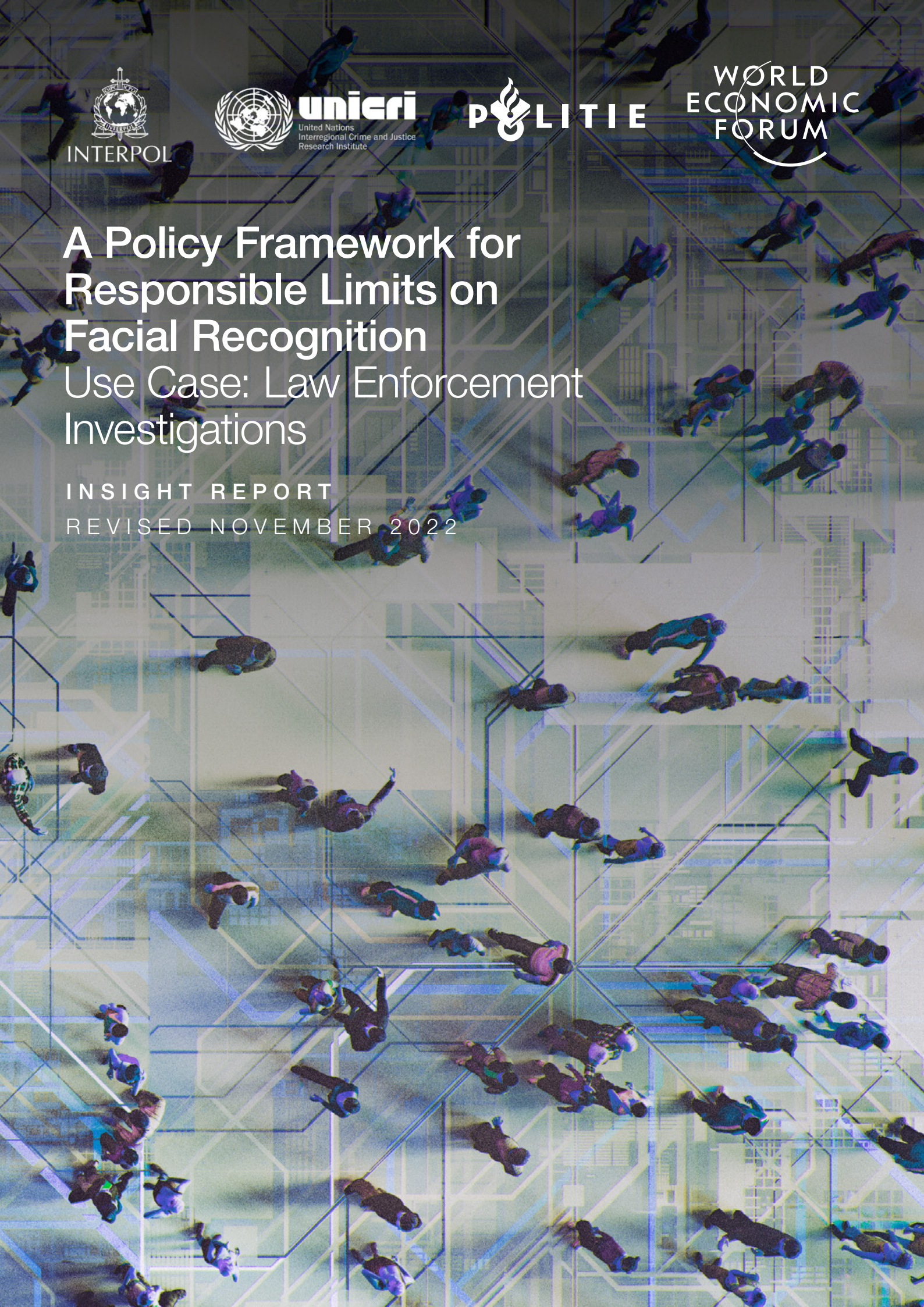


INTERPOL

unicri
United Nations
Interregional Crime and Justice
Research Institute

POLITIE

WORLD ECONOMIC FORUM

A Policy Framework for Responsible Limits on Facial Recognition

Use Case: Law Enforcement Investigations

INSIGHT REPORT

REVISED NOVEMBER 2022

With particular thanks and appreciation to:

Images: Getty Images, Unsplash

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

© 2022 World Economic Forum, UNICRI, INTERPOL and Netherlands Police. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Foreword

Irakli Beridze
Head of the Centre for Artificial Intelligence and Robotics, UNICRI

Marjolein Smit-Arnold Bik
Head of the Special Operations Division, Netherlands Police

Kay Firth-Butterfield
Head of Artificial Intelligence and Machine Learning; Member of the Executive Committee, World Economic Forum

Cyril Gout
Director of Operational Support and Analysis, INTERPOL

Remote biometric technologies – in particular, facial recognition – have gained a lot of traction in the security sector in recent years. The accuracy of these technologies has significantly increased with advancements in deep learning algorithms, growing access to huge volumes of training data and the pressure to reduce bias to negligible values.

The advent of this technology comes at a time when law enforcement agencies are increasingly expected to resolve ever more complex and often transnational crimes and conduct their investigations expeditiously – often with limited resources. In a field in which underperformance can be a matter of life or death, tools such as facial recognition technology can greatly benefit law enforcement investigations. But, improperly implemented or implemented without due consideration for its ramifications, facial recognition technology (FRT) could result in major abuses of human rights and cause harm to citizens, particularly those in underserved communities.

Undoubtedly, the rapid adoption of FRT has raised multiple concerns, mainly related to the possibility of its potential to undermine freedoms and the right to privacy. In parallel with this, there has been a growing emphasis on putting policies in place to address and mitigate these risks.

With the creation of this paper, the World Economic Forum, the International Criminal Police Organization (INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the Netherlands Police have built a global alliance to tackle this challenge and bring the issue of responsible use of FRT in law enforcement investigations to the international agenda. We have also engaged with a community of experts composed of governments, civil society and academia to collect their insights through a consultative process and have piloted our proposed framework with law enforcement agencies to ensure that what we propose can truly work in an operational law enforcement context. And it does.

This insight report presents a set of proposed principles for the use of facial recognition in law enforcement investigations along with a self-assessment questionnaire intended to support law enforcement agencies to design policies surrounding the use of FRT and to review existing policies in line with the proposed principles.

This is only the beginning of the conversation on law enforcement's use of FRT, but we are confident that this unique proposed approach can be an important contribution to the law enforcement community and help to inform public debate all across the globe. We encourage law enforcement agencies and policy-makers at the national level to reflect on this paper, to participate in a dialogue on the basis of it and to review or adopt legislation that supports the responsible use of facial recognition technology.

Introduction

Over the past decade, progress in artificial intelligence (AI) and sensors has fuelled the development of facial recognition technology (FRT) – software capable of matching a human face from a digital image or a video frame against a database of facial images. This has led to its rapid adoption in various industries, including law enforcement, transportation, healthcare and banking.

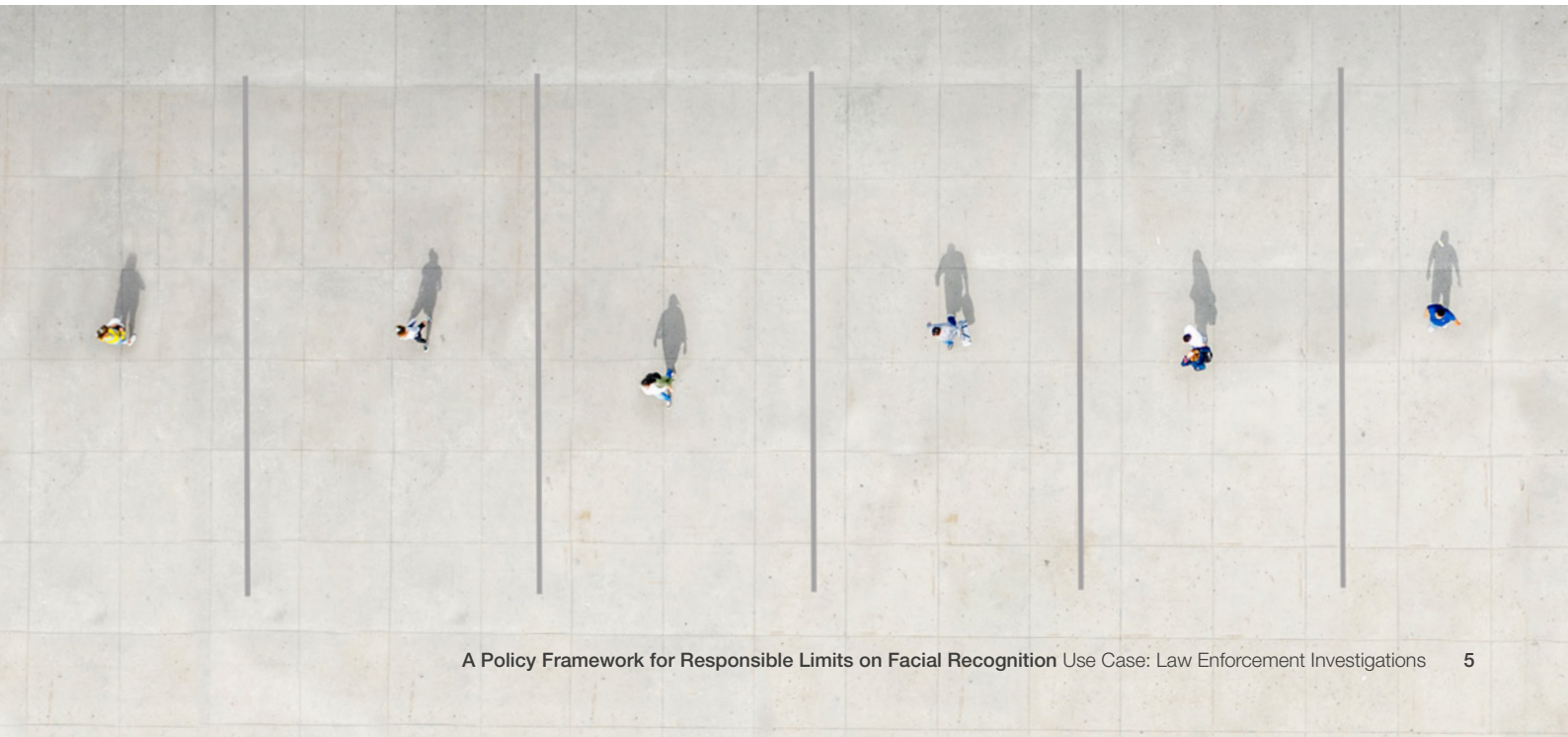
The development of FRT presents considerable opportunities for socially beneficial uses. For instance, it can find application in face-unlock mechanisms in mobile devices, in granting access to concerts and sporting events, and in attendance-tracking for employees and students. But it also creates unique challenges. To fully grasp these challenges and the trade-offs they may entail and to build appropriate governance processes, it is necessary to approach FRT deployment by examining specific applications. Indeed, passing through an airport border control with face identification, using face-based advertising in retail or employing facial recognition solutions for law enforcement investigations involves very different benefits and risks.

To ensure the trustworthy and safe deployment of this technology across domains, the World Economic Forum has spearheaded a global and multistakeholder policy initiative to design robust governance frameworks. The Forum launched the first workstream in April 2019, focusing on flow management applications[1] – replacing tickets with facial recognition to access physical premises or public transport, such as train platforms or airports. This workstream was concluded in December 2020 with the release of a tested assessment questionnaire by Tokyo-Narita Airport, an audit framework and a certification scheme co-designed with AFNOR Certification (Association Française de Normalisation).[2]

In November 2020, the second workstream was launched, focused on the law enforcement context – *supporting the identification of a person by comparing a probe image to one or multiple reference databases to advance a police investigation*. While law enforcement has been using biometric data, such as fingerprints or DNA, to conduct investigations, FRT is a new opportunity and challenge for law enforcement.

In terms of challenges, use by law enforcement raises multiple public concerns, primarily because of the potentially devastating effects of system errors or misuses in this domain. A study conducted in 2019 by the National Institute of Standards and Technology (NIST) showed that, although some facial recognition algorithms had "undetectable" differences in terms of accuracy across racial groups, others exhibit performance deficiencies based on demographic characteristics such as gender and race.[3] Law enforcement agencies should be aware of these potential performance deficiencies and implement appropriate governance processes to mitigate them. In doing so, they would limit the risk of false positives or false negatives and possible wrongful arrests of individuals based on outputs from an FRT system. Failure to build in such processes could have dramatic consequences. For example, in 2018 in the United States, an innocent African American man was arrested and held in custody as a result of being falsely identified as a suspect in a theft investigation in which FRT was used.[4] In addition to hampering rights such as the presumption of innocence, and the right to a fair trial and due process, the use of FRT by law enforcement agencies can also undermine freedom of expression, freedom of assembly and association, and the right to privacy.[5]

"While law enforcement has been using biometric data, such as fingerprints or DNA, to conduct investigations, FRT is a new opportunity and challenge for law enforcement.



