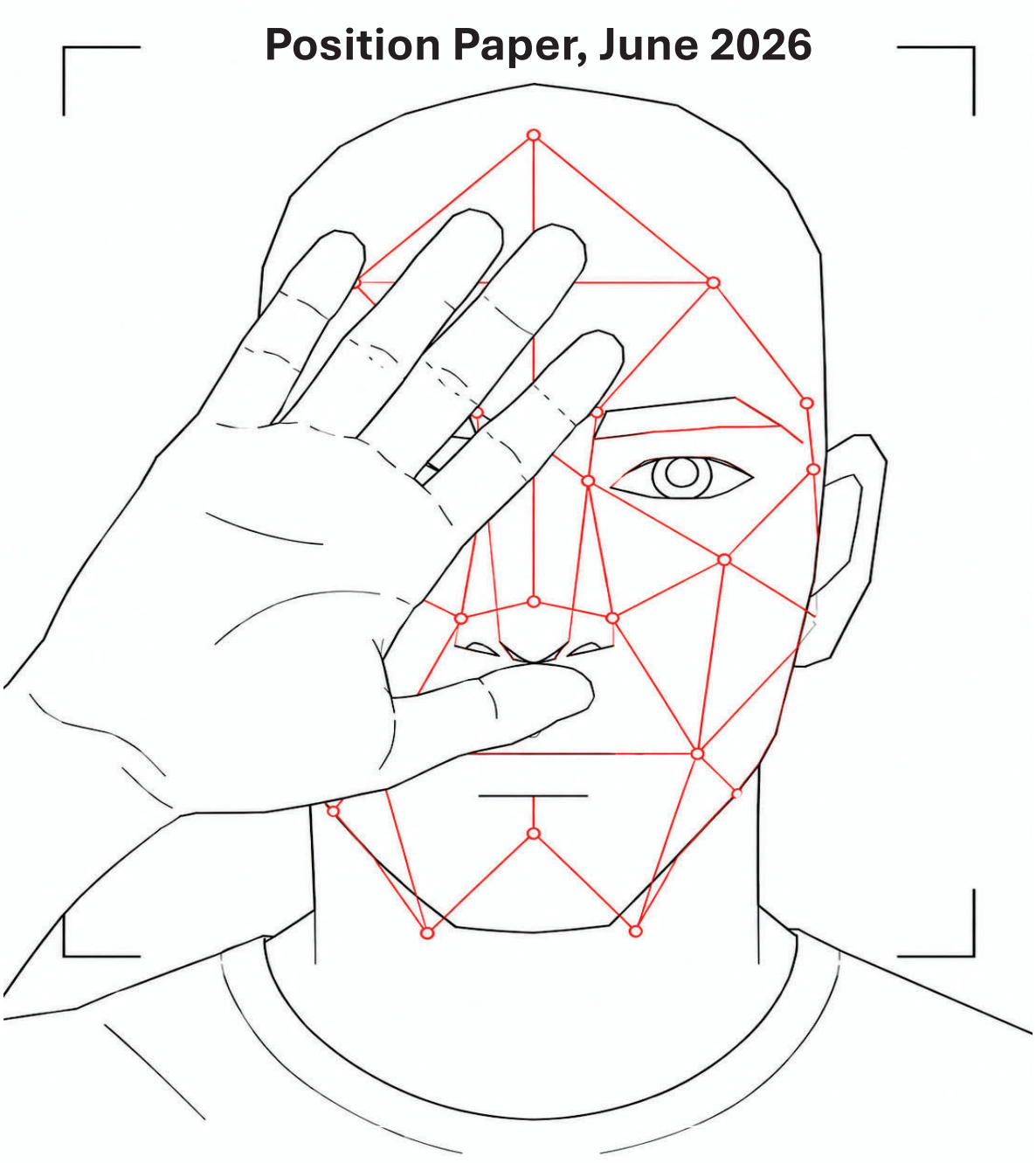
Facial Recognition Technology

Protecting Human Rights in Law Enforcement, Counter-Terrorism and National Security Contexts

Position Paper, June 2026



Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Saul

SPECIAL PROCEDURES
UNITED NATIONS
HUMAN RIGHTS COUNCIL

Contents

Introduction **1**

I FRT in law enforcement, counter-terrorism, and national security contexts **1**

