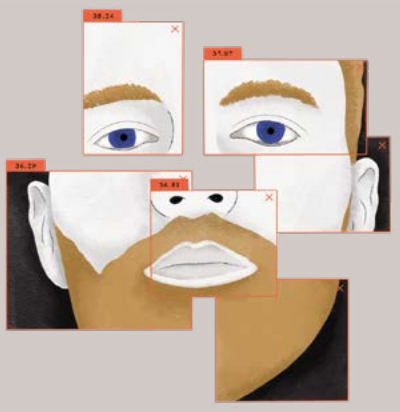
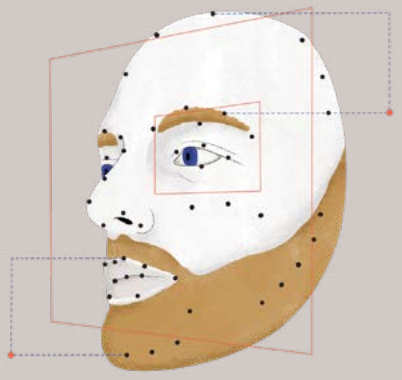
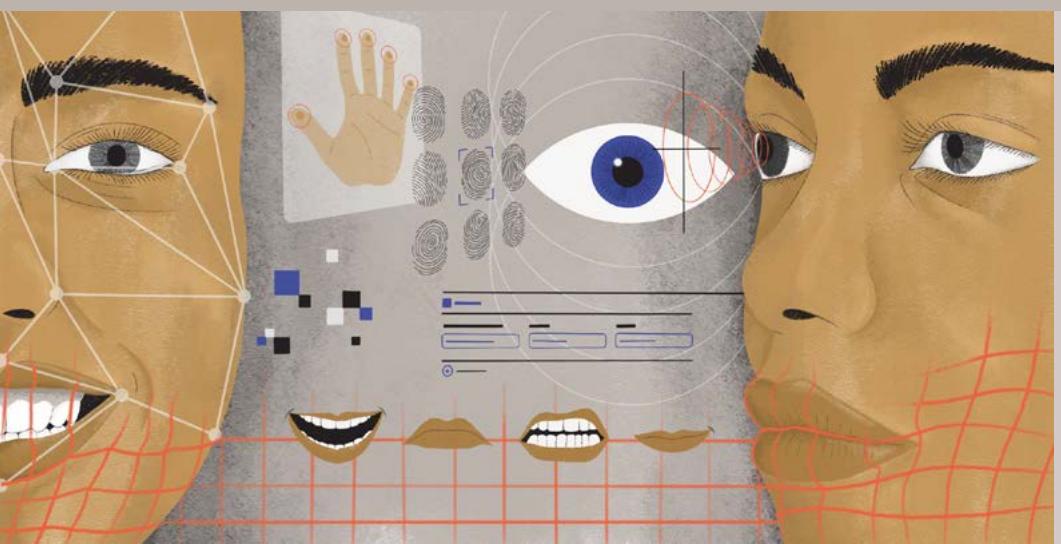




THE PRINCIPLES

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

Principles to reduce the human rights harms of facial recognition technology



INCLO

INCLO principles on law enforcement use of FRT

Our principles do not endorse police use of FRT but instead highlight the bare minimum standards for accountability and harm mitigation where it exists. They serve as a tool to build consensus on the severe risks posed by FRT and the urgent need for strict restrictions and outright bans.

These principles are designed to address:

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

THE PRINCIPLES

1. Law enforcement authorities must not use FRT without a specific legal basis.
2. Fundamental rights impact assessments should be mandatory.
3. Fundamental rights impact assessments must be independent of vendor assessment.
4. There should be no acquisition or deployment of any new FRT without a guarantee of future independence from the vendor.
5. All versions of all assessments must be made public before FRT deployment.
6. Public consultation should be obligatory.
7. Authorities must inform the public how probe images are used in an FRT operation.
8. The technical specifications of any FRT system must be made public before deployment.
9. Live FRT is prohibited.
10. Prior judicial authorization should be mandatory.
11. Authorities must document each retrospective or operator-initiated FRT search.
12. An FRT result alone is not a sufficient basis for questioning, arrest or detention.
13. Disclosure of the details of the FRT operation applied against individuals should be mandatory.
14. Any FRT misidentification of a person must be reported.
15. Annual reporting by authorities of misidentifications should be mandatory.
16. An independent FRT oversight body must be established before any deployment of FRT.
17. That independent FRT oversight body must publish annual reports.
18. Impact assessments must be made available to the oversight body before the system is deployed.

Use of FRT

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

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

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

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

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

LEGAL BASIS

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

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

- The specific parameters of its use, including whether it is retrospective or operator-initiated, who will use it, who it will be used against, where it will be used, why it will be used and how it will be used;

- The rights impacted, in particular rights to privacy, protection of personal data, freedom of expression and peaceful assembly, and non-discrimination;
- The nature and extent of the risks to those rights;
- How each of those risks will be mitigated;
- A demonstrated justification for how and why the benefits of the deployment will outweigh the rights' impacts; and
- The remedy available to someone who is misidentified[1] or whose biometric data was processed when it should not have been.