These concerns have led to intensified policy activity globally. In the US alone, some local and state governments have banned the use of FRT by public agencies, including law enforcement. Major cities such as San Francisco,[6] Oakland[7] and Boston[8] have adopted such measures. At the state level, Alabama,[9] Colorado,[10] Maine,[11] Massachusetts,[12] Virginia[13] and Washington[14] have all introduced legislation to regulate its use. Finally, at the federal level, various bills[15] – including most recently the Facial Recognition Act of 2022, introduced in September 2022[16] – have been proposed to regulate FRT but none of them has been adopted to this date.

Furthermore, large US technology companies have also formulated positions on this topic. In the wake of a series of events in 2020 that increased distrust toward police agencies in the US and worldwide, including the Clearview AI controversy,[17] IBM announced that it will no longer offer, develop or research FRT, while Microsoft pledged to stop selling FRT to law enforcement agencies in the US until federal regulation was introduced.[18] In 2022, Microsoft went further, putting new limits and safeguards on all uses of FRT as part of a broader set of AI principles.[19] In 2021, Amazon Web Services (AWS) also extended its moratorium on police use of its platform Rekognition, which it originally imposed in 2020.[20]

In other jurisdictions, policy-makers are attempting to limit police use of FRT to very specific use cases associated with robust accountability mechanisms to prevent potential errors that may lead to wrongful arrests. That is the direction proposed by the European Commission, which in 2021 released its draft of an Artificial Intelligence Act[21] – a comprehensive regulatory proposal that classifies AI applications under four distinct categories of risk subject to specific requirements.[22] This proposal includes provisions on remote biometric systems, which include FRT. It states that *AI systems intended to be used for the "real-time" and "post" remote biometric identification of natural persons* represent high-risk applications and would require an *ex ante* conformity assessment of tech providers before getting access to the European Union market and an *ex post* conformity assessment while their systems are in operation. Moreover, *"real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement* are prohibited unless they serve very limited exceptions related to public safety (e.g. the prevention of imminent terrorist threats or a targeted search for missing persons). In order to enter into force, however, the European Commission's proposal will first need to be adopted by the European Union parliament and the Council of the European Union.

At the United Nations, a similar approach is emerging, with the Office of the High Commissioner for Human Rights (OHCHR) presenting a report[23] in 2021 to the Human Rights Council on the right to privacy in the digital age, in which it recommends banning AI applications that cannot be used in compliance with international human rights law. With specific respect to the use of FRT by law enforcement, national security, criminal justice and border management, the report stated that *remote biometric recognition dramatically increases the ability of State authorities to systematically*

In addition to providing practical guidance and support to law enforcement and policy-makers, this governance framework seeks to inform public debate on the use of FRT.

identify and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement. The report also reiterates calls for a moratorium on the use of remote biometric recognition in public spaces, at least until authorities can demonstrate that there are no significant issues with accuracy or discriminatory impacts, and that these AI systems comply with robust privacy and data protection standards.

Courts have also started to play an important role in shaping the policy agenda on FRT. In 2021, the São Paulo Court of Justice in Brazil blocked[24] the deployment of FRT in the public transport system. This was perceived as a major victory by civil rights organizations that oppose the increasing use of FRT by public agencies. In a similar case in the UK, while the Court of Appeal found that the deployment of automated FRT by the police did have a legal basis for use in common law, its use by the South Wales Police at certain events and public locations was unlawful because it did not sufficiently define who could be on a watch list and where it could be used.[25]

In some countries, governments have adopted a cautious approach. That has been the case in the Netherlands. In 2019, the Minister of Justice and Security addressed a letter to members of parliament informing them about the existing uses of FRT by law enforcement agencies and reaffirming his support for robust governance processes in relation to this sensitive technology.[26] Further, he argued that the existing legal framework and safeguards, both technical and organizational, are sufficiently robust to ensure the responsible use of FRT by law enforcement agencies. Nevertheless, he requested additional privacy, ethical and human rights impact assessments before authorizing any further uses or pilots of FRT.

Despite these developments, most governments around the world continue to grapple with the challenges presented by FRT. The ambition of this work is thus to strengthen their efforts to overcome them, and support law- and policy-makers across the globe in designing an actionable governance framework that addresses the key policy considerations raised, such as *the necessity of a specific purpose, the performance assessment of authorized solutions, the procurement processes for law enforcement agencies, the training of professionals and the maintenance of the chain of command for emergency situations*.

To achieve this, the World Economic Forum, the International Criminal Police Organization (INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the Netherlands Police convened a multistakeholder community centred on co-designing a set of principles that outline what constitutes the responsible use of FRT for law enforcement investigations. These principles are accompanied by a self-assessment questionnaire to support law enforcement agencies to design policies surrounding the use of FRT and to review existing policies in line with the proposed principles.

In addition to providing practical guidance and support to law enforcement and policy-makers, this governance framework seeks to inform public debate on the use of FRT at the national, regional and international levels and provide an actionable framework to maximize the benefits of FRT while mitigating its risks.

While the policy framework proposed in this paper is not the only such policy guidance in this domain, it seeks to present a unique proposal built with an international perspective, incorporating a multistakeholder approach, including law enforcement, industry and civil society, in its development.

Methodology

For the past three years, the artificial intelligence/machine learning (AI/ML) platform of the World Economic Forum has been conducting a policy initiative on the governance of FRT. The objective of this initiative is to create an appropriate space for conversation to advance the drafting of policies related to the use of this biometric technology. The methodology, in essence, consists of a core community of partners and an extended global community of experts co-leading the development of a pilot project. This pilot-based approach to policy-making has been adopted as it is considered to have the potential to better inform and guide law enforcement users and policy-makers seeking to ensure the appropriate governance of FRT.

A multistakeholder approach based on a core community and a project community

A total of 64 individuals participated in this project community, representing technology companies, governmental and international organizations, civil society and academia.

The initiative brought the World Economic Forum together with INTERPOL and the Netherlands Police – both users of FRT – and UNICRI, a United Nations entity mandated to support United Nations Member States in formulating and implementing improved policies in the fields of crime prevention and criminal justice. With the objective of proposing a policy framework, this core community gathered virtually on a weekly basis between January 2021 and October 2022.

The core community additionally organized consultations with an extended group of stakeholders – the project community – to further benefit from broader expertise and insights. A total of 64 individuals participated in this project community, representing technology companies, governmental and international organizations, civil society and academia.

The first consultation with the project community was a workshop, organized in February 2021, which kicked off the project and sought to gain insights regarding the risks related to the use of FRT by law enforcement and the potential solutions to mitigate them. The second consultation was a request for comments on the draft of the principles for the responsible use of FRT for law enforcement investigations. The project community was allocated a month to share any comments on the proposal. Following this, four expert interviews were organized to gather additional insights. In total, 10 organizations and experts from the project community shared comments on the draft, which the core community incorporated into a revised draft of the principles.

The whole project was conducted under the Chatham House Rule, whereby participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.[27]

A policy framework composed of principles and a self-assessment questionnaire

This policy framework comprises two elements:

The principles, and their corresponding actions, which aim to define what constitutes the responsible use of FRT in law enforcement investigations. This list of nine principles was drafted by the core community composed of INTERPOL, UNICRI, the Netherlands Police and the World Economic Forum.

The self-assessment questionnaire, which complements the principles and is intended to support practitioners in the law enforcement community in effectively implementing these proposed principles. Law enforcement agencies already using FRT are encouraged to use the questionnaire to review their existing processes and assess the alignment of their approach with the proposed principles. The self-assessment questionnaire can also be used by agencies that do not currently have FRT in operation but which have the ambition to develop the capability. In this regard, it can be used as a guide to help them reflect upon the necessary steps to develop their capabilities responsibly and review their processes as they develop them.

Piloting to test and improve the policy framework

In October 2021, the first draft of the policy framework was publicly released, bringing the initial developmental phase of the project to a conclusion. The next phase of the project was launched in January 2022, focusing on piloting the policy framework. The pilot was intended to collect feedback from the pilot members in order to review and validate the utility and completeness of the principles and the self-assessment questionnaire, assessing it as a system and tool for law enforcement to ensure the trustworthy and safe deployment of FRT. Feedback from participating agencies on their overall compliance with the principles was not sought as it was outside the scope of the exercise. To this end, a series of three pilot meetings were convened as part of the pilot and pilot agencies were allocated four months to complete the self-assessment questionnaire and provide feedback on the policy framework.

A total of six law enforcement agencies from five countries participated in the project, namely, the:

- Brazilian Federal Police
- Central Directorate of the Judicial Police, France
- National Gendarmerie, France
- Netherlands Police
- New Zealand Police
- Swedish Police Authority

With the exception of the Brazilian Federal Police, each of the pilot agencies possesses operational FRT capabilities. The Brazilian Federal Police has implemented several FRT pilots, and operational capabilities are foreseen in the near future.

1 Law enforcement investigations: use cases and definitions

A description of how facial recognition technology is used in practice by law enforcement agencies.

FRT has many potential applications or use cases in law enforcement investigations, some of which will be touched upon in the sections that follow. These descriptions are intended to provide a better understanding of how FRT is or can be used by law enforcement agencies and to help illustrate the challenges that the governance framework seeks to address.

The different examples presented have been informed by the practices of the Netherlands Police and INTERPOL. It is important to note that specific practices may vary from jurisdiction to jurisdiction, and that the use cases described do not refer to any specific laws, policies, principles or recommendations that would limit or regulate their use and are intended solely for illustrative purposes.

BOX 1

The roles of the Netherlands Police and INTERPOL

The Netherlands Police and INTERPOL are entities with two distinct mandates. As a national law enforcement body, the Netherlands Police has the mandate to conduct investigations and is required to testify and report the outcome of its expertise before a judge in court. INTERPOL's mandate, on the other hand, is, *inter alia*, to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights. To do so, INTERPOL manages databases accessible to its 195 member countries. INTERPOL also provides recommendations on best practices, forensic expertise and other specialized expertise, produces analysis, delivers training activities and provides operational support to its member countries.

How facial recognition is used for law enforcement investigations

Unlike fingerprints and DNA, faces change significantly over time and can even differ from one day to the next. For instance, ageing, cosmetics, plastic surgery, the effects of drug abuse or smoking, and the way the subject poses can all influence facial appearance. This is one reason why the result of using FRT is always considered an *investigative lead*, meaning that, at most, the subject proposed by the system remains a *possible match* and a *potential candidate* only – even after a manual face comparison review by face experts.

FRT can be used for what are referred to in practice as biometric "identification" and "verification". Again, it should be emphasized that, notwithstanding this terminology, in the context of law enforcement the result of an FRT search remains an investigative lead and the system does not *per se* "identify" any individual. "Identification" (also referred to as "one to many") consists of searching for the identity of a person, whereas the activity of "verification" (also referred as "one to one") consists of verifying someone's identity against an identity document (ID).[28]

In addition to the distinction between biometric identification and verification, a further distinction can be drawn between what is referred to as "real-time" or "post-event" facial recognition. So-called "real-time" facial recognition involves the use of live or near-live material, such as video feed, generated by a camera (real-time passive capture) or footage captured by an officer using a mobile device (real-time active capture). The comparison and identification occur concurrently with the capturing of the biometric data. By contrast, with post-event facial recognition, the comparison and identification occur significantly after the biometric data has been collected.

Facial experts play a central role in the use of FRT systems and can be classified as *facial examiners*, *reviewers* or *assessors*. *Facial assessors* perform the least rigorous of facial comparison processes, carrying out only quick comparisons of image-to-image or image-to-person in screening and access control applications or field operations. *Facial reviewers* conduct comparisons of image(s)-to-image(s), generally resulting from the adjudication of a candidate list generated by FRT. *Facial examiners* are experts who perform an analysis of image(s)-to-image(s) using a rigorous morphological comparison and evaluation of images for the purpose of effecting a conclusion. In the case of the Netherlands Police and INTERPOL, for instance, the facial recognition search and comparison is performed by facial examiners who operate autonomously from the investigation teams; they do not have knowledge of the prosecution that requires them to run facial recognition analysis.[29]

To identify an unknown person of interest, investigators work with probe images and reference databases:

Probe image

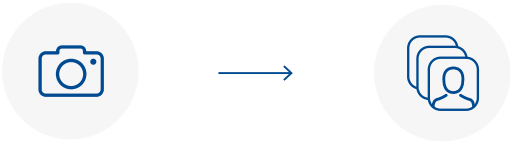
Probe images are facial photos of suspects or persons of interest that are part of the law enforcement investigation and are submitted to an FRT system to be compared to a database. Once a probe image is enrolled into an FRT system, a biometric template – a mathematical representation of the features or characteristics from the source image – is generated for subsequent processing by the system. To collect probe images, investigators (or digital/face experts) either already have an image of the suspect or they extract it from footage of videos/stills. In either case, they will seek to collect the best-quality image to ultimately improve the chance of identifying the person.

