

CANADIAN
CIVIL LIBERTIES
ASSOCIATION



ASSOCIATION
CANADIENNE DES
LIBERTÉS CIVILES



Toxic Surveillance: The Human Rights Impacts of Facial Recognition Technology (FRT) in Countering Terrorism

29 August 2025

Inputs from 11 INCLO members for the preparation of the United Nations Special Rapporteur's 2025 Position Paper on the Human Rights Impacts of Using Artificial Intelligence (AI) in Countering Terrorism, including guidance on good practices.

A. Introduction

The International Network of Civil Liberties Organisations (INCLO) is a network of 17 civil liberties and human rights organizations from around the globe.¹ We would like to thank the United Nations Special Rapporteur on counter-terrorism and human rights for the opportunity to provide input for the preparation of this Position Paper on the Human Rights Impacts of Using Artificial Intelligence (AI) in Countering Terrorism, including guidance on good practices.²

Drawing from the research carried out by INCLO members in respect of law enforcement use of Facial Recognition Technology (FRT) titled *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition*³, this submission addresses the human rights implications of AI in

¹ Participating members from INCLO include: Al-Haq in Palestine, Canadian Civil Liberties Association (CCLA); Centro de Estudios Legales y Sociales (CELS) in Argentina; Conectas Direitos Humanos in Brazil; Egyptian Initiative for Personal Rights (EIPR); Human Rights Law Network (HRLN) in India; Hungarian Civil Liberties Union (HCLU); Irish Council for Civil Liberties (ICCL); Kenya Human Rights Commission (KHRC); KontraS in Indonesia; and Legal Resources Centre (LRC) in South Africa.

² Call for Input – Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism, <https://www.ohchr.org/en/calls-for-input/2025/call-input-position-paper-human-rights-impacts-using-artificial-intelligence>

³ INCLO, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition*, February 2025, <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/>

countering terrorism, particularly where biometric surveillance tools like FRT are deployed. The submission outlines key risks, safeguards, and recommendations rooted in INCLC's commitment to rights-based technology governance.

FRT is a flawed but very powerful “toxic”⁴ form of biometric AI that is used to attempt to identify or characterize a person on the basis of their facial features.⁵ FRT is traditionally used as a surveillance tool, such as in countering terrorism, for identification. The goal of FRT-based identification is to determine the identity of an unknown individual whose face is captured on a picture or video by comparing the image of the unknown person against a reference database of images of known people. It can also be referred to as “one-to-many identification”. INCLC's principles are focused on this type of use of FRT-based surveillance systems. The system can be used in real-time or retrospectively.

Real-time or live facial recognition involves an algorithm comparing a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert for police, or a user of the FRT system, to potentially act upon instantaneously, near-instantaneously or without a significant delay. When used retrospectively, an FRT algorithm compares still images of faces of unknown people against a reference image database of known people in order to attempt to identify those unknown. When used retrospectively, the system returns a list of potential candidates accompanied by similarity scores. There is no guarantee that the person whose identity is being sought will be in the reference database; or that, if the ‘true match’ is in the reference database, that they will be featured at the top of the candidate list accompanied by the greatest similarity score;⁶ nor is there any guarantee that the person running the FRT search will choose the correct candidate, if they are indeed returned in the candidate list at all.⁷ For a retrospective FRT system to work, a threshold value is fixed to determine when the software will indicate that a probable match has occurred. Should this value be fixed too low or too high, respectively, it can create a high false positive rate (i.e. the percentage of incorrect matches identified by the technology) or a high false negative rate (i.e. the percentage of true matches that are not detected by the software).

⁴ Irish Council for Civil Liberties, Leading experts warn against Garda use of FRT, October 2023, <https://www.iccl.ie/digital-data/leading-facial-recognition-technology-experts-have-warned-against-garda-use-of-frt-saying-use-of-the-toxic-tool-would-result-in-a-massive-step-change-in-police-sur/>

⁵ Raviv, S, The Secret History of Facial Recognition, Wired, 21 January 2020, <https://www.wired.com/story/secret-history-facial-recognition/>.

