingly clear that issues around misidentification are further compounded by how a person's image is later used in a photographic line-up.[55]

If a person's biometric template is kept in a specific reference database or watchlist routinely used or accessed by a law enforcement authority, they could

52 Article 11, Universal Declaration of Human Rights, https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

53 Boffey, D, "Police to be able to run face recognition searches on 50m driving licence holders", *The Guardian*, 20 December 2023, https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-searches-on-50m-driving-licence-holders.

54 *Big Brother Watch: complaint against private sector facial recognition*, AWO Agency, https://www.awo.agency/blog/big-brother-watch-complaint-against-private-sector-facial-recognition/. See also https://www.awo.agency/files/2022-07-25-Facewatch-Coop-ICO-Complaint.pdf.

55 Hill, K, "Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes", *New York Times*, 29 June 2024, https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html#:~:text=The%20person%20running%20the%20search,provided%20the%20store's%20surveillance%20video.

be said to be trapped in a perpetual virtual line-up, even when they have no link whatsoever to a specific crime.[56]

VIII RIGHT TO EFFECTIVE REMEDY

Everyone has the right to an effective remedy for acts violating their fundamental rights.[57]

Whether a police force uses FRT in a live, retrospective or operator-initiated manner to either monitor or seek to identify a person, even when it does so legally, the system can, and does, get it wrong. This is because the technology is not designed to give police a single positive identification or "match". Instead, at best, it gives a person using FRT a guess list of who the person could be – a list of potential candidates accompanied by similarity scores.

A threshold value is fixed to determine when the software will indicate that a probable match has occurred. Should this value be fixed too low or too high, it can create a high false positive rate or a high false negative rate respectively. There is no single threshold setting which eliminates all errors. In addition, the length of the returned candidate list will depend on the configuration set by the user.

Either way, there is no guarantee that the "true match" will be returned in the list, as the person being sought may not be in the reference database. Nor is there a guarantee that, if the person is actually in the reference database, they will be at the top of the candidate list returned; there is also no guarantee that the police officer will choose the "true match" from the list, if such a match even exists.

The initial stages of a live FRT operation are entirely based on automated processing, whereby the system runs images captured on a live feed against images on a watchlist and creates alerts for potential actions to be taken. Similar to the retrospective FRT systems, whether so-called "matches" are found depends on the selected "similarity setting". Studies show the lower the threshold is set, the more matches will be found but the less accurate those so-called "matches" are likely to be, while a higher threshold yields fewer matches with a higher degree of confidence in their accuracy.[58]

---

56 Garvie, C, Bedoya, A & Frankle, J, *The Perpetual Line-Up, Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology, October 2016, https://www.perpetuallineup.org/.

57 Article 8, Universal Declaration of Human Rights, https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

58 Fussey, P & Murray, D, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Human Rights Centre, University of Essex, July 2019, p.107, https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

These inescapable issues with FRT give rise to innocent people who may happen to look like other people being dragged into a net of police suspicion without just cause. When people are wrongfully subjected to police action on the basis of FRT use and are neither informed that the action was contingent on FRT[59] nor able to take litigation to find out exactly how FRT was used against them,[60] this raises serious concerns about people's right to an effective remedy. Given this is a relatively new technology in policing, this issue is becoming more apparent as further cases of misidentification and wrongful arrests come to light.[61]

When a person is misidentified as someone accused of a crime, the impact on their life can be detrimental whether that impact is based on an action taken immediately after the misidentification, as in a live situation,[62] or after some time, as in a retrospective situation.[63]

However, crucially, concerns about the right to an effective remedy do not pertain to misidentifications alone. When the technology gets it "right" and correctly identifies a person, this does not necessarily mean that the use of the system is legitimate, proportionate, necessary and compliant with human rights.[64] The use of FRT which "correctly" identifies people can still lead to the most egregious human rights abuses[65] and, when combined with other surveillance technology and weapons systems, even war crimes.[66]

---

59 MacMillan, D et al., "Police seldom disclose use of facial recognition despite false arrests", *Washington Post*, 6 October 2024, https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/.

60 Williams, R, "I Was Wrongfully Arrested Because of Facial Recognition Technology. It Shouldn't Happen to Anyone Else", *Time*, 29 June 2024, https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/.

61 Sanford, A, *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*, Innocence Project, 14 February 2024, https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/.

62 Clayton, J, "*I was misidentified as shoplifter by facial recognition tech*", BBC, 26 May 2024, https://www.bbc.com/news/technology-69055945.

63 Bhuiyan, J, "Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit", *The Guardian*, 23 January 2024, https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.

64 *Glukhin v Russia*, App. No(s),11519/20, https://hudoc.echr.coe.int/eng?i=001-225655.

65 Gan-Mor, G & Pinchuk, A, *In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World: Surveillance in the West Bank/Occupied Palestinian Territories*, International Network of Civil Liberties Organizations, January 2021, p.11, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf. See also *Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT*, Amnesty International, May 2023, https://www.amnesty.org/en/documents/mde15/6701/2023/en/. See also Frenkel, S, "Israel Deploys Expansive Facial Recognition Program in Gaza", *New York Times*, 27 March 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html?ugrp=c&unlocked_article_code=1.f00.5DIt.O0vT0ELrgEOM&smid=url-share.

66 Fatafta, M, and Leufer, D, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes*, Access Now, 9 May 2024, https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/.

IX RIGHT TO FAIR TRIAL AND DUE PROCESS

The real-life impact of FRT use by law enforcement – whether it fails[67] or functions[68] – can be devastating. In the USA alone, there are, at the time of writing, seven known cases of law enforcement wrongfully arresting and incarcerating people on the basis of the police using error-prone FRT, six of whom are Black.[69] But it is unknown how many people wrongfully arrested and incarcerated in the USA may have taken plea deals.[70] If law enforcement authorities fail to disclose the use of FRT to people who have been detained, questioned, arrested, charged or prosecuted following an FRT search, this is a clear infringement of their right to due process and, in cases of prosecution, a fair trial.[71]

The opacity around the use of FRT systems and how they operate can obfuscate defendants' ability to fully understand how a case was built against them and, in some cases, deny them the means to challenge the accuracy and reliability of those systems in court. This issue is of even greater concern when a defendant is part of a demographic that suffers disproportionately due to the bias issues in FRT, and may need greater technical expertise to challenge the system's results. All of the above results in an imbalance of access to information and power in the police–civilian dynamic that is incompatible with due process.

67 Williams, R, *I Did Nothing Wrong. I Was Arrested Anyway*, American Civil Liberties Union, 15 July 2021, https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

68 *Glukhin v Russia*, App. No(s),11519/20, https://hudoc.echr.coe.int/eng?i=001-225655.

69 *ACLU calls on Detroit Police Department to end use of faulty facial recognition technology following yet another wrongful arrest*, American Civil Liberties Union, 7 August 2023, https://www.aclumich.org/en/press-releases/aclu-calls-detroit-police-department-end-use-faulty-facial-recognition-technology.

70 Press, E, "Does A.I. Lead Police to Ignore Contradictory Evidence?", *The New Yorker*, 13 November 2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.