A probe image is collected from an image source

The probe image is compared against a reference database

Reference database of known criminals, suspects and missing persons

Reference databases are repositories of images to which law enforcement agencies have lawful access and against which a probe image is compared. In law enforcement investigations, it is common for the reference database used to be a database of known suspects and convicts, composed of mugshots lawfully collected and stored by the law enforcement agencies. People in such databases are still suspects or have usually been convicted of a crime.



A reference database of known criminals, suspects and missing persons has been built over time by law enforcement

A probe image is compared against this reference database to check if the person is among known criminals, suspects and missing persons

Reference database built specifically for an investigation

Alternatively, a special database can be built specifically for an investigation. In this case, the public prosecutor would authorize the seizure of video footage from a crime scene. Such a database can then be compiled from multiple sources (CCTV, social media, electronic devices, etc.), and all of the faces detected on the footage will be stored within it. The probe image of, for instance, a possible suspect can then be searched against the special database to see if the suspect is present on the footage. At the end of the investigation, the database will be removed from the operational system and stored for accountability purposes, and in the event that the file may need to be produced in court as evidence during a judicial procedure.

Face images from the investigation are collected to create a special reference database

An image of a known criminal, suspect or missing person can be searched against the special reference database

“After the search, the facial examiners analyse the list of candidate images proposed by the software.

The following process for using FRT for law enforcement investigations is based on the practices followed by the Netherlands Police – other law enforcement agencies may follow slightly different processes, but the key principles will generally be the same:

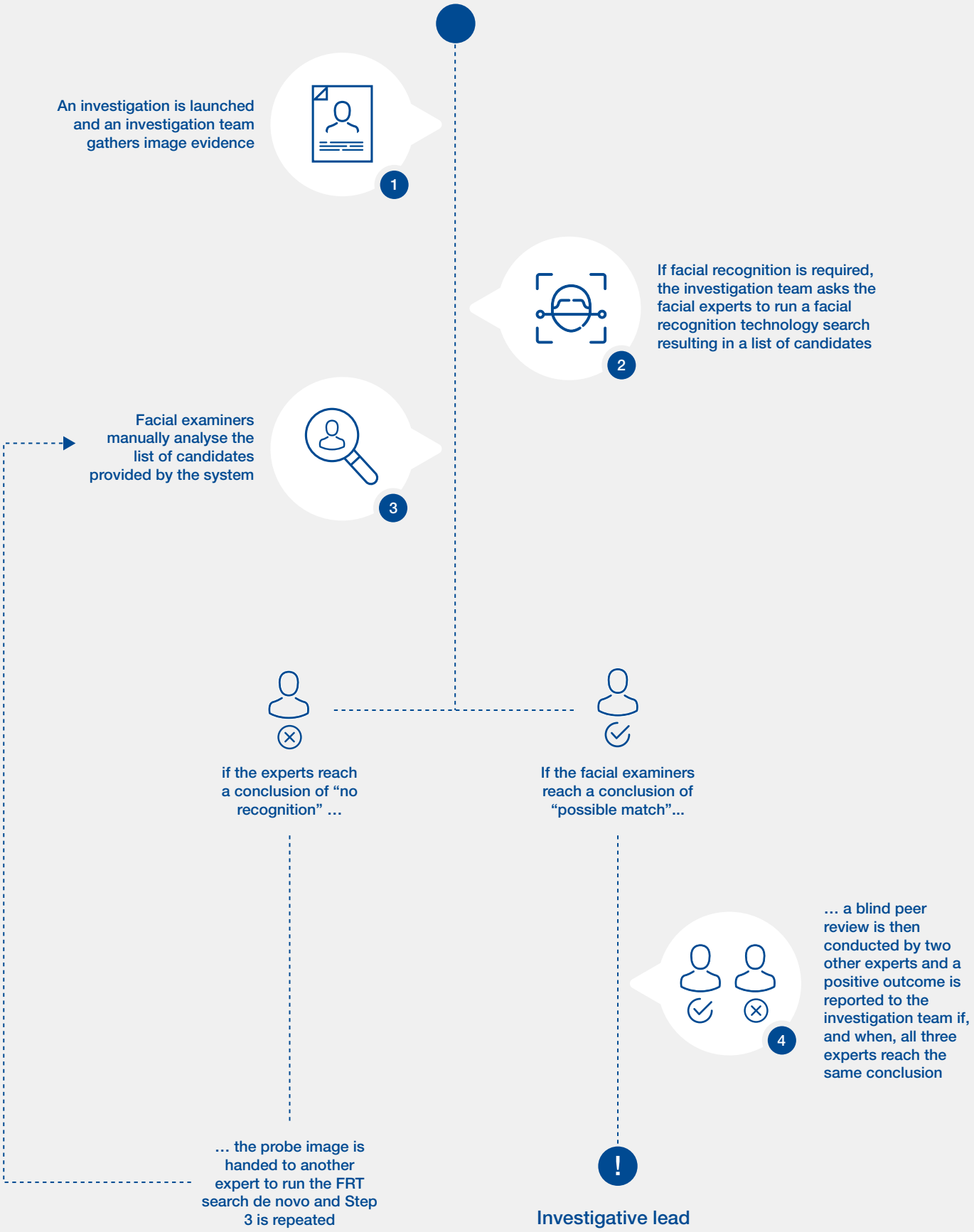
- **Step 1:** A (possible) crime is reported or suspected. An investigation team under the supervision of the public prosecutor is created and, if required by local legislation, requests warrants to collect images relevant to the crime, including images of the suspect(s). If suspects are detected on the images, the team will try to determine their identity. This can be done by human means – through recognition by people who know the suspects; for instance, police officers or witnesses – or by requesting an FRT search.

- **Step 2:** If an FRT search is requested by the investigation team, a facial examination team will run FRT software to compare the probe image against one or multiple databases. Before doing so, the facial examiners will first manually assess the quality of the probe image. If it is deemed suitable for an FRT search, they will enter the probe into the FRT system and allow the system to do the pre-search analysis and may also provide some notable facial landmarks (centre of the eye socket, etc.) to the software. The examiners will then set up the FRT software at a setting that is not too narrow – to avoid false negatives, which could lead to missing the suspect – nor too wide – to avoid false positives, which would result in a list of candidates too large to be of use.

- **Step 3:** After the search, the facial examiners analyse the list of candidate images proposed by the software. They will run this last operation manually, deploying their expertise to check if one of the images proposed by the system could be a possible match for the probe image. In order to avoid bias, the facial examiners should not be made aware of the background to the case. The outcomes of this step will be either a determination of a “possible match” or “no recognition” recorded, with a note of: 1) dissimilarities observed; 2) some similarities observed; 3) many similarities observed; or 4) some similarities and some dissimilarities observed, leading to an inconclusive determination.

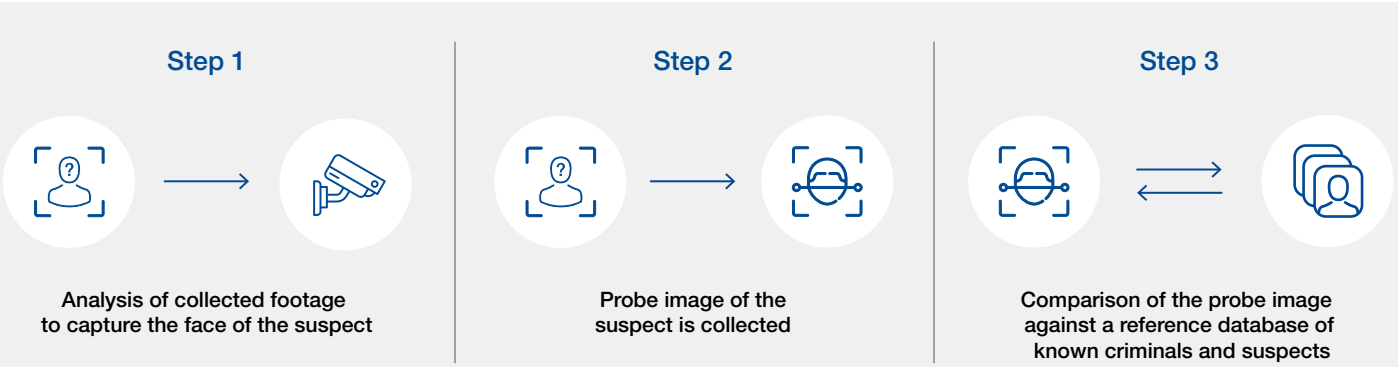
- **Step 4:** If the facial examiners confirm the conclusion of a “possible match”, the probe image and the image of the potential candidate from the reference database are handed to two facial experts for a blind peer review.[30] During the blind peer review, the facial experts, independently of each other, perform a full analysis of the probe and the reference image to determine the similarity/dissimilarity of the two faces. The end result to be reported to the investigation team is the final conclusion reached by consensus or, in the event of a lack of consensus, the most conservative conclusion in terms of similarities observed will prevail. On the other hand, if the facial examiners in Step 3 reach a conclusion of “no recognition”, the probe image is handed to one other expert to run the entire search *de novo* in order to reduce the risk of false negatives. If the *de novo* search results in a “possible match”, a blind peer review by two other facial experts will additionally be carried out as described above. Following the communication of the final result, the investigation team will proceed to review the results of the search, seeking to corroborate or disregard the proposed candidates.

The four-step process followed by the Netherlands Police when using facial recognition technology



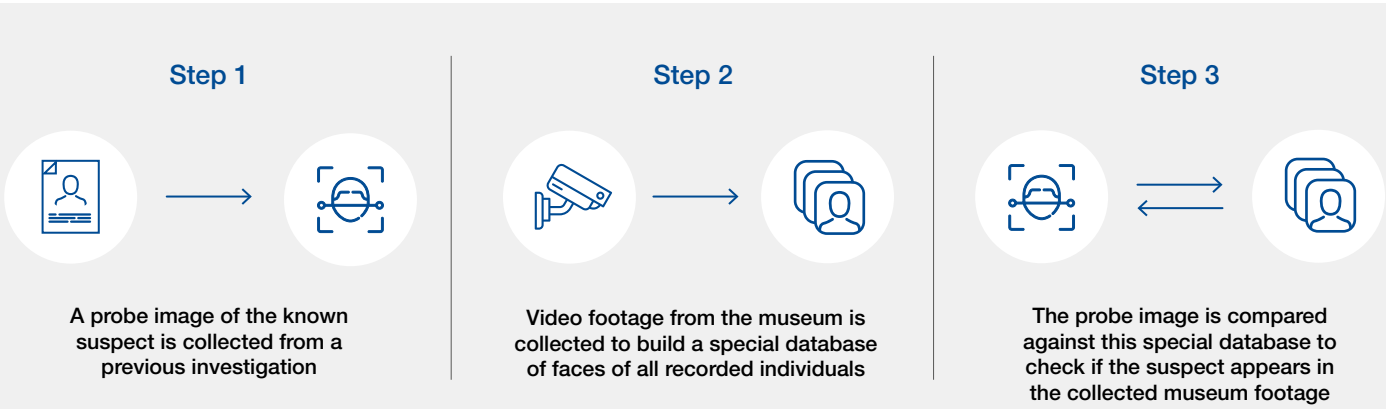
The following is a collection of scenarios intended to illustrate how FRT can be used for law enforcement investigations:

Finding the identity of an ATM fraud criminal
Fraudulently obtaining bank account data by usurping an individual's identity can enable an unauthorized person to access a bank account and withdraw cash from an ATM machine. Video footage from the ATM machine enables investigators to collect a facial image of the offender. The quality of the probe image with regard to FRT searches will vary, depending on, for example, the light exposure and whether the individual has concealed their face. If the quality of the image is adequate, the image can be compared against a database of known criminals using an FRT system. Facial examiners will then analyse and manually compare the probe image with each candidate image and assess if there is a possible match or not. In the event that the examiner reaches the conclusion of a possible match, a peer review will be carried out by a second facial examiner and, if the two agree on the conclusion, they will subsequently share the possible match with the investigators as an investigative lead.



Uncovering the identity of an assailant of police officers during a riot
During a riot, footage of a person attacking police officers may be collected by CCTV cameras. If an investigation is launched, an investigation team will seek to obtain the images captured by the cameras with the goal of identifying the assailant. With the help of the law enforcement agency's digital experts, the investigators will review the CCTV footage of the riot, looking for images of the alleged assailant. They will endeavour to collect the images with the best angle, lighting and exposure possible to optimize the image quality, thus increasing the chances of obtaining possible matches and identifying the assailant. If the images collected are of adequate quality, they can be compared by facial examiners against a database of known criminals using an FRT system to assess if there is a possible match or not. In the event that the examiner reaches the conclusion of a possible match, a peer review will be carried out by a second facial examiner and, if the two agree on the conclusion, they will subsequently share the possible match with the investigators as an investigative lead.