⁶ Press, E., Does A.I. Lead Police to Ignore Contradictory Evidence? New Yorker, November 2023, Robert Williams was wrongfully arrested in front of his wife and children, detained and arraigned by Detroit police after they used FRT to try to identify a shoplifter who stole a watch. The image of Williams was only the ninth most likely match for the probe photograph, which was obtained from surveillance video of the incident. But the analyst who ran the search did an assessment and decided Williams' image was the most similar to the suspect's. Two other algorithms were then run. In one, which returned 243 results, Williams wasn't even on the candidate list. In the other—of an F.B.I. database—the probe photograph generated no results at all, <https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence>

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

There is no single threshold setting which eliminates all errors.⁸ The multiple components of an FRT system, together with the steps involved in the working of such a system, and the multitudinous outside factors which can affect the performance of that system, makes attempts to identify a person with FRT a probabilistic, and therefore a deeply problematic, endeavour.⁹ These issues are further compounded by the fact that existing FRT accuracy tests do not account for the many variables characterizing real-world police use of FRT.¹⁰

Assessing the use of FRT in counter-terrorism illustrates the broader human rights risks posed by AI in security contexts. For example, UN experts and Committees have expressed profound concern “about the indiscriminate loss of life apparently caused by [Israel’s] artificial intelligence-enhanced targeting systems, especially when combined with the use of explosive weapons with wide-area effects.”¹¹ This is further epitomised in the recently revealed practices of the Israeli military in the Occupied Palestinian Territory who employed AI to allow Israeli forces “to play back the content of cellular calls made by Palestinians” whose calls it had intercepted en masse in total disregard for Palestinian human rights.¹² The surveillance data is reportedly stored at Microsoft datacentres in the Netherlands and Ireland.¹³

As a probabilistic and error-prone biometric surveillance tool, FRT raises serious concerns. FRT’s systemic flaws, coupled with the opaque nature of AI-driven decision-making and lack of adequate oversight or remedy, make FRT a particularly dangerous technology when deployed under broad counter-terrorism mandates. INCLO’s research demonstrates that such deployments often lack necessity and proportionality, and instead contribute to discriminatory and unlawful surveillance practices that undermine human rights and democratic freedoms.

⁸ Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., *Facial Recognition Technologies: A Primer*, May 29, 2020.

⁹ Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., *Facial Recognition Technologies: A Primer*, May 29, 2020.

¹⁰ Garvie, C., *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations* at 15–16, Geo. L. Ctr. on Privacy & Tech. (2022), <https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/>

¹¹ Gaza: UN experts deplore use of purported AI to commit ‘domicide’ in Gaza, call for reparative approach to rebuilding, 15 April 2024 <https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call>; A/79/363: Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories, 20 September 2024 <https://www.ohchr.org/en/documents/thematic-reports/a79363-report-special-committee-investigate-israeli-practices-affecting>.

¹² Harry Davies and Yuval Abraham, “A million calls an hour”: Israel relying on Microsoft cloud for expansive surveillance of Palestinians’ *The Guardian* (London, 6 August 2025) <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>

¹³ Harry Davies and Yuval Abraham, “A million calls an hour”: Israel relying on Microsoft cloud for expansive surveillance of Palestinians’ *The Guardian* (London, 6 August 2025) <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>

B. Key Questions

1. How does the use of AI in countering terrorism affect human rights? Which rights are impacted? Which specific applications of AI in efforts to counter terrorism pose the greatest risks to human rights?

The use of AI, particularly biometric technologies like FRT, in countering terrorism risks significantly affecting a range of fundamental human rights. Some of the rights directly impacted include the right to privacy, freedom of expression and assembly, equality and non-discrimination, freedom of movement, due process, and the right to an effective remedy.