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

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

Illustration by Alina Nailis - © 2024 INCLO

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

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

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

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

NON-EXCLUSION OF LEGAL BASIS

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

VENDOR LOCK-IN RISK ASSESSMENT

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

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

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

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

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

PUBLICATION OF RISK ASSESSMENT RESULTS

PRINCIPLE 5: All versions of all assessments, including strict necessity and proportionality assessments and human rights impact assessments,[2] carried out prior to any FRT deployment, and their results, must be made public prior to FRT deployment in a manner that maximizes public reach, especially among the people most likely to be subjected to the specific FRT use.

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

PUBLIC CONSULTATION

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

- Details about how the technology and system work in an explainable and accessible manner;
- Details about the parameters of the authorities' expected use within the respective jurisdiction, including the strict conditions under which the system is used;
- Details of the images used as probe images, and any devices through which they are captured;
- Details of the images featuring on all reference databases;
- Demographic data of those who are expected to be subjected to the use of the system;
- All written impact assessments required under these principles; and
- Details of the safeguards in place to prevent arbitrary use of the system.

Meaningful public consultation also requires:

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

PROBE IMAGE

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

- The criteria necessary for a person's image to become a probe image;
- The sources of probe images;

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

TECHNICAL SPECIFICATIONS AND POLICIES MADE PUBLIC

PRINCIPLE 8: Before any deployment of FRT by a law enforcement authority, the authority must make public details of the technical specifications of any FRT system it plans to use in a clear, intelligible manner. These details must include, but not be limited to:

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

3. How many images are in the database;
4. How the images are obtained;
5. How long the images stored are kept in the database;
6. How often the database is purged;
7. The process for having images removed from the database;
8. Who has access to the database and when / under what circumstances;
9. How the database is maintained;
10. The identity of the person/unit who is responsible for the maintenance and oversight of the database;
11. The privacy and data protection policy for the database;
12. How the law enforcement authority will assess and demonstrate that the creation of the reference database, or the addition of a person to the reference database, is necessary and proportionate; and
13. The criteria for a person's inclusion in the reference database.

BANNED USES

PRINCIPLE 9: No FRT system will be used on live or recorded moving images or video data.[3]

PRIOR JUDICIAL AUTHORIZATION

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

Any law enforcement officer carrying out a retrospective FRT search must be independent of the investigation of the offence, and any law enforcement officer

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

using FRT must have completed training, which will be updated annually. This training must focus on how to use the relevant system, how to assess the human rights impacts of using the system, how to determine whether use is strictly necessary and proportionate and how to fully comply with the law underpinning the use of FRT.

RECORD OF USE

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

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

- The total number of FRT search requests;
- The total number of FRT search requests that generated leads;
- The number of FRT searches whereby an arrest or charges followed;
- The number of FRT misidentifications;4
- The number of individuals who appeared as a possible match in the FRT search and who were subsequently questioned, arrested and/or charged;
- The demographic breakdown of individuals in probe photos by race and gender; and
- Information about the FRT system and algorithm(s) used, including vendor, version, similarity threshold and whether the similarity threshold was adjusted for the specific search.

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

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

PROHIBITION OF ACTION

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

4 As defined in the footnote to Principle 2.

OBLIGATION TO DISCLOSE

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

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

- A copy of the complete candidate list returned by the FRT system, in rank order and including the similarity score assigned to each image by the FRT system;
- The written report produced by the person who ran the FRT search, including the date, time of the search and any notes made about the possible match relative to any other individuals on the candidate list; and
- The name and training, certifications or qualifications of the person who ran the probe image in an FRT search.

REPORT OF MISIDENTIFICATION

PRINCIPLE 14: Any FRT misidentification[5] of a person must be reported to the person by the law enforcement authority as soon as possible after the misidentification is discovered and recorded.

ANNUAL REPORTING ON MISIDENTIFICATIONS

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

INDEPENDENT OVERSIGHT BODY

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

- Be established and regulated by law;
- Be separate to, and independent of, the executive authority or respective state;

5 As defined in the footnote to Principle 2.

- Have the necessary funds, skills, expertise and staff – legal and technological – to fulfil its responsibilities;
- Have free and immediate access to the necessary information it needs to carry out its work;
- Report annually to the public about its work and findings; and
- Report annually to the country's parliament.

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

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

ANNUAL REPORT BY INDEPENDENT OVERSIGHT BODY

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

- A detailed assessment of, and comment on, law enforcement's stated legal basis for the use of FRT;
- The number of individual probe images used in FRT searches;
- The number of images used in reference and databases;
- The number of true matches and false positives per deployment;
- The number of arrests per deployment;
- The number of stop and searches per deployment;
- The total number of FRT use requests made;
- The total number of FRT deployments;
- The number of requests made or searches performed pursuant to judicial authorization;
- The number of emergency requests made or deployments performed; and

- The reasons for requesting the search, including, but not limited to, any underlying suspected crime.

PRIOR NOTIFICATION OF IMPACT ASSESSMENTS TO OVERSIGHT BODY

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

Closing words

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

Acknowledgements

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

These principles were designed following INCLO's 2023 yearly meeting when the widespread lack of technical and legal expertise regarding police use of FRT was identified as a pressing concern across all member jurisdictions. Human rights specialists from the fields of law, technology, sociology, and communication across the 15 INCLO countries came together throughout 2023 and 2024 to develop this list of principles.

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

INCLO credits Taryn McKay for design, Sam Kelly for edits and Alina Najlis for illustrations.

Read the full report at inclo.net/frt