71 MacMillan, D et al., "Police seldom disclose use of facial recognition despite false arrests", *Washington Post*, 6 October 2024, https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/.

Assessing the human rights impact of policing FRT use

Is the use of FRT by police in compliance with international human rights?

Many of our rights are enshrined in the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights, the European Charter on Fundamental Rights (EU Charter) and the Inter-American Convention on Human Rights (IACHR).[72]

These rights are not absolute. However, according to international human rights law, generally speaking our rights may only be restricted or limited as long as the restriction:

- Is provided or prescribed by law and is not arbitrary;
- Pursues a legitimate aim;

72 See Articles 8–11 ECHR, Articles 12, 17, 18, 19, 21 and 22 ICCPR, and Articles 11, 12, 13, 15 and 16 IACHR.

- Is strictly necessary in a democratic society to achieve the aim in question; and
- Is proportional to the legitimate aim.

PRESCRIBED BY LAW AND NOT ARBITRARY

The meaning of "law" in this context implies certain minimum requirements of clarity, precision, accessibility and predictability. This is to allow individuals to foresee the consequences of their actions and regulate their behaviour and conduct accordingly, but also to safeguard against states arbitrarily interfering with people's rights when they exercise their power. As such, a law providing for the use of FRT – and therefore the processing of biometric facial data – that is not public cannot be considered a law, while merely passing a law allowing FRT use which fails to meet the basic requirements of clarity and accessibility in the first place, cannot be considered "lawful". Any interference with a right must have a legal basis, and that legal basis must be of sufficient quality to protect against arbitrary interferences.

- **Example:** In the case of Europe, the European Data Protection Board has stated the following in respect of police use of FRT:

  "The legal basis must be sufficiently clear in its terms to give citizens an adequate indication of conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance. A mere transposition into domestic law of the general clause in Article 10 LED73 would lack precision and foreseeability."[74]

- **Example:** In the UK, where police use live and retrospective FRT, there is no explicit or dedicated legal basis for the use of FRT by police. Instead the police rely on a range of other pieces of legislation and common law powers.[75]

---

73 Article 10, Law Enforcement Directive: Processing of special categories of personal data: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject."

74 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, European Data Protection Board, p. 5, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

75 The Data Protection Act 2018, Regulation of Investigatory Powers Act 2000, Protection of Freedoms Act 2012, Human Rights Act 1998, Equality Act 2010, Police and Criminal Evidence Act 1984.

Example: Research into 38 FRT initiatives in 9 Latin American countries found just 14 of them indicated an existence of regulations to support the use of FRT; even then, most of the regulations did not strictly provide for FRT use but, rather, broadly allowed for powers to use FRT ("to oversee compliance with provisions on evasion in public transport", for "immigration verification functions, foreigners and immigration control", etc.)[76]

PURSUES A LEGITIMATE AIM

The rights to privacy, freedom of expression and freedom of association come with limitation clauses. For example, an interference with the right to privacy under the European Convention on Human Rights could only be considered legitimate if it is "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[77] But if there is no evidence that a person's conduct has any link with a legitimate aim, then there is little or no justification for an interference with their rights.

- **Example:** Article 6 of the EU's Law Enforcement Directive (LED) obliges data controllers to distinguish between different categories of data subjects (i.e. people). On this, the European Data Protection Board has said:

  "With regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference. If no distinction according to Article 6 LED is applicable or possible, the exception from the rule of Article 6 LED has to be rigorously considered in the assessment of the necessity and proportionality of the interference."[78]

  It added that distinguishing between different categories of data subjects is "an essential requirement when it comes to personal data processing

76 Venturini, J and Garay, V (Nogueira, P trans.) *Facial recognition in Latin America Trends in the implementation of a perverse technology*, AlSur, 2021, https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf.

77 Article 8 (2), European Convention on Human Rights.

78 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, European Data Protection Board, p. 23, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

involving facial recognition" due to the potential for false positive and false negative hits.

NECESSARY IN A DEMOCRATIC SOCIETY TO ACHIEVE THE AIM IN QUESTION

The final part of the three-part test involves identifying the range of rights engaged by the interference in order to determine the necessity or otherwise of the measure, and to determine whether or not the interference appropriately or inappropriately undermines other competing rights. As part of this assessment, a proposed measure should be supported by evidence describing the problem that is being addressed by the measure, how the measure will be genuinely effective in addressing the problem, a determination as to whether or not the measure is the least intrusive measure to address the problem and an explanation as to why existing measures cannot address the problem. Whenever we consider a surveillance measure, tool or law, especially one as powerful, at scale, intrusive and invasive as FRT in all its use cases, we must consider whether or not it is efficacious. This is because a surveillance tool or measure's efficacy speaks to its necessity and proportionality. In addition, if a proposed measure includes the processing of sensitive data, such as biometric facial data, a higher threshold should be applied to the assessment of effectiveness.

- **Example:** In *Glukhin v Russia*, the European Court of Human Rights held that Russia's use of FRT to identify and apprehend a peaceful protester breached the protester's privacy and freedom of expression rights. The court held the applicable domestic legal provisions did not meet the "quality of law" requirement and that the processing of Mr Glukhin's personal data using FRT could not be regarded as "necessary in a democratic society". Specifically, it noted: "The domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or the processing of sensitive personal data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, any supervisory control mechanisms or the available remedies."[79]

79 *Glukhin v Russia*, App. No(s),11519/20, https://hudoc.echr.coe.int/eng?i=001-225655.

- **Example:** In *S. and Marper v the United Kingdom*,80 the European Court of Human Rights held that the UK's indefinite retention of biometric data (in this case, fingerprints and DNA samples) of people charged but not convicted was not necessary in a democratic society. Holding that the UK failed to strike a fair balance between competing public and private interests, it stated: "The Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society."

IS PROPORTIONAL

If the necessity test is not satisfied, there is no need to carry out a proportionality test. However, if the necessity test *is* satisfied, then a proportionality test must be carried out. The principle of proportionality is based on the idea that a measure should not exceed what is necessary to achieve the objective. As such, the measure's advantages should not be outweighed by its disadvantages. A test assessing the proportionality of a measure on a case-by-case basis must assess the importance of the objective and whether the measure meets the objective, must assess the scope, extent and strength of the interference, and must examine what safeguards are in place in respect of the measure, in order to reduce the rights risks associated with the measure.

- **Example:** As stated by the European Data Protection Supervisor: "At the core of the notion of proportionality lies the concept of a balancing exercise: the weighing up of the intensity of the interference *vs* the importance ('legitimacy', using the wording of the case law) of the objective achieved in the given context.
  "A well-performed test needs the express identification, and structuring

80 *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.

> into a coherent framework, of the different elements upon which the weighting depends, in order to be complete and precise."[81]

Is it reliable? Is it discriminatory?