The degree of impact on these rights depends on various contextual factors depending on individual use case of an FRT system, including the design and architecture of the AI system, the training data used, the accuracy and bias of the underlying algorithms, and the purpose and method of deployment, such as real-time surveillance versus retrospective identification.¹⁴

FRT exemplifies high-risk applications of AI in counter-terrorism due to its invasive nature and flawed accuracy, especially when used in live public surveillance or in retrospective policing investigations. These applications raise serious concerns when used without transparency, legal safeguards, or accountability mechanisms. The probabilistic nature of FRT means it can never guarantee correct identification, and inaccuracies are more likely to affect already marginalized or racialized communities. While states are permitted to interfere with rights in pursuit of legitimate aims such as national security, such interference must be necessary, proportionate, and the least rights-intrusive means available. In practice, however, AI-driven tools like FRT are often deployed without meeting these human rights standards, resulting in overreach and potential abuse, particularly in jurisdictions with weak legal protections or oversight. As such, these technologies, if unchecked, risk eroding the very rights they purport to protect.

AI in counter-terrorism affects a wide range of human rights, including:

Right to privacy: The right to privacy¹⁵, including a reasonable expectation of privacy while in public, is recognised as a ‘gateway’ right, given it enables the realization of other rights. AI-driven surveillance, especially facial recognition in public spaces, erodes anonymity and chills lawful conduct.

Freedom of expression and association: FRT and behavioral profiling are deployed at protests and public gatherings, leading to self-censorship and deterring civic participation.

¹⁴ Raposo, V.L. When facial recognition does not ‘recognise’: erroneous identifications and resulting liabilities. *AI & Soc* 39, 1857–1869 (2024). <https://doi.org/10.1007/s00146-023-01634-z>

¹⁵ Article 17, International Covenant on Civil and Political Rights, “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.”

<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

Right to equality and non-discrimination: AI systems trained on biased data disproportionately misidentify or target racial and ethnic minorities, migrants, and other marginalized groups.

Right to due process and a fair trial: Opaque decision-making and lack of explainability in AI systems challenge individuals' ability to understand or contest actions taken against them.

Right to an effective remedy: Victims of AI-enabled harm often face significant barriers in accessing justice due to lack of transparency and redress mechanisms. It is unclear what happens in most jurisdictions when an FRT system misidentifies an innocent person, or when a person is wrongfully arrested or treated and subjected to a decision based solely on automated processing and which produces an adverse legal effect on them.

High-risk applications include:

- Identification of individuals of interest
- Real-time facial recognition in public spaces

2. What key principles and safeguards should apply to the use of AI in countering terrorism to ensure the timely and effective protection of human rights? How do States and private entities' roles differ in their responsibilities?

INCLO members generally oppose the use of FRT by law enforcement due to the fundamental rights risks involved. Should a jurisdiction create a legal basis for a law enforcement authority to use FRT, it must include, at a minimum, a significant number of robust safeguards enshrined in law.¹⁶

No live use: No FRT system will be used on live or recorded moving images or video data.¹⁷

Authorized by Law: AI should not be used through FRT in countering terrorism, unless and until it is first 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.¹⁸

Legal Basis: The legal basis for the use of AI through 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 in its use for counter-terrorism. 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. Bulk or indiscriminate surveillance is incompatible with human rights norms.

¹⁶ As detailed in pages 48-60 of the report

¹⁷ INCLO FRT Principle 9, pg. 55

¹⁸ INCLO FRT Principle 1, pg. 49-50

Any assessment of the strict necessity and proportionality of the FRT use must detail the necessity of the deployment for the stated objective.¹⁹

Vendor Lock-in risk assessment: Before any FRT system is acquired or deployed there must be a prior assessment of vendor lock-in risk by the authority to use the system. The procurement of FRT systems should favour vendor offers that maximize open standards and interoperability and minimize proprietary components. The authority to use the system must fully understand how the technology and the system works.

Prohibition of action: A law enforcement officer should not question, arrest, detain or take any action against an individual on the basis of FRT use alone. An FRT result should only serve as an investigative lead. It is not reliable evidence, and any FRT result must be followed by independent reliable investigative actions before any further action.²⁰

Transparency: Affected individuals must be informed when and how AI is used, and public authorities should publish regular transparency reports.²¹

Human Oversight and Accountability: Decisions with legal or serious consequences must be subject to meaningful human review. Oversight bodies must have the power to audit systems and hold actors accountable.²²

Equality and Non-Discrimination: Robust pre-deployment and ongoing audits must test for disparate impact on protected groups. Tools that reinforce or amplify structural bias should be prohibited.