A Context of new technologies in counter-terrorism 1

B Characteristics of FRT **2**

II Previous UN and multilateral work on FRT **6**

A International standard setting 6

B European Union: Biometric data protection 9

C European Union: Biometrics and artificial intelligence 9

III Absence of explicit national legal regulation of FRT **10**

IV Common human rights critique of FRT **11**

A Right to privacy 12

B Freedoms of expression, peaceful assembly, and association 12

C Non-discrimination and equality 16

D Right to effective remedy 17

E Implications of the existing human rights critique 18

V FRT reliability and impacts on investigative practices **19**

A The reliability of FRT under real-world conditions 19

1 Risks of falsification and 'spoofing' 21

2 'Facial emotion recognition' and 'behavioural biometrics' 22

3 FRT and artificial intelligence 22

4 Further risks of assuming reliability 23

B Wider influence in justice and security systems 25

C Opportunity costs 26

D Distancing from communities 27

E Implications for human rights 27

1 Right to liberty 27

2 Right to a fair trial 28

3 Stronger guardrails on using FRT 29

F Border management concerns **29**

VI Export/transfer of FRT **31**

Conclusion **34**

Recommendations **34**

Endnotes 39

Acknowledgements

Research and analysis for this Position Paper was led by Adriana Edmeades-Jones, consultant Legal Adviser to the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism in 2023-2024.

This research was supported by the Government of Switzerland, the Human Rights Center at the University of Minnesota Law School, The University of Sydney, and Sydney Law School.

This Position Paper is part of the mandate's long-standing work on new technologies and counter-terrorism, including on mass surveillance, biometrics, spyware, travel and border management technologies, new financial technologies, drones, lethal autonomous weapons systems, cybercrime and artificial intelligence.[*] Further work on online terrorist content moderation is planned for 2026.

The expert advice is acknowledged of the thematic section on Technology and Human Rights of the Office of the High Commissioner for Human Rights in Geneva.

This Paper is available online at: https://www.ohchr.org/en/documents/position-papers/facial-recognition-technology-protecting-human-rights-law-enforcement

The Special Rapporteur's website: https://www.ohchr.org/en/special-procedures/sr-terrorism.

Cover image: ChatGPT-generated.

[*] See https://www.ohchr.org/en/special-procedures/sr-terrorism/new-technologies and https://www.ohchr.org/en/special-procedures/sr-terrorism/index-thematic-issues-2005-present.

Introduction

The rapid global spread of sophisticated automated facial recognition technology ('FRT') poses significant challenges for human rights, particularly when used for law enforcement, counter-terrorism and national security purposes. Despite ongoing controversy,[1] these systems are becoming an increasingly standard tool in these contexts. They can have legitimate uses where they are subject to effective regulation and stringent human rights safeguards. While the rise of FRT has attracted attention from policymakers, lawyers, and human rights experts in the context of monitoring peaceful protests, concerns about FRT and its effects on human rights reach far beyond protests. Such concerns are magnified by the rapidly growing combination of FRT with artificial intelligence (AI) and other intersecting digital surveillance technologies.

This Position Paper details how the specific features of FRT, and the manner in which it is frequently deployed by law enforcement and security authorities, inherently challenge human rights protection, which the relatively limited safeguards commonly proposed do not adequately address. The Paper goes beyond the existing human rights critique of FRT by considering what its features and vulnerabilities mean for its accuracy, its place within law enforcement and security practices, and its impact on judicial processes. Mindful that the technology is likely to continue to be rapidly developed and adopted, including in jurisdictions where regulatory frameworks may have limited currency or effectiveness, the Paper proposes the essential elements of a 'best practice' regulatory response. It builds on the mandate's broader 2020 Position Paper on Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?,[2] including its recommendations on data protection, data sharing, 'human rights by design', due diligence, children's rights, oversight, and sale/transfer/export controls.

The Paper proceeds in six parts. Part I provides a broad overview of FRT and the development of the market for it. Part II sets out existing international regulatory and policy approaches to FRT. Part III outlines the conventional human rights critiques of such products. Part IV addresses the effects of FRT use on the integrity of law enforcement investigations and on human rights, including at borders. Part V highlights the absence of specific legislative frameworks for the use of FRT systems, and the impacts on human rights protection. Part VI considers the risks of the international transfer of FRT. The conclusion and recommendations identify the elements necessary to effectively regulate the use of FRT by law enforcement in a human rights-compliant manner, whether it is used remotely, live, or retrospectively, and in the context of monitoring protest, investigations, border security, or otherwise.

I FRT in law enforcement, counter-terrorism, and national security contexts

A Context of new technologies in counter-terrorism

Since the seismic terrorist attacks on the United States of 11 September 2001, a broad range of highly complex surveillance technologies have been developed and transferred globally for use in counter-terrorism, law enforcement, national security, military and border security contexts. Global concern about the risks of terrorism has led States to grant broad and unprecedented powers to law enforcement and border security agencies, often in the form of widespread surveillance, including mass electronic surveillance, and other forms of intrusion to prevent

and counter terrorism and violent extremism.[3] Internationally, the Security Council has encouraged States to enhance the sharing of counter-terrorism information, including that acquired by use of new technologies and in particular contexts such as border management and traveller information. These developments have been enabled by the exponential increase in computing processing power; the increasing prevalence of digital devices and Internet connectivity; the decline in the cost of such technology and data storage;[4] the growth of private investment in new technologies, and a substantial increase in State counter-terrorism funding. The proliferation of AI is turbocharging the capacities of other digital technologies.