There are several steps involved in the use of FRT, whether the use is live, retrospective or operator-initiated. Each stage presents opportunities for risks of error/misidentification and discriminatory, disproportionate and unnecessary surveillance. As such, all stages have to be carefully considered when there is an assessment of how FRT impacts people's fundamental rights,[82] and given FRT has clearly demonstrated racial and gender biases,[83] these biases must always be remembered when each step of an FRT use is considered. The answers to the following questions may also have a bearing on the aforementioned tests as to whether a use of FRT is provided by law and not arbitrary: does it pursue a legitimate aim? Is it strictly necessary in a democratic society? And is it proportionate to the legitimate aim? INCLO is grateful for the research, audit assessments, model laws and ethical frameworks created by Radiya-Dixit,[84] Davis,

---

81 EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

82 EFF, Electronic Privacy Information Center (EPIC) and the National Association of Criminal Defense Lawyers (NACDL), amicus brief in *State of New Jersey v. Francisco Arteaga*, https://www.eff.org/document/state-new-jersey-v-francisco-arteaga.

83 Buolamwini, J, and Gebru, T, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. See also Deborah Raji, I, and Buolamwini, J, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products", *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, https://dl.acm.org/doi/10.1145/3306618.3314244. See also Cook, C, Howard, J, Sirotin, Y, Tipton, J, and Vemury, A, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems". *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2019 https://ieeexplore.ieee.org/document/8636231. See also *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, 19 December 2019. NIST wrote: "How accurately do face recognition software tools identify people of varied sex, age and racial background? According to a new study by the National Institute of Standards and Technology (NIST), the answer depends on the algorithm at the heart of the system, the application that uses it and the data it's fed – but the majority of face recognition algorithms exhibit demographic differentials. A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another." https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. See also Findley, B, "Why Racial Bias is Prevalent in Facial Recognition Technology", *Harvard Journal of Law and Technology*, November 2020, https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology.

84 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1 October 2022, https://doi.org/10.17863/CAM.89953.

Perry and Santow,[85] and Lynch, Campbell, Purshouse and Betkier[86] in helping to identify and shape these questions.

PROBE IMAGE

This involves a police officer, via a mobile device, CCTV or another source, obtaining an image of a person to run against a database of images of known people, using FRT. Questions to be considered in respect of this step include:

- Where does the probe image come from?
- Why was this image chosen?
- Who took the image?
- How old is the probe image?
- Was it taken from CCTV, a body-worn camera, a mobile phone or a social media account?
- Was it lawfully/legally obtained, stored and shared?
- What is the quality of the image? How high is the resolution? How good is the lighting?
- Is the person looking directly at the camera in the image?
- Is anything obstructing the person's face?
- Who had access to the image before it was used in an FRT search?
- Is there a legal basis for processing the image in a manner which leads to the extraction of the facial features of the person in the image, thereby creating biometric data?
- Is there a robust and effective oversight mechanism to safeguard the fundamental rights of the person whose image is being probed?

REFERENCE DATABASE SELECTION

85 Davis, N, Perry, L & Santow, E, *Facial Recognition Technology: Towards a model law*, Human Technology Institute, The University of Technology, September 2022 https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf.

86 Lynch, N, Campbell, L, Purshouse, J & Betkier, M, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework*, Law Foundation of New Zealand, 30 November 2020, https://doi.org/10.25455/wgtn.17204078.v1.

Similar to probe images, reference database selection plays a significant role not only in the reliability of a retrospective FRT search but also in how discriminatory a system can be in terms of who is subjected to an FRT search. The nature of FRT and the use of reference databases inescapably put innocent people at risk of being misidentified, but they also carry the risk of surveillance. For example, in Buenos Aires, Argentina, the city's live FRT system, which was set up to search for fugitives, was found to be unconstitutional for several reasons, not least because some 15,459 people who were *not* fugitives were included in the database without judicial approval. This resulted in FRT searches of the president, politicians, human rights activists and journalists – not just fugitives.[87] Questions to be considered include:

- How was the database of images compiled?
- Are there clear, objective and limited criteria with regard to who is added to the database?[88]
- Has there been a fundamental rights risk assessment carried out in respect of the people whose images are in the database?
- Where did the images originate?
- What technical and security measures are in place to secure the database and prevent wrongful access to it?
- If the database of images is sourced from the criminal justice system, what is the legal basis for using those images?
- If the database of images is sourced from the criminal justice system, are the images of people who have been arrested, charged and/or convicted?
- If the database of images is sourced from the criminal justice system, is there a legally defined retention period for storing those images?
- If the database of images is sourced from the criminal justice system, is there a risk that a disproportionate number of people from a particular community will be in that database because members of that community

87 Naundorf, K, *The Twisted Eye in the Sky Over Buenos Aires*, Wired, September 2023, https://www.wired.com/story/buenos-aires-facial-recognition-scandal/.

88 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1 October 2022, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf. See also *Guidelines on facial recognition*, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Council of Europe, June 2021, https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

are already overrepresented in the state's prisons? (If this is the case, members of those communities will face a higher risk of being misidentified by an FRT search.)

- Does the police force have a code of practice and/or written guidance regarding the retention and deletion of photographs taken by members of the police of people arrested and/or convicted?
- What is the legal basis for either creating or accessing this database?
- Was the database lawfully created and have the images been lawfully stored and processed?
- How old are the images in the database? Are they up to date?
- Were the images taken from CCTV, body-worn cameras, mobile phones or social media accounts?
- What is the quality of the images? How high is the resolution? How good is the lighting?
- Is the database composed of images of people looking directly at the camera?
- Is anything obstructing the faces of the people whose images are in the database?
- What safeguards are in place to protect the security of the database?
- Who has access to the database?
- Is there a logging policy to document who accesses the database, when and how?[89]
- Is there a legal basis for processing the images in the database in a manner which leads to the extraction of the facial features of the people in the database, and a legal basis to allow for an FRT search in respect of a probe image?
- Is the person in the probe image not in the database? (If this is the case, then all estimated matches returned by the system will be incorrect.)

89 Davis, N, Perry, L & Santow, E, *Facial Recognition Technology: Towards a model law*, Human Technology Institute, The University of Technology, September 2022, https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf.

- When a person's image is no longer necessary for the initial purpose of being placed in the database, is it deleted in a timely and effective manner?
- Is there a robust and effective oversight mechanism to safeguard the fundamental rights of the people whose images are in the database?

WATCHLISTS

Watchlists are the reference databases used in the real-time application of FRT, which involves comparing a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert for police or the user to potentially act upon instantaneously, near-instantaneously or without a significant delay. The questions that need to be considered regarding who should and should not be included in a watchlist are the same as those that need to be considered when probe images and reference databases are chosen or populated. Additional questions that need to be asked, for each live use of FRT, include:

- What is the legal basis for placing a person's image on a watchlist for each specific use of live FRT?
- Where will the law enforcement authority get the images to add to a watchlist?
- Will those images be of a certain quality or age?
- How long can an image be on a watchlist?
- How can a person be removed from a watchlist?
- What specific criteria must be met before a person's image is added to a watchlist, or before any watchlist is constructed?[90]
- What protocols must be followed before a person's image is added?
- Who can ask, and give, permission for a person's image to be added to a watchlist per deployment?
- How will the law enforcement authority assess and demonstrate that the creation of a watchlist, or the addition of a person to a watchlist, is necessary and proportionate?