Redress and Remedies: Accessible grievance mechanisms must be established, and individuals must have the right to challenge surveillance or profiling practices.

The roles of States and Private entities in ensuring timely and effective protection of human rights in the use of AI through FRT differs slightly. States and its agencies bear primary responsibility for ensuring compliance with international human rights law. Private entities are involved both as users and vendors or suppliers of these technologies. As users, their use of FRT raises the same human rights risks outlined and, therefore, must be obliged to comply with the same safeguards and within the same limitations.

As vendors, companies tend to present their systems packed into “global solutions” and are presented as “what is needed” without a clear explanation about how such a solution works and why the solution must be acquired as a whole. These practices can lead to a user or buyer becoming dependent on a vendor. For that reason, we take the position that authorities must not acquire or deploy any new FRT without a prior assessment of vendor lock-in risk, including, but not limited to:

¹⁹ INCLO FRT Principle 2, pg. 50-51

²⁰ INCLO FRT Principle 12, pg. 57

²¹ INCLO FRT Principles 14, & 15, pg. 59

²² INCLO FRT Principles 16, 17, & 18, pg. 59-60

- An evaluation of the interoperability and compatibility with current existing systems;
- A data ownership and portability assessment, evaluating the costs of migrating the 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 favor vendor offers that maximize open standards and interoperability and minimize proprietary components, while a duty must be placed on vendors to explain, in plain language, how a specific FRT system works, and a duty on the authority to fully understand how the technology and the system works.

3. Do existing guidelines, legislation and regulatory mechanisms prove effective in ensuring human oversight? Is there a need for a dedicated mechanism for AI in counter-terrorism?

With respect to the use of AI through FRT deployment, there is often a lag in regulatory or policy responses compared to the pace of technological deployment. INCLO's research shows widespread lack of transparency, absence of independent oversight, and inadequate safeguards for due process and equality in the use of FRT. This will only trickle down in the adoption of AI through the use of FRT for counter-terrorism.

In the UK, the office of the Biometrics and Surveillance Camera Commissioner continues to exist, but oversight is currently fragmented, with an interim Biometrics Commissioner, while the Surveillance Camera Commissioner role remains vacant and no permanent appointment has yet been made.²³ Proposed reforms, including the repeal of the Surveillance Code of Practice, under the now-stalled Data Protection and Digital Information (DPDI) Bill, has led to concerns that there will be "vulnerabilities for users of technologies and for the rights of individuals subject to them"²⁴ and, in the absence of a clear plan for how the Commissioner's functions will be replaced, risks there being more rather than less regulatory complexity. In the US, there have been calls for a regulatory office to oversee the management and regulation of complex technologies such as FRT, similar to how the pharmaceutical industry is regulated²⁵ and, similarly, an independent body charged with certifying policing technologies before they are

²³ Chris Burt, 'UK chooses stop-gap biometrics oversight, leaves surveillance camera role empty' (*Biometric Update*, July 2, 2025)

<https://www.biometricupdate.com/202507/uk-chooses-stop-gap-biometrics-oversight-leaves-surveillance-camera-role-empty>

²⁴ Fussey, P., and Webster, W., Independent report on changes to the functions of the Biometrics and Surveillance Camera Commissioner arising from the Data Protection and Digital Information (No.2) Bill, Centre for Research Into Information, Surveillance and Privacy, p.6, October 2023,

https://assets.publishing.service.gov.uk/media/653f7128e6c968000daa9cae/Changes_to_the_functions_of_the_BSCC.pdf