Looking for the identity of a museum thief
Following a break-in and the theft of items of art from a museum, a public prosecutor launches a criminal investigation. Relying on police intelligence, the investigation team already has a known suspect in mind who has operated in the past with a similar modus operandi and accordingly the team wants to verify this intelligence by ascertaining if this individual was in the museum on the day of the theft and in the days before. To do so, the investigators will seek to collect images of all the faces of visitors and staff who appear in the museum' security footage. This will be used to build an investigative special database. An FRT search will then be made against the special database using the probe image depicting the suspected thief that was collected as part of a previous investigation. A list of candidate images is displayed by the FRT system and then reviewed and analysed by a facial expert to establish whether a possible match is detected that could be used to confirm the possible connection of the individual with the break-in. In the event that the examiner reaches the conclusion of a possible match, a peer review will be carried out by a second facial examiner and, if the two agree on the conclusion, they will subsequently share the possible match with the investigators as an investigative lead.



Using facial recognition to fight child abuse
National law enforcement agencies and INTERPOL use FRT to investigate cases of child abuse. To dismantle international child abuse networks, INTERPOL runs investigations in partnership with national law enforcement agencies. Dedicated task forces within INTERPOL and national police departments collect images and pieces of evidence to facilitate the resolution of investigations.

Images and videos showing victims of child abuse are stored in dedicated databases with highly restricted access. These databases are very often developed using a range of tools and features to support the work of investigators, help them to analyse the images and find new leads. FRT can be used to help identify the victims, by searching their facial images in a database containing the facial images of missing persons. Missing minors, however, are not necessarily recorded in these facial databases because the face undergoes many changes throughout childhood and adolescence. In most cases, law enforcement relies on other means to identify victims. FRT can also be used to check if the same child appears in various image sources (termed clustering) and to estimate the period during which the victim has been abused. The primary goal of all of these findings is to identify, locate and rescue the victim as soon as possible.

Facial images of perpetrators, when collected and seized, can be searched in national criminal databases and in the INTERPOL criminal database in order to identify, locate and detain them with a view to prosecution. It is crucial for investigators to collect as much evidence as possible to document and strengthen the prosecution case, using all existing investigative tools, including FRT when relevant.

Using facial recognition to find missing persons
When there is serious evidence suggesting the need for international police cooperation in a missing persons case, national law enforcement agencies may ask INTERPOL to publish a Yellow Notice. A Yellow Notice is a request to law enforcement worldwide to help locate missing persons.[31] This file usually includes facial images, as well as other biometric attributes, such as fingerprints and DNA, where they are available. Once the law enforcement agency of a member country requests a Yellow Notice to be published, an FRT search is performed by INTERPOL to check if the person was previously recorded in the facial recognition database; for example, by another country as a criminal.

The Yellow Notice can be beneficial when a person is declared missing in a given country and found dead in another one. In this case, the Yellow Notice will help identity the deceased person.

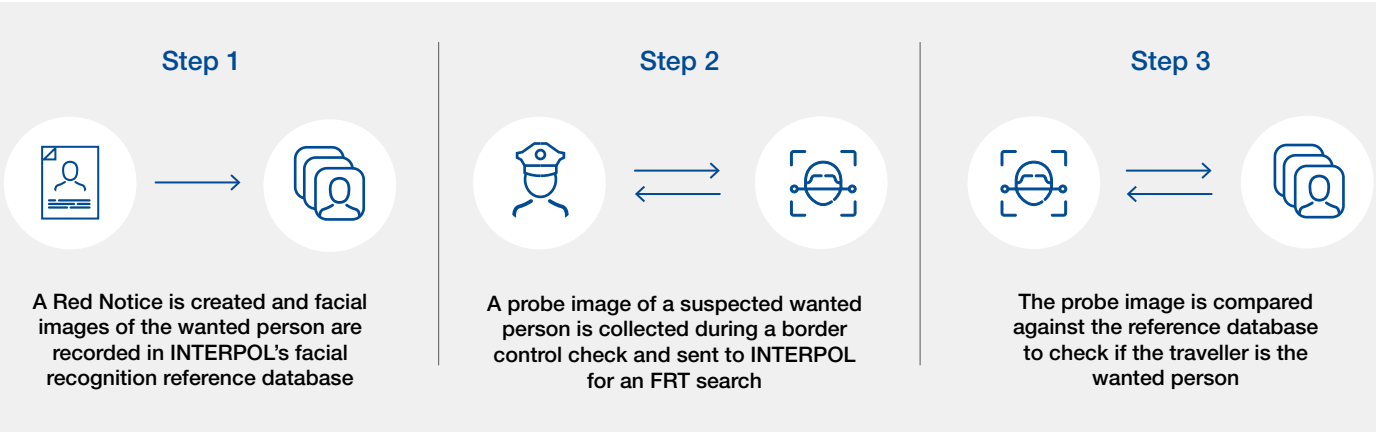
As, generally, databases of minors are not maintained, this use case is different in the case of missing children. With some exceptions, such as the National Tracking System for Vulnerable and Missing Children in India, the only way to identify missing children using facial recognition is by consulting investigation databases of child abuse cases and comparing images.[32]

Identity checking at a border control

Border officers use identity controls to, *inter alia*, detect and potentially detain fugitives and wanted persons who are the subject of an INTERPOL Red Notice – a global police alert to locate and provisionally arrest a person pending extradition, surrender or similar legal action.[33] Red Notices contain information about the individual that can be used to identify them. If there are facial images of the wanted person, these will be stored in INTERPOL's facial image reference database of criminals and missing persons – the INTERPOL Facial Recognition System (IFRS).

In the event that a national border guard controlling the identity of people crossing a border considers a traveller to be the possible subject of a Red Notice, the border guard may seek further verification of the individual's identity by taking their picture and fingerprints. In agreement with their national authorities, border officers may send the facial image to their INTERPOL National Central Bureau (NCB) and to INTERPOL's headquarters for an urgent search against wanted persons and criminals in the IFRS. Once received, INTERPOL facial examiners will run the search as soon as possible in the IFRS using the probe image provided and a list of candidate images will be proposed by the system. Facial examiners will then analyse and manually compare the probe image with each candidate image and assess whether a potential candidate emerges. If this is the case, a peer review will be carried out by a second facial examiner and, if the two agree on the conclusion, they will subsequently inform the concerned INTERPOL NCB and border agents.

It is important to note here that, even if the collection of the probe image and the search are performed almost concurrently – in near real-time – the imperative to act fast in these situations does not prevent the outcome undergoing expert verification and accordingly the standard procedures remain unmodified.



BOX 2

The use of real-time facial recognition technology

The use of real-time FRT for identification undoubtedly represents the most sensitive use case. The imperative to act fast – for instance, to prevent a specific, substantial and imminent threat to the life or physical safety or a terrorist attack – can, exceptionally, necessitate using FRT systems without the outcome undergoing expert verification. In this case, the system would automatically propose potential candidates based on live CCTV footage from public areas of interest or images collected by a law enforcement officer to be acted upon by investigators. In the absence of expert verification, the risk of the concerns outlined above are greatly exacerbated.

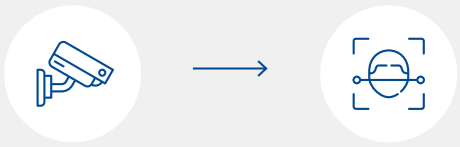
As a result, public awareness of real-time FRT is uniquely heightened. Notwithstanding the validity of the concerns surrounding this particular use case, there is often an unfounded belief that real-time facial recognition is the primary application of the technology. In reality, however, the use of real-time FRT is more limited than is often perceived. To date, a wide range of law enforcement agencies have implemented limited real-time pilots, with only a few agencies opting to adopt the use case into operations. The post-event application of FRT remains, by large, the leading use case.

In light of this, the guidance presented in this insight report is primarily based upon consideration of and tailored to the use of post-event FRT – unless otherwise expressly indicated. That said, the guidance provided is equally applicable to both real-time and post-event uses of FRT. However, in the context of real-time FRT, additional safeguards and higher standards for the application of the proposed principles will need to be taken on board by law enforcement agencies seeking to employ this use case in order to address the extra concerns that it presents.

Actively looking for a terrorist in public spaces
Note: *the following example is a potential use case and has not been activated by either INTERPOL or the Netherlands Police.*

In the aftermath of a terrorist attack, where the terrorist remains at large, CCTV footage may be obtained by law enforcement to collect a probe image of the fugitive terrorist. This probe image can then be distributed to all police patrols actively looking for the fugitive. In addition, the probe image can be compared in real time against live footage from CCTV cameras (or other image sources) located in the terrorist's assumed vicinity, being streamed to an FRT system. This real-time comparison may generate a potential lead that can be sent to police patrols, which can be deployed to the area to investigate.

Step 1



Analysis of collected footage to collect a probe image of the terrorist

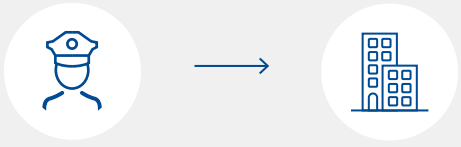
Step 2

Comparison of the probe image with other images collected from CCTV located in the terrorist's assumed vicinity

Step 3

The video comparison leads to a possible match

Step 4



Police patrols are deployed to the area to investigate the lead

2 Principles

A global- and multistakeholder-developed set of principles for the responsible use of facial recognition technology for law enforcement investigations.

Note: *The principles that follow have been identified as the foundations for ensuring that law enforcement agencies use FRT responsibly. Each principle contains a series of actions for them to either implement or take into consideration at the relevant stages of their decision-making process regarding FRT. The principles are not presented in any specific order of importance; however, Principle 1 – "Respect for human and fundamental rights" – can, by its nature, be considered the overarching principle of this framework and viewed as the motivation underlying the design of each of the other principles.*

It should be noted that these principles have been designed primarily with the post-event FRT use case in mind. As previously observed, however, they are equally applicable to the real-time use of FRT – although additional safeguards and higher standards for the application of the principles will be needed to cater for the nuances presented by real-time FRT.

Furthermore, it should be noted that these principles focus on law enforcement investigations only. All other law enforcement activities related to passport, residence permit and ID card issuance/verification, etc. are not covered here and are outside of the scope of this policy framework.

1 Respect for human and fundamental rights

1.1 FRT should be used only as part of a lawful investigation, and always only as an investigative lead, to support the identification of criminals/fugitives, missing persons, persons of interest and victims.

1.2 The rights provided for within the International Bill of Human Rights and other relevant human rights treaties and laws should always be respected, particularly the right to human dignity, the right to equality and non-discrimination, the right to privacy, the right to freedom of expression, association and peaceful assembly, the rights of the child and older persons, the rights of persons with disabilities, the rights of migrants, the rights of Indigenous people and minorities, and the rights of persons subjected to detention or imprisonment. The use of FRT by law enforcement for investigations should respect these rights and be necessary and proportionate to achieve legitimate policing aims.

1.3 Any restrictions or limitations to human rights are permissible under international human rights law only if they are necessary and proportionate to achieving a legitimate policing aim and are not applied in an arbitrary manner. These restrictions must be established in law and should correspond to the least intrusive means of pursuing such an aim.

1.4 Law enforcement agencies should be subject to effective oversight by bodies with enforcement powers in accordance with national laws or policies. Among other things, these or other bodies should have the specific task of hearing and following complaints from citizens and assessing the compliance of law enforcement activities with human and fundamental rights.

1.5 Law enforcement agencies should consider setting up an independent ethical oversight committee or assigning the responsibility to periodically review law enforcement officers' use of FRT to a pre-existing body, supporting them in achieving respect for human and fundamental rights.

1.6 Individuals should have the right to an effective remedy before an independent and impartial tribunal set up by law against actions concerning the use of FRT.

2 Necessary and proportional use

2.1 The decision to use FRT should always be guided by the objective of striking a fair balance between allowing law enforcement agencies to deploy the latest technologies, which are demonstrated to be accurate and safe, to safeguard individuals and society against security threats, and the necessity to protect the human rights of individuals.

2.2 Law enforcement agencies considering the use of FRT should always provide a documented and justified argument as to why FRT is the chosen option and why alternative options were not chosen.

2.3 The use of FRT by law enforcement agencies, from the request to the use of the outcome of the search, should always be aimed at, and limited to, a single specific goal, necessarily related to investigative purposes.

2.4 International, regional and national policies and/or laws should specify for which classes of crimes or investigations the use of FRT by law enforcement agencies is acceptable and/or lawful.

2.5 Acknowledging the right to privacy and other human rights, the collection of images from public and publicly accessible spaces for FRT identification purposes should be done only for a determined list of use cases, in a limited area and for an established processing time period in accordance with relevant national laws or policies.

2.6 As a consequence of the additional risks involved in the use of real-time FRT, an independent authority responsible for oversight of law enforcement operations (such as the independent ethical oversight committee described in Principle 1.5) should be in charge of authorizing applications for its use and, if there is not enough time, it should be authorized through the chain of command. In such cases, the chain of command should inform the independent authority as soon as possible and not later than 24 hours after authorizing the use, justifying its decision to use real-time FRT and explaining why it considered there was insufficient time to seek its authorization in advance. Law enforcement should use the results of any real-time FRT search only to verify an individual's identity and conduct additional verifications. All images captured during an operation involving the use of real-time FRT, both the original image and the biometric template, should be deleted from the system, according to the policies governing the storage of live images.