90 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1 October 2022, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf.

- How will a person know if they are on a watchlist?
- What remedy will be available to them if they are wrongfully placed on a watchlist?
- What remedy will be available to them if they are wrongfully misidentified and subjected to an action because of an error in the creation of the watchlist?
- Will the specific details of how and when a person is added to a watchlist be made public for each deployment of live FRT?

POTENTIAL PHOTO EDITING/TAMPERING:

There are documented cases of police authorities editing probe images before running them through a retrospective FRT search, putting the reliability of a search result at considerable risk and, therefore, risking the rights of individuals subsequently apprehended on the basis of the search results. Research from the USA shows the New York Police Department's Facial Identification Section, who are allowed to edit probe images, use tools to do things such as removing a facial expression, inserting a different person's eyes into the image and/or using a tool to create a cheek or chin area if the person in the image is not entirely visible in the image.[91] One alarming situation involved police officers, after running a pixelated CCTV still of a suspected shoplifter through an FRT system and it yielding no potential candidates, thinking it would be a good idea to run a search of Hollywood actor Woody Harrelson through the system because they felt the suspect resembled him. They subsequently arrested a man, "they believed was a match – not to Harrelson but to the suspect whose photo had produced no possible hits".[92] Elsewhere in the USA, police have been found carrying out FRT searches on sketches – that is, hand-drawn or computer-generated images based on descriptions that eyewitnesses have offered police.[93] Questions to be considered include:

- On what grounds can such editing be justified?
- Given the significant rights concerns, should police forces be allowed to alter probe images in this way?

91 Garvie, C, Garbage In, Garbage Out, Georgetown Law Center on Privacy and Technology, 2019, https://www.flawedfacedata.com/.

92 Ibid.

93 Ibid.

- Should there, at the very least, be a legal basis for such editing?

ALGORITHMIC SEARCH:

This step involves the subsystem that compares a probe photo against a database of images, in the case of retrospective or operator-initiated FRT, or facial images obtained from live video footage against facial images on a watchlist. Considering FRT algorithms are created and developed by private companies, are not generally open to independent audits and/or risk assessments, are shown by research to be biased against anyone who is not a white, middle-aged man[94] and are each trained using different datasets and likely produce different results depending on their individual algorithms, the following questions should be considered:

- What steps have the police taken to independently audit the veracity of the vendor's claims about the FRT system/respective algorithm?[95]
- Have proprietary interests prevented the police from obtaining information about how the algorithm works and the risks it poses?[96]
- Is there a legal mechanism to oblige vendors to publish and/or disclose certain information about their algorithms?
- Prior to any use of FRT, do the police regularly carry out fundamental rights impact assessments and demonstrate that their specific use of FRT does not have a detrimental effect on the rights of the public and/or that it does not have the potential to produce discriminatory effects?
- Are the results of these assessments published?
- What steps have the police taken to mitigate the risks posed to people disproportionately affected by FRT?

---

94 *81% of "suspects" flagged by Met's police facial recognition technology innocent, independent report says*, Sky News, 4 July 2019, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941. See also Fussey, P & Murray, D, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Human Rights Centre, University of Essex, July 2019, https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf. See also Buolamwini, J & Gebru, T, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, https://proceedings.mlr.press/v81/buolamwini18a.html.

95 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1 October 2022, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf

96 Lynch, N; Campbell, L; Purshouse, J; Betkier, M, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework*, Law Foundation of New Zealand, 30 November 2020, https://doi.org/10.25455/wgtn.17204078.v1.

- Do the police evaluate and publish the demographic make-up of the training dataset underlying the algorithm, to ensure the dataset is representative of the population where it is to be used?[97]
- Do the police publish the demographic data of those who are subjected to FRT searches?[98]
- Do the police publish the demographic data for arrests, stops and searches, and other outcomes resulting from the use of FRT?[99]
- Do the police have accountability mechanisms in place to address misidentifications when they arise, including a mechanism to notify those affected and offer redress?
- What changes do the police make to their protocols, databases and systems when they become aware that a misidentification has led to a person's stop and search, arrest, detention or charge?
- Do the police have accountability mechanisms in place to address unfair and unwarranted automated decision making when it arises on account of FRT, including a mechanism to notify those affected and offer redress?

Is the human-in-the-loop "safeguard" really a safeguard?

It is often said by police forces wishing to assuage concerns about FRT misidentification and human rights infringements that there is nothing to be concerned about because there will be a "human-in-the-loop" safeguarding against any automated decisions and there will always be a human reviewing a list of candidates before any further steps are taken, whether the use is live or retrospective. However, it is not always the case that a human – whether a police officer or an eyewitness – will correct an incorrect FRT "match". Michael Oliver, who has a face tattoo, was wrongfully arrested and detained for almost three days in Detroit after an FRT search returned him as a suspect and an eyewitness picked him out of a photo line-up, all despite the photo of the suspect displaying

97 Ibid.
98 Ibid.
99 Ibid.

no face tattoo.[100] In respect of human reviews, the following questions should be considered:

- What role does a human reviewer play in the case of retrospective FRT use?
- What role does a human reviewer play in the case of live FRT use?
- What research has the police carried out to demonstrate the accuracy of their human reviewers?[101]
- What specific training have the human reviewers undergone for differing use cases?
- What other information do human reviewers have about a case or individual before or when they are reviewing a candidate?
- Is the human reviewer independent of the investigation into the alleged offence at the centre of the FRT search?
- What steps are taken and/or what safeguards are in place to mitigate against the human reviewer's own biases?[102]
- Do the police have accountability mechanisms in place to address misidentifications after a human review, including a mechanism to notify those affected and offer redress?
- What changes do the police make to their protocols regarding their human reviewer after a misidentification of a person leads to that person being arrested, detained or charged?
- Do "human review" protocols take into consideration, and reflect, the differing rights risks that can stem from live and retrospective use of FRT?
- Is an eyewitness told about the use of FRT by the police?

---

100 "Faulty Facial Recognition Led to His Arrest – Now He's Suing", *Vice*, September 2020, https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing.

101 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1 October 2022, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf.

102 Such as confirmation bias, which refers to the confirmation of the reviewer's personal beliefs, and automation bias which implies a tendency to trust the legitimacy of information on the basis that it was produced by technology.

Is adequate FRT training provided to police officers to mitigate against risks?

Putting a powerful tool such as FRT in the hands of police who are untrained on how to use and understand it, combined with the absence of any independent oversight and assessment of that use, could only serve to further entrench and expand the issues with police use of FRT. It has been reported that, while the US Federal Bureau of Investigation (FBI) has carried out tens of thousands of FRT searches over recent years, just 5 percent of its 200 agents who use the technology have taken the FBI's own course on how to use it.[103] It is unclear what training takes place in other states where FRT is used by police. In respect of oversight, in the UK there is a Surveillance Camera Commissioner, while in the USA there have been calls for a regulatory office to oversee the management and regulation of complex technologies such as FRT, similar to how the pharmaceutical industry is regulated,[104] and/or an independent body charged with certifying policing technologies before they are deployed.[105] Questions to be considered include:

- What would an effective rights-based training course on police use of FRT entail?
- Should a police member receive a certificate or accreditation before being allowed to use FRT?
- Would any such training be enough to mitigate human rights concerns?
- Should details of this training be made public?
- What would an effective oversight body/mechanism look like?
- What powers should such a body have to make it effective and accountable?
- Would having an oversight body or mechanism be enough to mitigate concerns?