²⁵ Facial Recognition Technologies in the Wild: A Call for A Federal Office, Erik Learned-Miller, Vicente Ordóñez, Jamie Morgenstern, and Joy Buolamwini, May 29, 2020,

https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf

deployed.²⁶ The U.S. Commission on Civil Rights in a 2024 report confirmed that no federal laws currently expressly regulate FRT, and no constitutional safeguards specifically govern its use.²⁷ We take note of the bill, Facial Recognition Act of 2025 introduced in July 2025, which is still before congress for consideration.²⁸ In Canada, the Office of the Privacy Commissioner of Canada has issued regulatory guidance on police use of FRT, but this guidance is not legally enforceable.²⁹

Similarly, the Office of the Australian Information Commissioner (OAIC) is the main regulatory body with privacy-related jurisdiction at the federal level in Australia. Each State and Territory also has its own body responsible for privacy regulation. The OAIC has the power to conduct investigations into acts or practices that may breach the Privacy Act and to conduct privacy assessments to determine whether entities are maintaining and handling personal information in accordance with the Privacy Act. But the OAIC has moderate efficacy in upholding the rights engaged by FRT.

The use of AI through FRT for counter-terrorism presents urgent risks that are not addressed by current legislative frameworks. There is the need for a dedicated mechanism to address all these risks that are apparent with the use of such technologies. These mechanisms would, among other things, define appropriate and lawful uses of AI in counter-terrorism, protect fundamental rights, ensure transparency, oversight, and accountability.

4. How can due diligence, including human rights impact assessments, be integrated into the AI lifecycle?

INCLO supports mandatory, ongoing human rights impact assessments (HRIAs) at different stages of the deployment of FRT for counter-terrorism. Before deployment, the responsible authority must assess the system's legality, necessity, proportionality, and potential discriminatory impact.³⁰ During deployment, the system should be monitored in real-world use, with particular attention to its impact on marginalized groups. Facial recognition systems operate in real-life scenarios and do not reflect laboratory conditions. Flaws in the datasets reference databases/watchlists and probe images result in limited accuracy, which can lead to huge fundamental rights violations. After deployment, auditing of outcomes, accountability reporting, and a clear process for discontinuation are required if the system perpetuates harm.³¹

²⁶ 75 Friedman, Barry and Heydari, Farhang and Isaacs, Max and Kinsey, Katie, Policing Police Tech: A Soft Law Solution (June 1, 2022). Berkeley Technology Law Journal, Vol. 37, 2022, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4095484

²⁷ U.S. Commission on Civil Rights Releases Report: The Civil Rights Implications of the Federal Use of Facial Recognition Technology, September 19, 2024, <https://www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial>

²⁸ Facial Recognition Act 2024, H.R.4695, Congress, <https://www.congress.gov/bill/119th-congress/house-bill/4695/text>

²⁹ Privacy regulators call for legal framework limiting police use of facial recognition technology, Office of the Privacy Commissioner in Canada, May 2022, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

³⁰ INCLO FRT Principles 2 & 5, pg. 50-51, 52

³¹ INCLO FRT Principles 11 & 15, pg. 55-57, 59

We believe stakeholder consultation must be integrated into the process of human rights impact assessment to be effective. Members of the communities who would be disproportionately affected by the use of FRT must be consulted.

5. How can the right to equality and non-discrimination be safeguarded?

INCLIO research finds that FRT system errors do not affect all individuals equally. The use of FRT, in particular, for cases such as counter-terrorism, poses an unquestionable risk in relation to the prohibition of discrimination, given the known problems with respect to performance over certain protected characteristics.³² Its application in both real-time and retrospective identification amplifies the risk of misidentification, especially for marginalized groups, due to algorithmic bias and operational inaccuracies. Highly regarded testing shows that face recognition algorithms misidentify Black people, people of color, and women at higher rates. Widely reported testing from the federal agency in the US, the National Institute for Standards and Technology (NIST) in 2019 found FRT algorithms were up to 100 times more likely to misidentify Asian and African American people than white men, and that women and younger individuals were also subject to disparately high misidentification rates.³³ While some reports indicate that demographic differentials in false-match rates have lessened for some algorithms, testing by NIST and academic researchers indicates that the problem persists.³⁴ In addition, some authorities are more likely to apply FRT to marginalized communities which are already

³² Birhane, A., 'The unseen black faces of algorithms' (2022) Nature, <https://www.nature.com/articles/d41586-022-03050-7>

³³ Grother P., et al., U.S. Department of Commerce, National Institute for Standards and Technology, Face Recognition Vendor Test Part 3: Demographic Effects 2–3, 8 (Dec. 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>; See also Harwell, D., Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use, Washington Post, December 19, 2019, <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>.