2.7 FRT, and other face analysis technologies, should be used for no purpose other than biometric identification/recognition/verification. The use of FRT to infer ethnicity, gender, sex, age, emotion, opinion, health status, religion and sexual orientation, and the use of FRT for predictive analysis, should not be permitted.

3 Human oversight and accountability

3.1 Lines of responsibility for the outcome of a given use of FRT should be well defined and transparent. A law enforcement agency should never issue analysis and conclusions from FRT without interpretation by an examiner and oversight by a manager with the right expertise (with the unique exception described in Principle 2.6).

3.2 The use of FRT should always be conducted by an individual trained as described in Principle 8 (with the exception of situations of emergency as presented in Principle 2.6). The skills of facial experts are critical and necessary to maintain the highest level of accuracy in the identification process.

3.3 A peer review (blind verification or examination by a second expert) should systematically be performed before a result is communicated to the requesting investigation team. The result provided should be consensus-based or, in the event of a lack of consensus, the most conservative conclusion in terms of similarities observed should prevail.

3.4 The law enforcement agency should verify that a mechanism exists whereby citizens can file a complaint with or seek redress for any harms before a competent body designated by national authorities.

3.5 If an individual proposed by an FRT system as a potential candidate is subsequently taken into custody, brought in as a witness or assumes any other official role in a law enforcement process, that person should be informed that he/she was subject to a search using FRT, provided that this would not compromise the investigation.

4 Optimization of system performance

4.1 Law enforcement agencies should require vendors to follow FRT standards, such as those set by the International Organization for Standardization (ISO) and the European Committee for Standardization (CEN), to evaluate the performance of their algorithms at the design and deployment stages.

4.2 Law enforcement agencies should introduce a standardized procurement process in a transparent way, requiring vendors to comply with the above-mentioned standards and to submit their algorithms to large-scale independent audits/testing undertaken against appropriate test standards (lab tests and, if possible, field tests). After evaluating all candidates, agencies should select the provider who can demonstrate the best-performing algorithm.

4.3 Due diligence with respect to system performance should be undertaken by reference to large-scale independent tests, such as those conducted by NIST in the US. These tests provide a scientifically robust, transparent baseline of performance.

4.4 Independent lab tests to validate the performance of the FRT should be designed to model, as closely as practical, the real-world objectives and conditions (including data landscape, operators of the technology, timetables affecting decisions made using the technology, etc.) in which the FRT is applied in practice.

4.5 Law enforcement agencies should notify the technology provider of relevant errors identified in order to have the system reviewed.

4.6 To leverage accuracy gains, law enforcement agencies should expect to make, and establish procedures for, regular upgrades or replacement of the FRT.

5 Mitigation of error and bias

5.1 The risk of error and bias by machines and humans should be mitigated to the greatest extent possible. This should be done through an *ex ante* and *ex post* evaluation strategy:

5.1.1 *Ex ante* evaluations: technology providers, and where it applies, technology integrators, should ensure biases and errors are mitigated to the greatest extent possible before the deployment of the system by law enforcement agencies. The level of performance across demographics and the design of the quality management system should be evaluated by an independent third party. This evaluation should be organized by the technology provider and the results made available to law enforcement agencies that procure FRT and to the public for review. Law enforcement agencies that procure FRT should require in their procurement criteria information about the specific metrics the provider uses to gauge bias and other relevant risks. Before deploying FRT systems, law enforcement agencies should set up pilot tests to ensure the system is operating as intended.

5.1.2 *Ex post* evaluations: law enforcement agencies – if necessary, with the support of competent authorities – should deploy risk-mitigation processes to identify, monitor and mitigate the risks of error and biases throughout the entire life cycle of the system. A regularly programmed internal audit (that could include the use of the self-assessment questionnaire related to these principles) and, if possible, an independent third-party audit should be conducted to validate the robustness of these processes. The conclusions of these audits should be made publicly available.

To continually improve the quality of the processes and the system's performance, law enforcement agencies, technology providers and technology integrators should establish an in-service support agreement throughout the entire life cycle of the system.

6 Legitimacy of probe images and reference databases

6.1 Law enforcement agencies should ensure that their processing of probe images and reference databases are compliant with international, regional and national laws and/or policies, which should include storage criteria, purpose limitation, retention period, deletion rules, etc.

6.2 The collection of probe images should be conducted on a legal basis and aimed at a specific purpose.

6.3 The reference database(s) used for FRT investigations should always have a legal basis and be used under the authorization of competent authorities. Consequently, reference databases that include data collected without legal basis from the internet, electronic devices or other sources should not be used.

6.4 Probe images should not be inserted into the reference database by default. Probe images of unidentified subjects may be stored in a database for further investigation; however, such images should be appropriately labelled (e.g. as an unidentified suspect or unidentified victim) and the reasons for their insertion into the database detailed. Differently labelled categories of image can be stored on the same database but should be logically separated so that facial experts can, with requisite authorizations, independently search the specific categories. Additional care should be afforded to ensure that, if the underlying status justifying the insertion of the probe image into the database (e.g. as an unidentified suspect) changes, the image is removed from the database.

6.5 Exporting images and biometric metadata to public cloud-based FRT that could potentially be outside the local jurisdiction should be prohibited.

6.6 Law enforcement agencies should maintain a strict and transparent chain of custody of all images (probe image sets and reference databases) used for FRT. The law enforcement agency should specify, and enforce, clear and transparent rules designating who does and does not have access to the images, and under what circumstances.

6.7 Law enforcement agencies should specify well-defined protocols for determining when, and on the basis of what criteria, images are to be deleted from a probe set or a reference database. The law enforcement agency should create, and adhere to, a well-defined and transparent protocol for the disposal of images that have been deleted from a probe set or reference database or are otherwise no longer needed; any such protocol should be designed to protect the privacy of any individuals appearing in the images identified for disposal.

6.8 For all solved cases or for cases where the investigation has been concluded, the biometric template of the probe image should be deleted from the FRT system and the original facial image stored for accountability purposes in line with existing national law and policies.

7 Integrity of images and metadata

7.1 Law enforcement agencies should establish standards and thresholds of image quality for reference database images in order to mitigate the risk of errors. Reference database images that do not meet the defined standards and image-quality thresholds should not be used.

7.2 Law enforcement agencies should also establish best practices to evaluate image quality for probe images. Before any search using an FRT system, the facial examiner should conduct a manual assessment of the image to ascertain if the probe image is of a high-enough quality to conduct a facial comparison. If the expert is unable to do so manually, the probe image should be rejected. Although a minimum number of pixels between the eyes is often recommended, care should be taken when using this as a threshold as it is often insufficient to confirm image quality.

7.3 Standards for probe images and reference database images should be identified by each law enforcement agency, taking into account the strength of the algorithm, the results of internal testing of the FRT system, the nature of the use case and any recommendations from the technology provider regarding its specific system. Standards, such as International Civil Aviation Organization (ICAO) photo standards, may serve as guidance for assessing image quality of reference database images. Guidance on best practices for probe images and additional recommendations for reference database images could also be provided by groups such as the Facial Identification Scientific Working Group (FISWG), the European Network of Forensic Science Institutes Digital Imaging Working Group (ENFSI-DIWG) and the INTERPOL Facial Experts Working Group (IFEWG).

7.4 Law enforcement examiners should be aware of the risk of image manipulation, such as morphing and deepfakes, when images come from uncontrolled sources and/or production modes. When suspected, these images should be rejected or processed with extreme precaution.

7.5 Forensic upgrading (e.g. contrast and brightness correction) should comply with existing published guidance or standards (such as by FISWG).

7.6 The use of tools for non-forensic upgrading (e.g. pose correction) should be used only during the FRT search phase. If non-forensic upgrading is carried out, the insertion or modification of facial features or geometry on an existing image should be performed with care in order to avoid distortion of the image.

7.7 In case of a possible match, and to reach a final conclusion, forensic upgrading of face quality only should be accepted. For reporting purposes, the original image should be presented together with the description of forensic upgrading methods to ensure the auditability and reproducibility of the upgrading process.

7.8 While processing data, law enforcement agencies should always conduct a proper and verified attribution of identity to photos in the reference dataset, and verify the serial number of photos, their traceability and origin.

7.9 The integrity of the reference database should be evaluated regularly, in accordance with the applicable legal framework and best practices.

7.10 Vulnerabilities to hacking and cyberattacks should be identified to ensure robustness and avoid data leaks and data manipulation.

8 Skilled human interface and decision-making

8.1 FRT should be used only by trained persons who follow the procedures ordered through the chain of command and/or by management.

8.2 Everybody within the organization, especially the chain of command/management, should understand the capacities and limits of the technology and system used.

8.3 Law enforcement agencies that use or intend to use FRT should provide or facilitate training on an ongoing basis and should be informed by the latest research in machine learning and remote biometrics.

8.4 The training (and certification when it applies) of facial experts, and those in the chain of command/management, should include:

8.4.1 Knowledge of and updates of mandatory regulations, laws or policies concerning the use of biometrics.

8.4.2 Awareness of the risk of biases by the FRT system (anticipation of false positives and false negatives, awareness of differences in performance on various demographics, knowing how to calibrate and adjust the threshold of the system, understanding how to configure the system in the manner appropriate to the specific circumstances and risks of a given use case, and how to fix the length of the candidate lists).

8.4.3 Understanding of the risk of biases by the human agent (overestimation of own capability, risk of over-reliance on technology, blind spots, risk of human bias such as other-race-effect bias).

8.4.4 Awareness of the risk of false positives from twins, siblings and other related individuals.

8.4.5 Awareness of the risk of image manipulation, including data integrity attacks and data morphs, and, when available, the tools to identify them.

8.4.6 How to implement risk-mitigation methodologies (one match vs. differential diagnosis approach, blinding techniques, blind verifications, etc.).

8.4.7 Understanding of the nature of an investigative lead as the outputs of an FRT search and best practices for verifying the identity of leads generated.

8.4.8 Instruction in data governance procedures, including the collection, storage, integrity and traceability of data.

8.4.9 How to use tools, when available, that assist examiners in understanding the reasoning behind systems' decisions/recommendations.

8.5 Recognizing that innate capability to recognize faces exists on a spectrum, examiners should be recruited by factoring in performance on face comparison tests, acknowledging that experience and training also matter.

9 Transparency

9.1 Information about the use of FRT by law enforcement agencies should be available to the public. This information should be made available on a permanent basis or on request, and communicated by the appropriate official authorities, be it the law enforcement agency itself or another government entity.

9.2 Law enforcement agencies, or the most appropriate other official authority – with input from the law enforcement agency – should, in line with the applicable laws and policies, make public:

9.2.1 A clear definition of the use of FRT for law enforcement investigations, specifying the purpose and objectives, such as to identify criminals/fugitives, persons of interest, missing persons and victims.

9.2.2 The vendor selected (if applicable) and the name and version of the software.

9.2.3 How they use probe images: procedures and criteria to select, store/not store images and, if stored, for how long.

9.2.4 How they use the reference database: procedures to consult the database, criteria to select, store/not store probe images in this reference database and, if stored, for how long; as well as details about whether this database can be used to train or refine other FRT systems or machine learning models in general.

9.2.5 The policy regarding the type of data that may be shared with other organizations, including personal data and databases of face images.

9.2.6 The name of law enforcement departments or units able to launch searches and view the results of searches.

9.2.7 The functional title, type of expertise and level of training of individuals using the system.

9.2.8 The process to determine a possible match, namely blind-review or peer-review of possible matches.

9.2.9 Information about the mechanisms in place (see Principle 1.5) to ensure FRT is used as intended.

9.2.10 Auditable records of search requests made by law enforcement agencies, such as the number of requests, the number of investigative leads generated and the type of crimes related to these requests.

9.2.11 The results of audits and/or evaluations of the performance of the FRT system conducted by the vendor of the technology and/or by the law enforcement agency. This should include a description of: the design of the evaluation; the data used in the evaluation; and the results (metrics) obtained.

9.2.12 Information about how an individual can contact the law enforcement agency to submit a query or complaint concerning its use of FRT.