---

103 Johnson, K, *FBI Agents Are Using Face Recognition Without Proper Training*, Wired, September 2023, https://www.wired.com/story/fbi-agents-face-recognition-without-proper-training/.

104 Learned-Miller, E, Ordóñez, V, Morgenstern, J, and Buolamwini, J, *Facial Recognition Technologies in the Wild: A Call for A Federal Office*, 29 May 2020, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf.

105 Friedman, B, Heydari, F, Isaacs, M & Kinsey, K, "Policing Police Tech: A Soft Law Solution", *Berkeley Technology Law Journal*, Vol. 37, 2022, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4095484.

- Is there a danger that calls for training and oversight mechanisms ultimately serve to green-light FRT use by police and act as a tick-box exercise?

Are the disproportionately impacted communities consulted adequately?

A significant issue concerning the use of FRT by police is that the very communities disproportionately affected by error-prone technology are not consulted in a transparent manner about the tech, how it works and how it impacts the criminal justice system and people's lives and fundamental rights. Questions to be considered include:

- Should consultation with members of the public and members of communities disproportionately affected by FRT be mandated?
- How could that consultation be effective?
- Should that mandated consultation include details from the police to the public about the specific technology used, the manner in which it is used, how the different subsystems and algorithms work, details of the datasets it was trained on and the production of a data protection impact assessment and fundamental rights impact assessment?
- Should that consultation include details of how probe images are chosen, how reference databases are created and how watchlists are created?
- Should that consultation take place every time the police change their policies or specific technology use?

Are people informed that they are being subjected to FRT?

Another significant transparency issue is members of the public simply not knowing that FRT is being used in their environment. For example, in the UK, when live FRT is being used the police are supposed to alert the public to its use. However, this often happens on social media, which is not a sufficient way of alerting the public considering many people are not on certain social media sites and those who are may not have seen the respective post. Police in the UK are also supposed to mark out the physical area where live FRT is being used so the public can avoid the area should they not wish for their biometric data to be processed.

However, signs are usually placed too close to the area so that it is often too late or too cumbersome to avoid the area. Questions to be considered include:

- Data protection law in the EU provides that individuals have a right to know about the processing of their personal data. For CCTV this means that the data controller of the CCTV must have signs erected to indicate the use of CCTV and those signs must include at least the following information:
    - The identity and contact details of the data controller;
    - The contact details for the data protection officer, if one has been appointed;
    - The purposes for which data is processed;
    - The purpose and legal basis for the processing;
    - Any third parties to whom data may be disclosed;
    - The security arrangements for the CCTV footage;
    - The retention period for CCTV footage; and
    - The existence of data subject rights and the right to lodge a complaint with the local data protection authority.
- Could such signage go some way to mitigate against the transparency issue here?
- How effective, and widely applied, is CCTV signage policy already?

Has the relevant information about the system been disclosed to those accused based on FRT?

A third transparency issue emerging in the USA is that when FRT is used in investigations leading to someone's arrest and the defendant finds themself before the courts, their defence teams are denied access to any information about how that system worked, its propensity for error or bias and even the name of the system itself.[106] But, in a significant win for transparency, in June 2023, in one of the first cases of its kind, the Appellate Division of the Superior Court of New

106 *New Jersey Appellate Division One of First Courts in Country to Rule on Constitutional Rights Related to Facial Recognition Technologies*, ACLU, June 2023, https://www.aclu-nj.org/en/press-releases/new-jersey-appellate-division-one-first-courts-country-rule-constitutional-rights.

Jersey, while noting that FRT is "novel and untested", ruled in *State of New Jersey vs. Francisco Arteaga*[107] that the following, as sought by the defence counsel, had to be disclosed to the defendant:

1. The name and manufacturer of the facial recognition software used to conduct the search in this case, and the algorithm(s), version number(s) and year(s) developed;
2. The source code for the face recognition algorithm(s);
3. A list of what measurements, nodal points or other unique identifying marks are used by the system in creating facial feature vectors including, if those marks are weighted differently, the scores given to each respective mark;
4. The error rates for the facial recognition system used, including false accept and false reject rates (also called false positive or match and false negative or non-match rates), as well as documentation on how the error rates were calculated, including whether they reflect test or operational conditions;
5. The performance of the algorithm(s) used on applicable National Institute of Standards in Technology Face Recognition Vendor Tests, if available;
6. The original copy of the query or "probe" photo submitted;
7. All edited copies of the query or "probe" photo submitted to the facial recognition system, noting, if applicable, which edited copy produced the candidate list that the defendant was in, and a list of edits, filters or any other modifications made to that photo;
8. A copy of the database photo matched to the query or "probe" photo and the percentage of the match, rank number or confidence score assigned to the photo by the facial recognition system in the candidate list;
9. A list or description of the rank number or confidence scores produced by the system, including the scale on which the system is based (e.g. percentage, logarithmic, other);
10. A copy of the complete candidate list returned by the face recognition or the first 20 candidates in the candidate list if longer than 20, in rank order

107 *Superior Court of New Jersey Appellate Division Docket No. A-3078-21 State of New Jersey vs. Francisco Arteaga*, decided 7 June 2023, https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-3078-21.html.

and including the percentage of the match or confidence score assigned to each photo by the facial recognition system;

11. A list of the parameters of the database used, including:
    a. How many photos are in the database;
    b. How the photos were obtained;
    c. How long the photos are stored;
    d. How often the database is purged;
    e. What the process is for getting removed from the database;
    f. Who has access to the database;
    g. How the database is maintained; and
    h. The privacy policy for the database;
12. The report produced by the analyst or technician who ran the facial recognition software, including any notes made about the possible match relative to any other individuals on the candidate list; and
13. The name and training, certifications or qualifications of the analyst who ran the facial recognition search query.

The above list of items is a useful compilation of details to be considered when we seek transparency around the use of FRT by police. Similar details must be disclosed regarding the live use of FRT and, specifically, the parameters of how, why and when a watchlist was created and how a person came to be included.

INCLO principles for law enforcement use of FRT

These principles are designed to address:

- Direct law enforcement use of FRT;
- Any law enforcement use of FRT carried out by a law enforcement authority in a separate jurisdiction; and
- Any law enforcement use of FRT carried out by a third party.

1. Law enforcement authorities must not use FRT without a specific legal basis.
2. Fundamental rights impact assessments should be mandatory.
3. Fundamental rights impact assessments must be independent of vendor assessment.
4. There should be no acquisition or deployment of any new FRT without a guarantee of future independence from the vendor.
5. All versions of all assessments must be made public before FRT deployment.
6. Public consultation should be obligatory.