³⁴ Grother, P., U.S. Department of Commerce, National Institute for Standards and Technology, Facial Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials 15, July 2022, https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf; see also Aman Bhatta et al., The Gender Gap in Face Recognition Accuracy Is a Hairy Problem, Procs of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2023, https://openaccess.thecvf.com/content/WACV2023W/DVPBA/papers/Bhatta_The_Gender_Gap_in_Face_Recognition_Accuracy_Is_a_Hairy_WACVW_2023_paper.pdf; K.S. Krishnapriya et al., Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone, 1 IEEE Transactions on Tech. & Soc'y 8, 2020, <https://ieeexplore.ieee.org/document/9001031>; K.S. Krishnapriya et al., Characterizing the Variability in Face Recognition Accuracy Relative to Race, 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops, April 2019, <https://arxiv.org/abs/1904.07325>; ACLU Comment re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Exec. Order 14074, Section 13(e)), January, 2024, <https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e>

over-surveilled, over-policed and overincarcerated,³⁵ meaning FRT can be used as a tool to create or deepen structural inequalities and discrimination.

To safeguard equality, 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.³⁶

Consultations carried out must include representatives of affected communities in design and evaluation processes. These consultations with disproportionate communities should mandate disclosure about the specific technology used, the manner in which it is used, how the different subsystems and algorithms work, details of the datasets it was trained on and the production of a data protection impact assessment and fundamental rights impact assessment. The consultation should also state how reference databases are created and how watchlists are created.

Authorities must also exclude datasets generated through discriminatory practices such as biased policing, and there must be a mandated disaggregated data analysis to detect disparate impacts.

6. What are the implications of cross-jurisdictional information sharing involving AI?

Cross-border sharing of data and AI-generated outputs in counter-terrorism raises concerns, such as a lack of uniform human rights standards across the jurisdictions, risk of complicity in rights violations (e.g., profiling or extraordinary rendition) and transfer of flawed or biased intelligence between jurisdictions. Cross-border sharing of information has the capacity to bypass safeguards such as the legal basis³⁷ and render some other core principles ineffective, such as the need for judicial authorization and establishment of independent oversight.³⁸ Shared operations could also result in obscurity, undermining the transparency requirement. Furthermore, shared data can perpetuate or amplify biases due to demographic norms.

If cross-jurisdictional sharing must occur involving AI in the use of FRT, then a clear, enforceable privacy and transparency focused legal framework must be put in place, addressing all the issues from a cross-jurisdictional standpoint.

³⁵ Amnesty International, Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid, 2 May 2023, <https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/>

³⁶ INCLO FRT Principle 2, pg. 50-51

³⁷ INCLO FRT Principle 1, pg. 49-50

³⁸ INCLO FRT Principles 10 & 16, pg. 55, 59-60

7. Which instruments regulating the sale and transfer of AI technologies in counter-terrorism support human rights?

We are not aware of any instrument regulating sale and transfer of AI technologies in the form of FRT for the purpose of counter-terrorism that supports human rights.

8. How can marginalized groups be meaningfully included in AI governance related to counter-terrorism?

Principle 6 of INCLO's FRT Report [Eyes on the Watchers: Challenging the Rise of Police Facial Recognition](#) addresses how marginalized groups can be meaningfully included in AI governance related to counter-terrorism in the use of FRT.

Before any 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;
- All written impact assessments mentioned in this submission; and
- Details of the safeguards in place to prevent arbitrary use of the system.

9. How can AI reduce errors and enhance precision in counter-terrorism operations? How should explainability, foreseeability, and transparency be addressed?