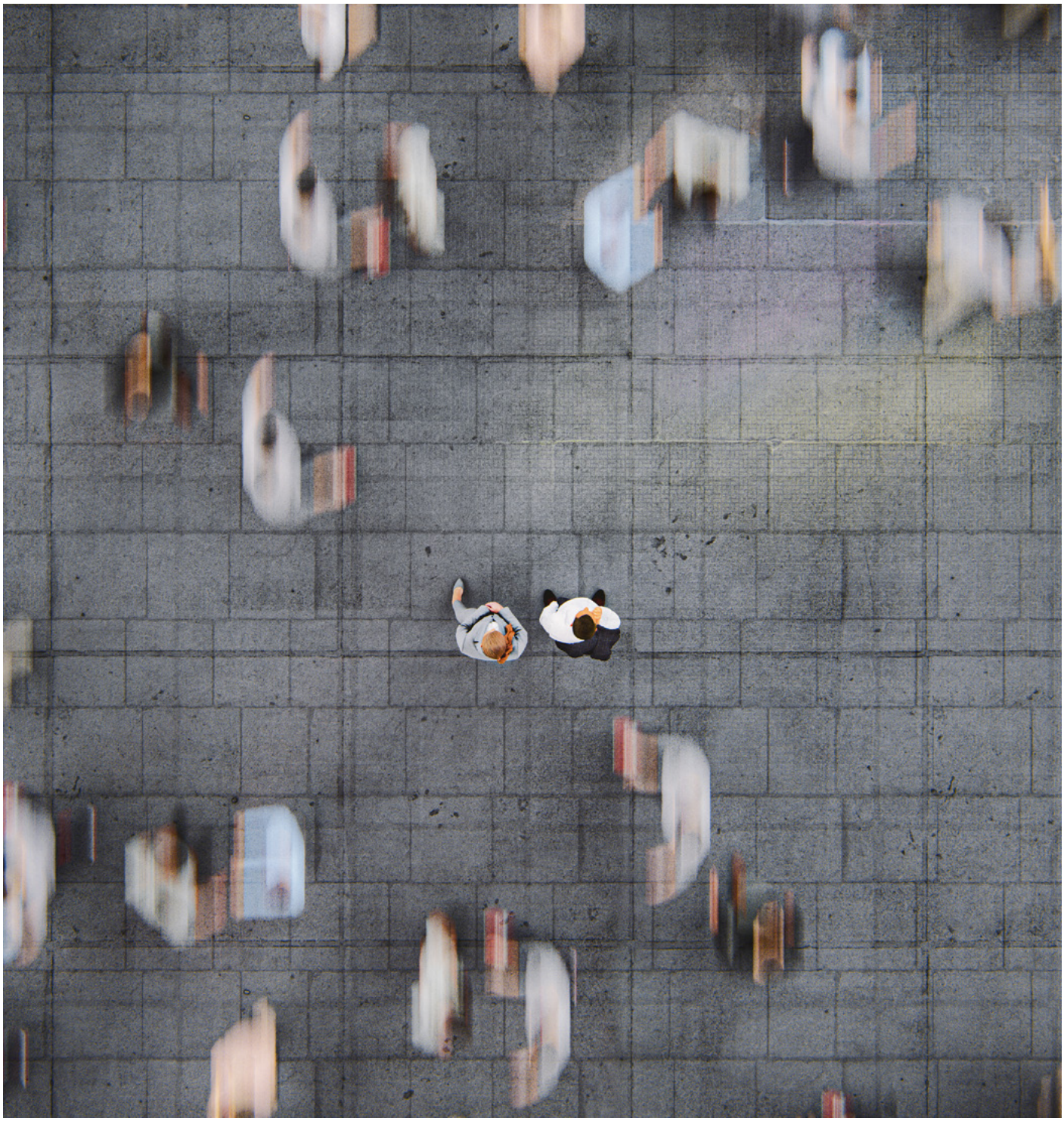
9.2.13 A record of complaints filed by members of the public against the use of the FRT and the law enforcement agency's response of those formal complaints.

9.2.14 Any other information that can be publicly shared without compromising law enforcement investigations and that may be relevant for the public.

9.3 Information made available to the public should be concise, easily accessible, understandable and provided in clear and plain language. Exceptions to this should be permitted only if they are necessary and proportionate to pursue legitimate purposes and in accordance with the law.

3 Self-assessment questionnaire

A self-assessment tool to support law enforcement agencies in ensuring they have introduced the measures needed for responsible facial recognition.



Note: *This self-assessment questionnaire has been designed to reflect the preceding principles and is intended to support law enforcement agencies to develop policies surrounding the use of FRT and to review existing policies in line with the proposed principles. It does so by prompting law enforcement agencies to consider how they approach the use of FRT and the rules and procedures they may or may not have in place to responsibly govern the use of FRT in investigations.*

The self-assessment questionnaire is intended to serve as a tool to support law enforcement agencies on a continuous basis throughout their use of FRT and, accordingly, should not be considered as a one-off exercise or checklist. It is recommended that agencies regularly run the process of completing the self-assessment questionnaire or reviewing the relevant parts, as follows:

1. *Before implementing FRT for the first time*
2. *Before employing FRT in the context of a new use case*
3. *After every software update to the core algorithm of the FRT system*
4. *After changes in the current policies that have an impact on the software, databases or practices concerning the use of FRT*

Completing the self-assessment questionnaire will require consultation with multiple stakeholders (both internal and external), including but not limited to the FRT system provider, biometric experts, IT experts, and legal advisers. It is recommended that the individual(s) completing the questionnaire endeavour to answer all questions, reaching a single conclusion, that the agency is either:

1. *Compliant*
2. *Non-compliant, with a clarification of why not*
3. *Non-compliant, with a statement of actions that can be taken for improvement*
4. *Non-compliant, with a statement that action cannot be taken and a clarification of why not*

It is recommended that once completed, the final result, along with an explanation and summary of the outcome of the self-assessment questionnaire, is made public to increase transparency and accountability.

1 Respect for human and fundamental rights

1.1 Does your use of FRT for law enforcement investigations respect the International Bill of Human Rights and other relevant human rights treaties and laws?

1.2 Is the output of an FRT search always considered only as an investigative lead?

1.3 What procedures are in place to guarantee that restrictions or limitations to some human rights are allowed only if they are necessary and proportionate to achieving a legitimate policing aim?

1.4 Are you working with oversight bodies to effectively assess the compliance of law enforcement activities with human and fundamental rights?

1.5 Are these bodies tasked with hearing and following complaints from citizens?

1.6 Is there an independent ethical oversight committee to periodically review your use of FRT and support you to achieve respect for the human and fundamental rights?

1.7 Is there an existing judicial authority that offers effective remedies to individuals who consider their rights to have been violated through the use of FRT?

2 Necessary and proportional use

2.1 What uses of FRT are allowed in your jurisdiction and what is the basis in applicable international, regional and national laws or policies?

2.2 What was the objective that guided the decision to use FRT?

2.3 Which alternatives were considered before taking the decision to deploy FRT in your agency, and what were the criteria that ultimately led to the decision to reject those alternatives?

2.4 How do you ensure that your use of FRT, from the request to the use of the outcome of the search, is appropriate, limited and exclusively related to investigative purposes?

2.5 What uses of FRT are allowed in your jurisdiction (based on laws defined by international, regional and national laws or policies)?

2.6 What are the use cases for which you are authorized to collect images from public spaces for FRT identification?

2.7 What processes and controls are in place to ensure that the collection of images from public and publicly accessible spaces for FRT identification purposes is done only for a determined list of use cases, in a limited area and for a finite time period?

2.8 What procedures are in place governing work conducted with independent authorities in charge of authorizing real-time uses of FRT for identification purposes under exceptional circumstances?

2.9 In cases where your agency deploys real-time FRT, is there an independent authority or an established ethical oversight committee (see Principle 1.5) that regulates its use?

2.10 If real-time use of FRT is authorized through the chain of command because of a lack of time to inform the independent authority, what processes have you introduced to ensure that the chain of command informs the independent authority within 24 hours and justifies its decision to use real-time FRT, outlining why it felt there was insufficient time to obtain authorization in advance of its use?

2.11 In cases of real-time use of FRT, what processes have you implemented to make sure all images recorded by the real-time FRT system, including the biometric template and the original face image, are deleted, according to the defined policies for the storage of live images?

2.12 What processes have you implemented to prevent the use of FRT to infer ethnicity, gender, sex, health status, age, emotion, opinion, religion or sexual orientation recognition or for predictive analysis?

3 Human oversight and accountability

3.1 What processes have you introduced to ensure that an FRT output is always verified by an examiner with oversight by a manager with the appropriate level of expertise (except in the case described in Principle 2.6)?

3.2 How do you ensure the FRT system is always used by individuals trained as suggested on Principle 8 (except in the case described on Principle 2.6)?

3.3 Is a systematic peer review performed before reaching any final decision?

3.4 When two experts are assigned to evaluate the results, how do you reach a consensus between the examiner and reviewer(s)?

3.5 What mechanisms are in place for citizens to file a complaint with or seek redress from a competent body?

3.6 Do you inform individuals taken into custody, brought in as a witness or involved in an investigation that they were identified using an FRT system, provided this does not compromise the investigation?

4 Optimization of system performance

4.1 What existing or forthcoming standards do you ask your vendor to follow to evaluate the performance of your FRT system?

4.2 Have you introduced procurement rules to select providers who comply with these standards of performance?

4.3 Have you introduced procurement rules to select providers who have submitted their FRT system to an independent evaluation such as that organized by NIST?

4.4 Have you selected the technology provider who presented the best results?

4.5 Are the independent lab tests of performance designed to model, as closely as possible, the real-world objectives and conditions in which the FRT is applied in practice?

4.6 Do you notify the technology provider when you identify relevant errors in the use of the FRT system?

4.7 What procurement rules have you introduced to ensure the regular upgrading or replacement of the FRT?

5 Mitigation of error and bias

5.1 How is your technology provider (or where it applies, the integrator) making sure that biases and errors are mitigated to the greatest extent possible before the FRT system's deployment?

5.2 Has the FRT software been tested by an independent third-party organization on the level of performance across different demographic groups?

5.3 Has the design of the quality management system of the FRT system been evaluated by an independent third-party organization?

5.4 Have technology providers and integrators communicated the results of those evaluations to law enforcement agencies and the general public?

5.5 Do your procurement criteria require information to be supplied about the metrics that technology providers use to gauge bias and other relevant risks?

5.6 Did you set up pilot tests before deploying the FRT system?

5.7 Have you deployed risk-mitigation processes to identify, monitor and mitigate the risks of error and biases throughout the entire life cycle of the system?

5.8 Have you programmed internal audits and, if possible, an independent third-party audit, to validate the robustness of your risk-mitigation processes? If yes, have you publicly shared the results of these audits?

5.9 Have you established an in-service support agreement throughout the entire life cycle of the system in collaboration with technology providers and integrators?

6 Legitimacy of probe images and reference databases

6.1 Is your processing of probe images and reference databases, including storage criteria, purpose limitation, retention period and deletion rules, compliant with international, regional and national laws or policies?

6.2 What processes have you introduced to ensure that the collection of probe images is conducted on a legal basis and aimed at a specific purpose?

6.3 How do you ensure that images contained in your reference databases are collected only with a legal basis?

6.4 Do you label unidentified probe images according to their corresponding categories – e.g. as "unidentified suspect" or "unidentified victim"?

6.5 Do you store unidentified probe images in your reference databases? If yes, can they be searched separately?

6.6 Do you remove unidentified probe images from the unsolved probe database if an image's underlying status, which justified the image's insertion in the database, changes?

6.7 What technical measures have you put in place to prevent the export of images and biometric metadata to public cloud-based FRT systems that could potentially be outside the local jurisdiction?

6.8 How do you ensure a strict and transparent chain of custody of all images (probe image sets and reference databases)?

6.9 Are there clear and transparent rules designating who does and does not have access to probe images and reference databases and under what circumstances?

6.10 Have you established clear and transparent protocols for determining when, and based on what criteria, images are to be deleted from a probe image set or a reference database, taking into particular consideration the need to ensure the protection of the privacy of any individuals appearing in such images?

6.11 Is the biometric template of the probe image deleted from the FRT system for all solved cases or for cases for which the investigation has been concluded?

6.12 For all solved cases or for cases for which the investigation has been concluded, is the original facial image stored in line with existing national law and policies for accountability purposes?

7 Integrity of images and metadata

7.1 Have you established image quality standards for reference database images?

7.2 Do you exclude reference images that do not meet those quality standards?

7.3 Do you have a procedure in place to perform an image quality assessment of the probe image before any FRT search is launched?

7.4 Have you established a threshold of a minimum number of pixels between the eyes for the probe image to be used?

7.5 Do you exclude probe images that do not satisfy a manual assessment of image quality?

7.6 What quality reference standards and thresholds are you following? Have you considered best practices and recommendations, such as those presented by ICAO, FISWG, ENFSI/DIWG and IFEWG?

7.7 How do you manage the risks of image manipulation (deepfakes, morphing, etc.)? Do you deploy a specific procedure to detect them when you collect images from uncontrolled sources?

7.8 If you detect a manipulated image (deepfake, morphing, etc.), how do you process this image?

7.9 If you perform forensic upgrading of face quality, which methods of image processing do you use? Can any of these processes be considered to modify the original face features, adding or removing data from the image?

7.10 Do you comply with published guidance or standards (such as by FISWG) when using tools for forensic upgrading of face quality?

7.11 How do you ensure that non-forensic upgrading of face quality is used only during the search phase?

7.12 In case of a possible match, do you use the forensic upgraded image for final conclusions?

7.13 How do you document forensic upgrading to ensure the auditability and reproducibility of the upgrading process?

7.14 What processes do you follow to ensure the proper attribution of identity to photos in the reference dataset and to verify the serial number of photos, as well as their traceability and origin?

7.15 Have you performed a system security verification to identify vulnerabilities to hacking and cyberattacks?

8 Skilled human interface and decision-making

8.1 Is FRT used only by trained persons?

8.2 Does everybody within the organization understand the capacities and limits of the technology and system used?

8.3 Is a training programme offered and, if so, how often is it offered?

8.4 How do you evaluate the quality of the training programme over time, taking into consideration the latest progress in research (e.g. have you established a scientific committee or equivalent, etc.)?