7. Authorities must inform the public how probe images are used in an FRT operation.
8. The technical specifications of any FRT system must be made public before deployment.
9. Live FRT is prohibited.
10. Prior judicial authorization should be mandatory.
11. Authorities must document each retrospective or operator-initiated FRT search.
12. An FRT result alone is not a sufficient basis for questioning, arrest or detention.
13. Disclosure of the details of the FRT operation applied against individuals should be mandatory.
14. Any FRT misidentification of a person must be reported.
15. Annual reporting by authorities of misidentifications should be mandatory.
16. An independent FRT oversight body must be established before any deployment of FRT.
17. That independent FRT oversight body must publish annual reports.
18. Impact assessments must be made available to the oversight body before the system is deployed.

Use of FRT

PRINCIPLE 1: Law enforcement authorities must not use FRT, or collect, store, use or disclose personal information related to any FRT use, unless any such actions are authorized by a specific law.

This law must specify the strict circumstances under which FRT use can be authorized and be written in a manner that ensures citizens and residents can understand and foresee the exact conditions and circumstances in which FRT is deployed or will be deployed.

This law must also explicitly state that FRT should never be used to:

- Identify whistleblowers, journalists or journalistic sources;

- Identify people who have no evidentiary link, direct or indirect, to a crime;
- Categorize people by a protected characteristic or for social scoring;
- Try to infer the emotions or intentions of a person;
- Try to predict the future actions of a person;
- Identify protesters or collect information on people attending peaceful assemblies; or
- Identify people in or around polling stations.

Any FRT use must also be in full compliance, at a minimum, with the following principles:

LEGAL BASIS

PRINCIPLE 2: Any legal basis for a law enforcement authority use of FRT must include a non-delegable duty on the part of the authority to carry out a series of impact assessments with respect to all fundamental rights prior to deployment of any new use case of FRT. These assessments must include, but not be limited to, an assessment of the impact on fundamental rights and an assessment of the strict necessity and proportionality of the FRT use.

The former must identify, assess and address the adverse effects of an FRT deployment on human rights. This assessment must explicitly outline:

- The specific parameters of its use, including whether it is retrospective or operator-initiated, who will use it, who it will be used against, where it will be used, why it will be used and how it will be used;
- The rights impacted, in particular rights to privacy, protection of personal data, freedom of expression and peaceful assembly, and non-discrimination;
- The nature and extent of the risks to those rights;
- How each of those risks will be mitigated;
- A demonstrated justification for how and why the benefits of the deployment will outweigh the rights' impacts; and

- The remedy available to someone who is misidentified[108] or whose biometric data was processed when it should not have been.

Any assessment of the strict necessity and proportionality of the FRT use must detail the necessity of the deployment for a stated and legitimate objective and include:

- Evidence of the problem being addressed by the FRT deployment;
- An evidence-based explanation as to how the FRT deployment will be genuinely effective in addressing the problem; and
- A demonstration of why existing and less intrusive measures which do not include FRT will not be sufficient to meet the legitimate objective.

An authority must not deploy any new use case of FRT if an impact assessment determines that the FRT system and the demographic composition of the system's algorithm training dataset produce results biased, directly or indirectly, against any protected characteristic including race, gender or age in an operational setting.

A law enforcement authority must not deploy any new use case of FRT if it is neither strictly necessary nor proportionate.

These assessments will be carried out yearly for each FRT system after being deployed. Should an FRT system fail any such assessment after being deployed, the system will be decommissioned.

NON-EXCLUSION OF LEGAL BASIS

PRINCIPLE 3: Law enforcement authorities' Principle 2 obligations apply irrespective of explicit legal mechanisms requiring FRT system vendors to publish or disclose certain information about their algorithms and source data.

VENDOR LOCK-IN RISK ASSESSMENT

PRINCIPLE 4: Law enforcement authorities must not acquire or deploy any new FRT without a prior assessment of vendor lock-in risk, including, but not limited to:

- An evaluation of interoperability and compatibility with existing systems;

108 "Misidentification" for the purposes of these principles means the wrong selection of a person from a candidate list by a human reviewer of an FRT search which precedes a law enforcement action against that person – such as, but not limited to, being placed on a reference or database, questioned, arrested, detained or prosecuted.

- A data ownership and portability assessment, evaluating the costs of migrating data to a different vendor's system;
- A comparison of the proprietary systems, components and algorithms with the existing open alternatives, should there be any; and
- A strategy to change vendors if needed, including the foreseeable costs of such a change.

The procurement of FRT systems should favour vendor offers that maximize open standards and interoperability and minimize proprietary components.

It is the duty of the vendor to explain, in plain language, how a specific FRT system works, and the duty of law enforcement authorities to fully understand how the technology and the system work.

This assessment will be carried out yearly for each FRT system deployed. Should vendor lock-in risk rise, actions will be taken to reduce dependency on third parties, including, if needed, decommissioning the FRT system.

PUBLICATION OF RISK ASSESSMENT RESULTS

PRINCIPLE 5: All versions of all assessments, including strict necessity and proportionality assessments and human rights impact assessments,[109] carried out prior to any FRT deployment, and their results, must be made public prior to FRT deployment in a manner that maximizes public reach, especially among the people most likely to be subjected to the specific FRT use.

PUBLIC CONSULTATION

PRINCIPLE 6: Before any law enforcement authority deployment of an FRT system, the authority must hold meaningful public consultations, including members of the communities who will be disproportionately affected by FRT use. These consultations must include sharing:

- Details about how the technology and system work in an explainable and accessible manner;
- Details about the parameters of the authorities' expected use within the respective jurisdiction, including the strict conditions under which the system is used;

109 These assessments must be made in accordance with international definitions and standards.

- Details of the images used as probe images, and any devices through which they are captured;
- Details of the images featuring on all reference databases;
- Demographic data of those who are expected to be subjected to the use of the system;
- All written impact assessments required under these principles; and
- Details of the safeguards in place to prevent arbitrary use of the system.

Meaningful public consultation also requires:

- Publishing all submissions made by members of the public, experts, civil society or other actors during the consultation process;
- Allowing sufficient time for the authorities to reflect on these submissions before any decision concerning deployment is reached; and
- Putting in place mechanisms and guarantees to ensure the consultation process can influence, shape and even cancel the deployment.

PROBE IMAGE

PRINCIPLE 7: Law enforcement authorities must use the tools available to them to make public details of how probe images are used in an FRT operation in a clear, intelligible manner, online and offline, and in such a way that is accessible to everyone. These details must identify, but not be limited to:

- The criteria necessary for a person's image to become a probe image;
- The sources of probe images;
- The length of time such probe images are retained before they are destroyed;
- The legal basis for obtaining, retaining and processing probe images; and
- The contact details for the oversight body (see Principle 16) appointed to safeguard the fundamental rights of people whose images are used in an FRT search.