In the use of AI through FRT for counter-terrorism, we note the possibility of a high rate of false positives, opacity in black-box systems, undermining accountability, and unpredictable algorithmic behavior, especially in dynamic environments. As a result, our report sets out actions to protect against these possible concerns.

On transparency and explainability, INCLO's FRT Report, [Eyes on the Watchers: Challenging the Rise of Police Facial Recognition](#) mandates that before any FRT system is deployed, the authority making use of such a system must be able to make available details of the technical specifications of the system.³⁹ 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;

³⁹ INCLO FRT Principle 8, pages 53-55

- 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 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.

Furthermore on transparency, authorities must be required to document use of the technology and provide such documentation to the oversight body.⁴⁰ Misidentification should likewise be reported to include the nature, source and impact of the error and any steps taken by the authority in response to the misidentifications.⁴¹

In addressing foreseeability of potential harms, it is compulsory that authorities commission independent impact assessments (not by vendors) to evaluate legality, necessity, proportionality, and discriminatory effects.⁴² These assessments must be shared with oversight bodies.⁴³ This ensures that systems are thoroughly vetted for accuracy and human rights implications ahead of deployment.

⁴⁰ INCLO FRT Principle 11, pg. 55-57

⁴¹ INCLO FRT Principle 15, pg. 59

⁴² INCLO FRT Principle 2, pg. 50-51

⁴³ INCLO FRT Principle 18, pg. 60

We also take the position that, “An FRT result alone is not a sufficient basis for questioning, arrest or detention.”⁴⁴ This is an important point to ensure that AI outputs do not autonomously drive enforcement decisions.

In essence, we urge that only fully explainable and auditable systems be deployed; individuals should be given clear and comprehensible information about how decisions are made; real-world accuracy and bias testing should be continually carried out; and these examinations should be submitted for oversight review prior to deployment.

10. How can effective remedies be ensured for AI-enabled rights violations?

Accessing redress for harms caused by FRT is extremely challenging, especially when individuals are unaware of the technology’s deployment or its errors. This accounts for why we continually advocate for several mechanisms aimed at remedy, accountability, and transparency, which are the bases for effective remedies.

The first step, to ensure effective remedy for harm caused by use of AI tools through the use of FRT, is to mandate authorities to properly document their use of the technology.⁴⁵ This will create an audit trail, allowing individuals or oversight bodies to trace when and how FRT was used. The next phase is adequate reporting and disclosure, which is tied to transparency. With this in place, an independent oversight mechanism can allow for proper investigation, adjudication and issuance of enforceable recommendations. Collectively, these actions would build a system capable of acknowledging harm, enabling redress, and preventing the recurrence of harm.

C. Conclusion

The use of AI in counter-terrorism, particularly through biometric surveillance technologies such as FRT, poses serious and well-documented threats to fundamental human rights. INCLO’s research demonstrates that these technologies are frequently deployed without sufficient legal basis, transparency, oversight, or accountability thereby undermining privacy, equality, due process, and public trust.⁴⁶ Given their probabilistic and error-prone nature, AI systems like FRT are not fit for high-stakes environments unless subject to strict limitations and robust safeguards.

To ensure AI is governed in a manner consistent with international human rights law, states must adopt enforceable legal frameworks that include independent oversight, mandatory human rights impact assessments, transparency obligations, and meaningful public consultation, especially with communities most likely to be affected. We believe that no AI-enabled tool should be used in counter-terrorism unless its deployment meets the standards of legality, necessity, and proportionality, and unless it demonstrably avoids discriminatory harm.

⁴⁴ INCLO FRT Principle 12, pg. 57

⁴⁵ INCLO FRT Principle 11, pg. 55-57

⁴⁶ INCLO’s FRT Report *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition* <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/>

INCLC urges the United Nations and Member States to adopt a precautionary, rights-based approach to AI in counter-terrorism, one that prioritizes human dignity, strengthens democratic accountability, and safeguards the rights of all, particularly those most vulnerable to state surveillance and abuse.