8.5 Have you ensured that the training (and certification when it applies) of face experts and agents within the chain of command/management includes information about:

- 8.5.1 Mandatory regulations, laws or policies concerning the use of biometrics?
- 8.5.2 Risk of machine biases related to FRT systems?
- 8.5.3 Risk of human biases when using FRT systems?
- 8.5.4 Risk of false positives from twins, siblings and other related individuals?
- 8.5.5 Risk of image manipulation, including data integrity attacks and data morphs, and training on existing or new tools used to detect them?
- 8.5.6 Implementation of risk-mitigation methodologies?
- 8.5.7 Nature of the investigative leads and best practices for verifying the identity of leads generated?
- 8.5.8 Data governance procedures, including the collection, storage, integrity and traceability of data?
- 8.5.9 Use of tools that assist examiners in understanding the reasoning behind systems' decisions/ recommendations?

8.6 Have you implemented recruitment processes to primarily hire examiners who perform well on standardized face comparison tests?

9 Transparency

9.1 Is information about your use of FRT publicly available on a permanent basis or by request?

9.2 Have you, or another official authority with input from your agency, publicly shared information about:

9.2.1 The purpose of the FRT solution deployed and a clear definition of its use and the various FRT use cases?

9.2.2 The vendor and the name and version of the selected software?

9.2.3 Your processes regarding the use of probe images, including procedures and criteria to select, store/not store images and, if stored, for how long?

9.2.4 Your processes regarding the use of reference databases, including procedures to consult the databases, and criteria to select, store/not store probe images in this reference database and, if stored, for how long?

9.2.5 Information of whether the reference databases can be used to train or refine other FRT systems or machine learning models in general?

9.2.6 The policy regarding the type of data that may be shared with other organizations, including personal data and databases of face images?

9.2.7 The list of law enforcement departments that have access to FRT search requests?

9.2.8 The functional title, type of expertise and level of training of individuals using the system?

9.2.9 The process to determine a possible match process, namely blind-review or peer-review of possible matches?

9.2.10 Information about the mechanisms in place (see Principle 1.5) to ensure FRT is used as intended?

9.2.11 Auditable records of search requests made by law enforcement such as the number of requests, the investigative leads generated and the type of crimes related to the requests?

9.2.12 The results of audits and/or evaluations of the performance of the FRT system conducted by the vendor of the technology?

9.2.13 The results of audits and/or evaluations of the performance of the FRT system conducted by the law enforcement agency?

9.2.14 Information about how an individual can contact law enforcement to submit a query or complaint?

9.2.15 A report presenting the complaints, and responses from law enforcement agencies to citizens' complaints about the use of FRT?

9.3 How do you ensure that the information provided to the public about law enforcement's use of FRT is concise, easily a*ccessible, understandable and provided in clear and plain language?*

Conclusion

The deployment of FRT for law enforcement investigations around the world is arguably among the most sensitive use cases of facial recognition due to the potentially disastrous effects of system errors or misuses in this domain. The rapid pace and the extent to which FRT has been integrated into law enforcement has served, for many, to underscore the pressing need to take action to mitigate these risks as much as possible. At the same time, public expectations of law enforcement are exceptionally high and law enforcement is increasingly under pressure to effectively solve crimes and serve justice faster and faster. In the face of ever-more complex and dynamic criminal activities and limited resources, many in the law enforcement community feel that FRT is not only as option, but a necessity.

This insight report is about *balance*. It suggests that a balance can be struck between the exigencies of law enforcement to innovate and use new technologies to investigate criminal activities and the need to address concerns voiced by critics surrounding this particularly controversial technology.

The set of principles contained in this report serves as a proposal for what a robust governance response could look like. It takes into account the diverse perspectives of law enforcement, industry and civil society and has been developed with a global perspective in mind, striving to support not only law enforcement agencies in all countries across the globe, but also policy-makers and technology providers in this field, as well as keeping the general public informed about the current status of FRT in law enforcement.

The work to develop this framework has benefited significantly from the pilot exercise conducted in the first half of 2022. The results of the pilot have served to improve the overall quality of the framework and to ensure that what is presented is actionable, relevant and useable in an operational law enforcement context. The collaboration and participation of the Brazilian Federal Police, the Central Directorate of the Judicial Police of France, the National Gendarmerie of France, the Netherlands Police the New Zealand Police and the Swedish Police Authority have, in this regard, been invaluable in creating this unique output.

The pilot exercise served to clearly demonstrate that very different procedures exist from agency to agency, which in turn shows a lack of standardization and evidences the absence of guidance to facilitate such standardization. A consensus formed around one aspect in particular, however, and could be seen in the agencies' diverse procedures, namely the importance of the human element of the use of FRT. This human element manifested in three ways. First, it is essential that the human being understands the technology – its functioning, its use and its limitations – in order to be in a position to be able to mitigate the risks. Second, agencies agreed that any output of an FRT search should be reviewed by a trained facial expert. Third, even after this review, the conclusion of the search remains always and solely an *investigative lead* to be verified by investigators. Collectively, this serves to ensure that a human being is always central to the use of FRT and that identification is never automated. The risk of unfortunate instances of wrongful arrests resulting from the use of FRT can be minimized if this approach is strictly implemented in the manner proposed in this framework.

The pilot has additionally shed light on three other key areas that need additional attention in future:

– *Transparency and communication* with the public about the use of FRT was recognized as a significant challenge for law enforcement agencies. Many agencies highlighted and demonstrated a clear understanding of the importance of this element as a means to build public trust, although they voiced concerns about their own inexperience in this regard and the lack of practical guidance to support them to improve transparency.

– *Training* was repeatedly identified as being instrumental to realizing the ambitions of the entire framework proposed. The pilot exercise demonstrated clearly that training was not always consistently addressed by law enforcement agencies, with great disparity being seen in terms of the nature, scope and duration of training provided to officers using FRT systems. Going beyond the training of users, it is also vital to ensure that decision-makers in law enforcement equally receive adequate training to enable them to develop and implement internal governance frameworks for the use of FRT in their agencies.

– *Real-time FRT* presents unique challenges, and law enforcement agencies need additional tailored guidance. Although the belief that real-time FRT is the primary application of FRT in law enforcement is unfounded, several pilots of passive real-time FRT have been conducted across the globe and the use of mobile devices for active real-time FRT is growing. While this framework addresses such uses of FRT by law enforcement, further consideration is needed of the additional safeguards and standards that would be required to ensure the outcome of a process involving real-time FRT is reliable and accurate.

Having developed, tested and validated the principles and the complementary self-assessment questionnaire, attention now shifts to leveraging and scaling the work done. Of primary importance in this regard is the need to initiate efforts to encourage decision-makers in law enforcement agencies and national policy-makers to take on board this framework as a guide for their agencies' use of FRT and, ultimately, in the creation or amendment of related rules, procedures and legislation for the use of this technology by law enforcement.

The law enforcement community at large, as well as policy-makers at the national and international level, industry partners, civil society organizations and academia engaged in the global debate about the governance of FRT are encouraged to join in these efforts and to promote the adoption and deployment of governance frameworks such as this.

Glossary

Accuracy of facial recognition
The accuracy of an FRT system is based on the number of correct predictions, which consist of a combination of two so-called "true" conditions:

- True positives: when the FRT correctly identifies a person enrolled in the system.
- True negatives: when the FRT correctly finds no match for a person who is not enrolled in the system.

Accuracy is defined as the percentage of correct predictions, i.e. it is calculated by dividing the number of the two types of correct predictions by the number of total predictions.

Algorithm
A series of instructions to perform a calculation or solve a problem, implementable by a computer. Algorithms form the basis of everything a computer can do and are, therefore, a fundamental aspect of all FRT systems.

Audit
Verification activity, such as an inspection or examination of a process or quality system, to ensure compliance with requirements.

Bias in facial recognition technology
False positives and false negatives rate variations caused by a specific factor; for example, demographic dependencies across groups defined by sex, age, religion, race or country of birth. This lack of accuracy is usually caused by the training dataset of the algorithm, which does not contain enough or accurate representations of the demographics in each case.

Biometric identification
Applications that use biometric comparison to verify a biometric "claim of identity".

Biometric recognition
Automated recognition of individuals based on their biological and behavioural characteristics. It encompasses both biometric verification and biometric identification. Automated recognition implies that a machine-based system is used for the recognition, either for the full process or assisted by a human being.

Biometrics
A variety of technologies in which unique identifiable attributes of people, including but not limited to a person's fingerprint, iris print, handprint, face template, voice print, gait or signature, are used for identification and verification.

Biometric template
A set of stored biometric features. A biometric template is created by converting a probe image into a mathematical file of characteristics, distinct from the original facial image, that can be used for subsequent authentication and verification activities.

Biometric verification
Applications that search a database of the biometric characteristics of known individuals to find and return the identifier attributable to a single individual.

Clustering (NxM)
The automated grouping of biometric samples – for example, a collection of facial images – based on computer-evaluated similarities. In the case of FRT, this can be used to check if the same person appears in various image sources.

Computer vision
A field of computer science that works on enabling computers to identify and process images in a way similar to how humans perform these actions, and then provide appropriate output.

Explainability
A property of AI systems that provides a form of explanation for how outputs are reached. Explainability is important to improve decision understanding and increase the trust of operators and users of the FRT systems.

Face detection
The automatic process of finding human faces by answering the question, "Are there one or more human faces in this image?" Face detection differs from face identification/verification as it does not involve biometric analysis.

Face identification (or one-to-many)
The process of answering the question, "Is this unknown person the same person as in any of the images in a reference database?" Identification compares a probe image to all of the images stored in a reference database, so it is also called "one-to-many" matching. A list of candidate matches is returned based on how closely the probe image matches each of the images from the reference database.

Face verification (or one-to-one)
The process of answering "yes" or "no" to the question, "Are these two images depicting the same person?" In security or access scenarios, verification relies on the existence of a primary identifier (such as an ID), and facial recognition is used as a second factor to verify the person's identity.

Facial assessor/reviewer/examiner
Three distinct categories of roles in the process of conducting a face analysis:

- **Facial assessor:** Performs a quick comparison of image-to-image or image-to-person, typically with controlled images, carried out in screening and access control applications or field operations. Due to limitations such as time constraints, assessors perform the least rigorous of all facial comparison processes. An example is a person at a port of entry or in the field using a mobile FRT system to assist with an identity verification.
- **Facial reviewer:** Performs a comparison of image(s)-to-image(s) generally resulting from the adjudication of a candidate list generated by an FRT. The comparison results are often used in either investigative and operational leads or intelligence-gathering applications.
- **Facial examiner:** Performs a comparison of image(s)-to-image(s) using a rigorous morphological analysis, comparison and evaluation of images for the purpose of effecting a conclusion, often used in a forensic application.

Facial comparison
An estimation, calculation or measurement of similarity or dissimilarity between a biometric probe and biometric reference(s).

Facial recognition technology
Software that is able to detect, enrol and compare faces from a digital image or a video frame against a database of enrolled reference facial image(s). This biometric software compares and analyses patterns of a person's facial features to support the identification of that person.

False negative
A test result that incorrectly indicates that the person on the probe image is not enrolled in the reference database when in fact the person is enrolled.

False positive
A test result that incorrectly indicates that the person on the probe image is enrolled in the reference database when this is not the case.

Forensic upgrading of face quality
Enhancement of the quality of an image without the creation of new content, insertion or modification of facial features or geometry. This can include horizontal flip, brightness or contrast correction.

Law enforcement agency
Any government agency responsible for the enforcement of the law, such as police forces, the military or internal affairs units.

Non-forensic upgrading of face quality
Image-processing techniques that may involve the creation of new content, insertion or modification of facial features or geometry. This can include pose correction or removal of a face mask. The use of non-forensic upgrading is normally implemented during the search phase and not for final conclusions.

Peer review face analysis
A peer review process based on blind verification or second opinion that validates the conclusions of any initial human analysis.

Potential candidate
Unlike fingerprints and DNA, which provide definitive evidence, the output of an identification process made by FRT is always, at most, only a potential candidate. One of the reasons for this is the fact that face appearance might be affected by different factors, such as ageing, cosmetics, plastic surgery, the effects of drug abuse or smoking, the pose of the subject, etc., which can affect the final conclusion reached by the FRT system. Importantly, the potential candidate is considered only as an investigative lead.

Probe image
The image collected from a person of interest to be submitted to face identification or face verification.

Real-time and post-event facial recognition:[34]

- **Real-time facial recognition:** In the case of real-time FRT systems, the capturing of the biometric data, the comparison and the identification all occur instantaneously, near-instantaneously or in any event without a significant delay. Real-time systems involve the use of live or near-live material, such as video footage, generated by a camera or other device with similar functionality.
- **Post-event facial recognition:** In the case of post-event FRT systems, in contrast, the facial image has already been collected and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed-circuit television cameras or private devices, which have been generated before the use of the system in respect of the natural persons concerned.