TECHNICAL SPECIFICATIONS AND POLICIES MADE PUBLIC

PRINCIPLE 8: Before any deployment of FRT by a law enforcement authority, the authority must make public details of the technical specifications of any FRT

system it plans to use in a clear, intelligible manner. These details must include, but not be limited to:

- A detailed description of all hardware and software components (including name and manufacturer, algorithm version number and year of development) to be used in the system. This includes servers, databases, networking equipment, cameras and any third-party software or services integrated into the system;
- A breakdown of the system into its various subsystems and modules, describing the functionality and purpose of each part. This includes both the core facial recognition algorithm and any auxiliary systems such as image preprocessing, data encryption and user interfaces;
- A visual representation of the system design and architecture, illustrating how data is collected, processed, stored and accessed. This should include the points of data entry, processing stages, data storage locations and data retrieval processes;
- The error rates for the FRT system used, including false positive and false negative rates, as well as documentation on how the error rates were calculated, including whether they reflect test (laboratory) or operational conditions reflecting the demographic make-up of where the FRT is to be deployed; and
- A list of the parameters of the reference database used, including:
    1. The legal basis and internal procedure that must be followed before adding a person to the database;
    2. The sources of database images;
    3. How many images are in the database;
    4. How the images are obtained;
    5. How long the images stored are kept in the database;
    6. How often the database is purged;
    7. The process for having images removed from the database;
    8. Who has access to the database and when / under what circumstances;
    9. How the database is maintained;

10. The identity of the person/unit who is responsible for the maintenance and oversight of the database;
11. The privacy and data protection policy for the database;
12. How the law enforcement authority will assess and demonstrate that the creation of the reference database, or the addition of a person to the reference database, is necessary and proportionate; and
13. The criteria for a person's inclusion in the reference database.

BANNED USES

PRINCIPLE 9: No FRT system will be used on live or recorded moving images or video data.[110]

PRIOR JUDICIAL AUTHORIZATION

PRINCIPLE 10: A law enforcement officer will not be permitted to use FRT unless there is prior judicial authorization for such use, except in duly justified urgent cases, whereby a higher-ranking officer, wholly independent of the investigation, must give approval. In such exceptional cases, judicial authorization must still be requested without undue delay and no later than 48 hours after use.

Any law enforcement officer carrying out a retrospective FRT search must be independent of the investigation of the offence, and any law enforcement officer using FRT must have completed training, which will be updated annually. This training must focus on how to use the relevant system, how to assess the human rights impacts of using the system, how to determine whether use is strictly necessary and proportionate and how to fully comply with the law underpinning the use of FRT.

RECORD OF USE

PRINCIPLE 11: Law enforcement authorities must document each retrospective or operator-initiated FRT search performed and provide this documentation to the oversight body every quarter. This documentation will include the following.

---

110 As an example of situations covered by this principle, see Scenario 3, page 43 of the EDPB *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* and Section 307.5 - 3.2 of the Detroit Police Department's (DPD) 2024 manual regarding their use of FRT, which prohibits the use of FRT on live streaming or recorded videos. It states: "Members shall not use Facial Recognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source."

- For retrospective FRT use, a copy of any written request made for an FRT search must include:
    - The date and time of the request;
    - The name and position of the requesting individual officer and the law enforcement unit they are attached to;
    - Details of how the request was necessary and proportionate;
    - The reason for the request, including, but not limited to, any underlying suspected crime;
    - The name of the judicial authority to whom the request was made and, in exceptionally urgent circumstances, the name of the higher-ranking officer who gave the temporary authorization;
    - The outcome of the request; and
    - If the request was granted, the composition/make-up of the reference database searched.
- For retrospective *and* operator-initiated FRT use, the documentation must include:
    - The outcome of each search, the number of candidates returned in each search and all actions taken by the law enforcement authority subsequent to each search;
    - The name and position of the individual officer who carried out the search; and
    - Aggregate information on the use of FRT, including:
    - The total number of FRT search requests;
    - The total number of FRT search requests that generated leads;
    - The number of FRT searches whereby an arrest or charges followed;
    - The number of FRT misidentifications;111
    - The number of individuals who appeared as a possible match in the FRT search and who were subsequently questioned, arrested and/or charged;

111 As defined in the footnote to Principle 2.

- The demographic breakdown of individuals in probe photos by race and gender; and
- Information about the FRT system and algorithm(s) used, including vendor, version, similarity threshold and whether the similarity threshold was adjusted for the specific search.

In addition to the above, every database of images used by a law enforcement authority for an FRT search must be audited at least annually to ensure that it does not contain images that are no longer legally permitted to be retained, that it does not contain wrong information and that it is not being accessed or used inappropriately or unlawfully. These audits must also be provided to the oversight body.

Any other information requested by the oversight body to fulfil their legal obligations must be provided in a reasonable time.

PROHIBITION OF ACTION

PRINCIPLE 12: A law enforcement officer will not question, arrest, detain or take any action against an individual on the basis of FRT use alone. Use of FRT will not result in a person being included in a photographic or physical line-up. Law enforcement officers are also prohibited from taking action based solely on the combination of an FRT lead and a witness or confirmatory identification procedure, such as a photographic or physical line-up. An FRT result is an investigative lead only. It is not reliable evidence, and any FRT result must be followed by independent reliable investigative actions before a law enforcement officer can take any action.

OBLIGATION TO DISCLOSE

PRINCIPLE 13: Law enforcement authorities must disclose to persons detained, questioned, arrested, charged or prosecuted subsequent to a use of FRT and their legal representative (if any), without restriction, details of the FRT operation applied to them and the technical specifications of the system involved in the investigation or procedure applied. These must include all of the details listed in Principle 8 and:

- The source code for each algorithm used;
- The data used for training and fine-tuning the system;

- A list of what measurements, nodal points or other unique identifying marks are used by the system in creating facial feature vectors including, if those marks are weighted differently, the scores given to each respective mark;
- Access to a test environment with an executable version of the software;
- The original copy of the probe image used;
- Any/all information associated with the probe image, including metadata, that was in the possession of, or made available to, the person conducting the FRT search;
- Details of the FRT system's threshold value fixed by the manufacturer (and by the law enforcement authority if they change the value) to determine when the respective software indicates that a potential match has occurred; and
- Specifically in the case of retrospective FRT use:
    - Any/all edited copies of the probe image used noting, if applicable, which edited copy produced the candidate list that included the defendant, and a list of edits, filters or any other modifications made to that image;
    - A copy of the database image matched to the probe image and the rank number and similarity scores assigned to the image by the FRT system in the candidate list;
    - A list or description of the rank number and similarity scores produced by the FRT system, including the scale on which the system is based;
    - A copy of the complete candidate list returned by the FRT system, in rank order and including the similarity score assigned to each image by the FRT system;
    - The written report produced by the person who ran the FRT search, including the date, time of the search and any notes made about the possible match relative to any other individuals on the candidate list; and
    - The name and training, certifications or qualifications of the person who ran the probe image in an FRT search.

REPORT OF MISIDENTIFICATION

PRINCIPLE 14: Any FRT misidentification[112] of a person must be reported to the person by the law enforcement authority as soon as possible after the misidentification is discovered and recorded.