Reference database
The repository of images against which a probe image is compared. In the law enforcement context, two main typologies of database exist:

- **Reference database of known suspects** Composed of photos and mugshots of criminals, missing persons and persons of interest.
- **Investigative special database** Uniquely created for the purpose of an investigation, which is deleted when the case is closed.

Training dataset for facial recognition technology models
Repository of images of annotated faces that are used as an input to a, FRT model during the training phase, in order to make it learn from examples and provide correct predictions based on unseen data.

Contributors

Lead Authors

Maria Eira
Information and Technology Officer, Centre for AI and Robotics, UNICRI

Luc Garcia
Face Examiner, Forensics and Police Data Management Sub-Directorate, INTERPOL

Sébastien Louradour
French Government Fellow, World Economic Forum (until September 2021)

Lofred Madzou
Project Lead, Artificial Intelligence and Machine Learning, World Economic Forum (until February 2022)

Odhran McCarthy
Programme Officer, Centre for AI and Robotics, UNICRI

John Riemen
Lead Biometric Specialist, Netherlands Police

Arunima Sarkar
Artificial Intelligence Lead, Centre for the Fourth Industrial Revolution, World Economic Forum

Acknowledgements

The World Economic Forum, INTERPOL, UNICRI and the Netherlands Police wish to thank the following people for their insightful contributions:

Pilot Members

Xavier Bitaud
Department of Technologies Applied to the Investigation, Central Direction of the Judicial Police, General Directorate of the National Police, France

Thomas Gillot
Department of Technologies Applied to the Investigation, Central Direction of the Judicial Police, General Directorate of the National Police, France

Carla Gilmore
Inspector, Manager, Emergent Technology, New Zealand Police

Niklas Klasson
Forensic Expert, National Forensic Centre, Swedish Police Authority

Elisabet Leitet
Senior Forensic Expert, National Forensic Centre, Swedish Police Authority

Jean-Jacques Soboul
Department of Technologies Applied to the Investigation, Central Direction of the Judicial Police, General Directorate of the National Police, France

Michelle Soper
Principal Adviser, Emergent Technology, New Zealand Police

Alexsandro Vasconcellos
Biometrics Expert, National Institute of Identification, Polícia Federal, Brazil

Manon Vuillermet
Major, Deputy of the Criminal Databases Division, National Criminal Intelligence Service, National Gendarmerie, France

Notable Other Contributors

Balques Al Radwan
Associate Expert, Cybersecurity and New Technologies Unit, UN Office of Counter-Terrorism (UNOCT)

Phenicia Baatout
Adviser on Security and Technology, Council of the European Union

Ricardo Baeza-Yates
Research Professor, Institute for Experiential AI, Northeastern University

Vincent Bouatou
Deputy Director, Strategic Innovation, IDEMIA

Daniela Buruiana
Seconded National Expert, Eurojust

Raja Chatila
Professor of Robotics, Université Paris Sorbonne

Michaella Chupin
Consultant, OPTIC Technology

Eric Clement
Adviser, Cooperation for Security and Video-Surveillance, French Ministry of Interior

Joesph Courtesis
Inspector (retired) ,New York Police Department

Samuel Curtis
AI Policy Researcher, The Future Society

Agnes Delaborde
Research Engineer in AI and Robotics Evaluation, Laboratoire national de métrologie et d'essais

Benedict Dellot
Head of AI Monitoring, Centre for Data Ethics and Innovation, UK Government

Itiel Dror
Senior Cognitive Neuroscience Researcher, University College London

Jean-Luc Dugelay
Professor of Image Engineering & Security, Eurecom Nice Sophia Antipolis

Zsuzsanna Felkai Janssen
Head of Sector for Migration and DG Coordinator for Artificial Intelligence, European Commission DG HOME

Nicole Foster
Director, AWS Global AI/ML and Canada Public Policy, Amazon

Akvilė Giniotienė
Head of Unit, Cybersecurity and New Technologies Unit, UN Office of Counter-Terrorism (UNOCT)

Hannes Glantschnig
Public Prosecutor, Assistant to the National Member for Austria, Eurojust

Inês Gonçalves Ferreira
Legal and Policy Research Fellow, Centre for AI and Robotics, UNICRI

Patrick Grother
Biometric Standards and Testing Lead, NIST

Ben Hayes
Director, AWO Agency

Bruce Hedin
Principal Scientist, H5

Gabor Ivanics
Cyber Taskforce Lead, Eurojust

Sylvia Jamgotchian
Policy Analyst, Office of the Executive Director, INTERPOL

Ameen Jauhar
Lawyer and Social Policy Researcher, Senior Resident Fellow, Vidhi Centre for Legal Policy – India

Rozemarijn Jens
Research Fellow, Centre for AI and Robotics, UNICRI

Aglika Klayn
EC3 J-CAT Coordinator, EUROPOL

Brenda Leong
Senior Counsel & Director of Artificial Intelligence and Ethics, The Future of Privacy Forum

Ruth Linden
Policy Adviser, EUROPOL

Teresa Magno
Investigative/Trial Judge, Assistant to the National Member for Italy, Eurojust

Apostolos Malatras
Team Leader, Knowledge and Information, European Union Agency for Cybersecurity (ENISA)

Alex Moorehead
Human Rights Officer, UN Office of the High Commissioner for Human Rights (OHCHR)

Jean-Philippe Morange
Senior Legal Officer, Counter-Terrorism Executive Directorate (CTED)

Johanna Morley
Face Examiner, Forensics and Police Data Management Sub-Directorate, INTERPOL

Gregory Mounier
Head of Team, Innovation Lab, EUROPOL

Michael O'Connell
Managing Director, Critical Insights Consultancy

Irina Orssich
Team Leader Artificial Intelligence – Technologies and Systems for Digitising Industry, European Commission DG CONNECT

Claire Poirson
Lawyer, Bersay Avocats

Emmanuel Saliot
Adviser on Security and Technology, Council of the European Union

Eric Salobir
President, OPTIC Technology

Sylvester Sammie
Human Rights Officer, UN Office of Counter-Terrorism (UNOCT)

Cristina San Juan
Consultant, UN Office on Drugs and Crime (UNODC)

Anne-Maria Seesmaa
Associate Legal Officer, Counter-Terrorism Executive Directorate (CTED)

Elisabeth Sellos-Cartel
Deputy Director, Cooperation for Security and Video-Surveillance, French Ministry of Interior

Jessica Smith
Deputy Director, Centre for Data Ethics and Innovation – UK Government

Roberta Solis
Crime Prevention and Criminal Justice Officer, UN Office on Drugs and Crime (UNODC)

Melissa Taylor
Special Programs Office, NIST

Luc Tombal
Director, Defence and Security, Sopra-Steria

Jai Vipra
Senior Resident Fellow, Vidhi Centre for Legal Policy – India

Editing and Design

Sophie Ebbage
Designer, Studio Miko

Alison Moore
Editor, Astra Content

Endnotes

1. World Economic Forum, *A Framework for Responsible Limits on Facial Recognition: Use Case: Flow Management*, 2020: https://www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management (link as of 16/8/21).
2. World Economic Forum, *Responsible Limits on Facial Recognition: Use Case: Flow Management – Part II*, 2020: https://www.weforum.org/whitepapers/responsible-limits-on-facial-recognition-use-case-flow-management (link as of 16/8/21).
3. NISTIR 8280, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2019: https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects (link as of 16/8/21).
4. Bobby Allyn, "'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man", npr, 24 June 2020: https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig (link as of 18/8/21).
5. ACLU, *The Dawn of Robot Surveillance: AI, Video Analytics and Privacy*, 2019: https://www.aclu.org/report/dawn-robot-surveillance (link as of 16/8/21).
6. Kate Conger, Richard Fausset and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology", New York Times, 14 May 2019: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (link as of 5/10/22).
7. Sarah Ravani, "Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns", San Francisco Chronicle, 16 July 2019: https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php (link as of 5/10/22).
8. Ally Jarmanning, "Boston Lawmakers Vote to Ban Use of Facial Recognition Technology by the City", npr, 24 June 2020: https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city (link as of 5/10/22).
9. Madison Booth, "Senate Passes Bill Limiting Use of AI by Law Enforcement", Alabama Daily News, 2 February 2022: https://www.aldailynews.com/senate-passes-bill-limiting-use-of-ai-by-law-enforcement/ (link as of 5/10/22).
10. Hannah Metzger, "Task Force to Assess Use of Facial Recognition by Colorado Law Enforcement, Government", Colorado Politics, 9 June 2022: https://www.coloradopolitics.com/legislature/task-force-to-assess-use-of-facial-recognition-by-colorado-law-enforcement-government/article_52846144-e83e-11ec-b930-7fe52b4e1214.html (link as of 5/10/22).
11. ACLU, "Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country", press release, 30 June 2021: https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country (link as of 5/10/22).
12. Emma Peaslee, "Massachusetts Pioneers Rules for Police Use of Facial Recognition Tech", npr, 7 May 2021: https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech?t=1623343113224 (link as of 16/8/21).
13. Bill Atkinson, "Virginia to Enact Statewide Ban on Facial Recognition Use", Government Technology, 9 April 2021: https://www.govtech.com/public-safety/virginia-to-enact-statewide-ban-on-facial-recognition-use.html (link as of 16/8/21).
14. Monica Nickelsburg, "Washington State Passes Landmark Facial Recognition Bill, Reining in Government Use of AI", GeekWire, 13 March 2020: https://www.geekwire.com/2020/washington-state-passes-landmark-facial-recognition-bill-reining-government-use-ai/ (link as of 16/8/21).
15. iapp, "Will There Be Federal Facial Recognition Regulation in the US?", 11 February 2021: https://iapp.org/news/a/u-s-facial-recognition-roundup/ (link as of 16/8/21).
16. United States Congressman Ted W. Lieu (D-Los Angeles County), "Reps Ted Lieu, Sheila Jackson Lee, Yvette Clarke, and Jimmy Gomez Introduce Bill to Regulate Law Enforcement Use of Facial Recognition Technology", Press Release, 29 September 2022 : https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce (link as of 5/10/22).
17. Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", The New York Times, 18 January 2020: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (link as of 30/9/2022).
18. Rebecca Heilweil, "Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress", Vox, 11 June 2020: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police (link as of 16/8/21).
19. Sarah Bird, "Responsible AI Investments and Safeguards for Facial Recognition", Microsoft, 21 June 2022: https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition/ (link as of 23/08/2022).
20. Amazon, "We Are Implementing a One-Year Moratorium on Police Use of Rekognition", 10 June 2020: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition (link as of 16/8/21).
21. EUR-Lex, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence*, 21 April 2021: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (link as of 16/8/21).

22. Jorge Liboreiro, "'The Higher the Risk, the Stricter the Rule': Brussels' New Draft Rules on Artificial Intelligence", Euronews, 21 April, 2021: https://www.euronews.com/2021/04/21/the-higher-the-risk-the-stricter-the-rule-brussels-new-draft-rules-on-artificial-intellige (link as of 16/8/21).

23. United Nations, "Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet", 15 September 2021: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469 (link as of 12/8/2022).

24. accessnow, "Privacy Win for 350,000 People in São Paulo: Court Blocks Facial Recognition Cameras in Metro", 12 May 2021: https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/ (link as of 16/8/21).

25. Royal Court of Justice, "In the Court of Appeal (Civil Division) on Appeal from the High Court of Justice of Queen's Bench Division (Administrative Court)", Case No. C1/2019/2670: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf (link as of 12/8/2022).

26. Rijksoverheid, "Letter of the Minister of Justice and Security of the Netherlands to MPs to Inform Them About the Use of Facial Recognition Technology by Law Enforcement Agencies" (in Dutch), 20 November 2019: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/11/20/tk-waarborgen-en-kaders-bij-gebruik-gezichtsherkenningstechnologie (link as of 16/8/21).

27. Chatham House, "Chatham House Rule": https://www.chathamhouse.org/about-us/chatham-house-rule (link as of 16/8/21).

28. In law enforcement, there exist instances in which "one to one" also relates to identification activity; for example, in disputed identity cases or where an image is compared in a case with a possible suspect.

29. While these arrangements are used by the Netherlands Police and INTERPOL for the performance of facial analysis, other models exist. Alternative models were seen over the course of the pilot phase of the project.

30. As noted, the described process is informed by the practices of the Netherlands. However, different agencies may follow slightly different processes in practice. With respect to blind peer reviews, for instance, at INTERPOL these are performed by only one other expert.

31. INTERPOL, "Yellow Notices": https://www.interpol.int/How-we-work/Notices/Yellow-Notices (link as of 11/10/22).

32. Ministry of Women and Child Development, Government of India, National Tracking System for Missing & Vulnerable Children: https://trackthemissingchild.gov.in/ (link as of 1/9/22).

33. INTERPOL, "Red Notices": https://www.interpol.int/How-we-work/Notices/Red-Notices (link as of 16/8/21).

34. Definitions extracted from "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts", 21 April 2021: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN (link as of 18/8/21).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org