ANNUAL REPORTING ON MISIDENTIFICATIONS

PRINCIPLE 15: Law enforcement authorities that use FRT must produce an annual report outlining anonymized statistics pertaining to misidentifications. These reports must include the nature, source and impact of the error and any steps taken by the law enforcement authority in response to the misidentifications regarding use of the FRT system, the operators using the FRT system and the procedures and protocols regarding FRT use. These reports must be made public and provided to the oversight body described in Principle 16.

INDEPENDENT OVERSIGHT BODY

PRINCIPLE 16: An independent FRT oversight body must be established before any deployment of FRT by a law enforcement authority to assess the use of FRT and its compliance, or otherwise, with fundamental rights, the applicable regulation and these principles. This body must:

- Be established and regulated by law;
- Be separate to, and independent of, the executive authority or respective state;
- Have the necessary funds, skills, expertise and staff – legal and technological – to fulfil its responsibilities;
- Have free and immediate access to the necessary information it needs to carry out its work;
- Report annually to the public about its work and findings; and
- Report annually to the country's parliament.

The oversight body will be provided with the expertise and resources to develop an evaluation methodology for its assessment of the use of FRT and compliance, or otherwise, with fundamental rights, applicable regulations and these principles. This evaluation methodology must include the minimum set of requirements that the FRT system must meet, below which the system must be decommissioned.

112 As defined in the footnote to Principle 2.

The oversight body will have the power to order decommissioning when the minimum set of requirements are not met.

ANNUAL REPORT BY INDEPENDENT OVERSIGHT BODY

PRINCIPLE 17: The independent FRT oversight body described in Principle 16 will publish annual reports which will include all of the written assessments mentioned in these principles and:

- A detailed assessment of, and comment on, law enforcement's stated legal basis for the use of FRT;
- The number of individual probe images used in FRT searches;
- The number of images used in reference and databases;
- The number of true matches and false positives per deployment;
- The number of arrests per deployment;
- The number of stop and searches per deployment;
- The total number of FRT use requests made;
- The total number of FRT deployments;
- The number of requests made or searches performed pursuant to judicial authorization;
- The number of emergency requests made or deployments performed; and
- The reasons for requesting the search, including, but not limited to, any underlying suspected crime.

PRIOR NOTIFICATION OF IMPACT ASSESSMENTS TO OVERSIGHT BODY

PRINCIPLE 18: In addition to Principle 5, the details and findings of each impact assessment, as described in Principles 2 and 3, must be made available to the oversight body before the system is deployed to assess and evaluate the law enforcement authority's findings.

How to use these principles

As demonstrated by this report, the pervasive deployment of FRT systems by police has a negative impact on the lives and fundamental rights of those under the surveillance of these technologies. The risks and harms are significant while, in the absence of legal frameworks providing for accountability and transparency, the seeking or obtaining of redress for those harms is very difficult. Worse, in cases where people are utterly unaware that FRT is being used against them, any such access to redress is near impossible.

In the face of the ever-expanding use of FRT by police forces across the world, the aim of this report and the principles is to both help reduce those harms and empower civil society and the general population with a clear understanding of these technologies. We hope they can use this information to voice their opposition to the deployment of FRT in their respective states.

To achieve these goals, we believe the principles can be used in the following four ways:

1. This document can be used as an **advocacy tool when debating and discussing FRT with law and policy makers**. Our principles encompass the entire spectrum of deploying an FRT system, from establishing the legal foundation that permits its use to the practical implementation of FRT by law enforcement. Principles such as 1, 2, 6 and 12 address critical high-

level safeguards that should be embedded in any legislation regulating FRT. These bare minimum legal provisions are built on the principles of transparency, public participation and access to remedy that are part of the basic consensus of democratic regimes. The principles also provide detailed requirements beyond basic regulations, covering development guidelines and public policies. For example, Principle 4 details what an assessment which aims to reduce vendor lock-in should include. Another example is Principle 13, which details the information that should be disclosed to persons detained or prosecuted subsequent to a use of FRT.

2. Beyond law and policy making, we hope this document serves as a tool when engaging **police forces as they define their protocols and procedures for FRT use**. A key concern is the interaction between an FRT system, its users within a police force and the effects on an investigation or prosecution, which leads to potential harm. For this reason, we have included principles, such as Principle 11, that detail the documentation that should be produced when using these systems, as records of use to facilitate accountability.

3. The principles are rooted in international human rights standards and judgments, reflecting the idea that they naturally safeguard the fundamental rights essential to democracies. For that reason, we think these principles may be of use **before courts when building cases against the harms produced by FRT systems**. These principles serve as a tool to challenge the use of FRT when laws either include provisions that violate fundamental rights or lack specific regulations for FRT deployment.

4. Finally, we accompany the principles with a review and explanation of the harms, risks and fundamental rights impacted by the deployment of FRT by police. We list, in detail, the kinds of questions that must be asked of authorities intent on using FRT. We hope that this information will help ensure that any **advocacy or campaign initiative** is grounded in a clear understanding of the issues. We hope this will empower civil society to voice their concerns in an accessible manner to members of the public who, together with civil society, can build and develop campaigns against the use of FRT.

These are some of the uses we hope this report and principles will serve. The matters covered by these principles are not the only considerations that could be taken when debating the use of FRT systems; indeed, as the systems become more sophisticated, new considerations will emerge. However, we hope that, after

reading this document, readers are better informed of the risks associated with FRT and more convinced that, when used by police forces, there is scant evidence that FRT improves our lives and, on the contrary, much to indicate a high likelihood of harm.

Closing words

The authors of and contributors to this guidebook believe that the best use of FRT is that it not be used by police at all. As exhaustively explained throughout this guidebook, the risks and potential harms associated with using FRT systems outweigh any possible benefits. The substantial costs – to both individual privacy and societal trust – make its deployment in the policing context **unjustifiable**.

Acknowledgements

This project was developed, drafted and edited by Olga Cronin (INCLO/ICCL), Víctor Práxedes Saavedra Rionda (INCLO), Elizabeth Farries (University College Dublin Centre for Digital Policy), Kirill Koroteev (Agora), and Timilehin Ojo (INCLO/CCLA).

This is a collaborative effort by 15 INCLO member organizations. For their contributions towards the development, case study, drafting, editing and research, INCLO sincerely thanks: Myriam Selhi, Lucila Santos (INCLO), Vanessa Lopez (Dejusticia), Sherylle Dass (LRC), Devon Turner (LRC), Manuel Tufró (CELS), Ben Wizner (ACLU), Kieran Pender (HRLC), David Mejia-Canales (HRLC), Martin Mavenjina (KHRC), Gil Gan-Mor (ACRI), Anaïs Bussières McNicoll (CCLA), Karim Medhat Ennarah (EIPR), Sehba Meenai (HRLN), Remport Ádám (TASZ), Nadine Sherani (KontraS), Emmanuelle Andrews (Liberty), Nathan Freed Wessler (ACLU), Jun Pang (Liberty), Daniel Konikoff (CCLA) and Daniel Ospina Celis (Dejusticia).

INCLO credits Designed For Good's Taryn McKay for design, Sam Kelly for edits and Alina Najlis for illustrations.