States have placed ever more trust in the reliability of technical solutions to the security threats posed by terrorism and organized crime. Counter-terrorism and law enforcement justifications have dominated in political discourse, allowing State agencies increasingly unchallenged opportunities to intervene in individuals' lives, especially through forms of surveillance and digital monitoring. In response, the surveillance technology industry has expanded worldwide, confident that counter-terrorism and border security policies will continue to favour large-scale surveillance-based technological solutions to existing and emerging threats.[5]

The roll-out of complex biometric identification and surveillance systems has been prominent in these developments. The spread of biometric surveillance technology has been hastened by Security Council resolutions, which have called upon States to collect and share the biometric information of terrorist suspects, including those travelling internationally for the purpose of participating in acts of terrorism ('foreign terrorist fighters').[6] In particular, resolution 2396 of 2017 imposes a mandatory obligation on all States to 'develop and implement systems to collect biometric data, which should include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law' and encourages States 'to share this data responsibly among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies'.[7] In support of States' obligations, the UN Office of Counter-Terrorism ('UNOCT'), the Security Council's Counter-Terrorism Committee Executive Directorate ('CTED'), and the multi-stakeholder, Biometrics Institute compiled a Compendium of recommended practices in 2018.[8] The Council also endorsed the 2015 Madrid Guiding Principles on Foreign Terrorist Fighters and its 2018 Addendum, under which Principle 38 briefly addresses some human rights aspects of biometrics, including children's rights, procedural safeguards, and oversight.

The theoretical value of biometric systems is that they relate to information which: is universal (i.e. it can be found on all individuals and so can be applied to everyone); is unique (i.e. it differs between people); is permanent (i.e. it remains the same for the same person despite ageing or changes in appearance); is measurable (i.e. it provides data points which are capable of measurement and digitization); allows the system to perform effectively (i.e. in a manner which is accurate, speedy, and robust); and is acceptable (i.e. satisfies general societal norms and expectations).[9] This Position Paper focuses on the human rights concerns arising from one particularly prominent biometric technology – facial recognition. There is, however, an equally urgent need to effectively regulate other biometric systems, including problematic emerging technologies such as emotion and gait recognition and other 'behavioural biometrics'.

B Characteristics of FRT

Among biometric identification and surveillance methods, FRT is special because it can both verify and identify individuals at scale and speed but also, in certain applications, do so

remotely and covertly. Tracing its origins to the early 1960s,[10] and with rudimentary working systems dating from the 1970s,[11] in the past decade FRT has become an inescapable aspect of the modern world, applied in contexts ranging from the quotidian (unlocking smartphones) to the extreme (identifying covert foreign agents during war[12]or attempting to profile groups such as ethnic minorities). FRT is an automated probabilistic method which seeks to recognize individuals through comparing images of faces, making determinations regarding degrees of similarity or difference across a variety of points within those images.

Hygiene and proximity concerns for the longstanding biometric technologies of fingerprint or DNA analysis following the Covid-19 pandemic[13] appear to have further cemented FRT as a standard technology.[14] Its value and appeal to authorities derive from its combination of attributes: it promises to 'give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner'.[15] As one commentator has summarized:

> FRT may be understood as converging characteristics of previous technologies within a single algorithm. With sufficient CCTV [closed circuit television] infrastructure, it effectively permits tracking across locations, akin to global positioning systems. It can identify individuals, like DNA and fingerprint matching, but without the need for physical contact and processing time…[16]

The three main FRT methods in law enforcement

FRT generally takes three forms:[17]

Firstly, Operator Initiated Facial Recognition ('OIFR'), by which a person is compelled by law to, or sometimes voluntarily, provides an image of their face to be matched against a reference image for the purpose of confirming that they are who they say they are. This use of FRT has become widespread in various contexts including electronic border gates and logging into digital platforms. The United Nations Joint Staff Pension Fund, for instance, uses OIFR via its Digital Certificate of Entitlement as a log-in method.[18]

Secondly, Live Facial Recognition ('LFR'), which is a form of one-to-many matching technology using a live image of an unknown person (obtained via CCTV, mobile, body-worn, or drone camera) and searching an existing database of images to identify the unknown person. This form of FRT – as used by law enforcement agencies to identify those present in public settings against databases of known individuals and/or watchlists – has been the focus of much debate in recent years.[19]

Thirdly, Retrospective Facial Recognition ('RFR') involves after-the-fact application of FRT to a pre-recorded image (which may be drawn from CCTV, body camera footage, social media, or a smartphone photograph) and seeking to match it to an existing database and identify the unknown person. While termed 'retrospective,' the time lag applying to RFR may in fact be negligible depending upon the capacity of the system using it.[20] RFR, unlike LFR, need not be subject to geographical or temporal limits, and may not be visible to those being surveilled. RFR has potentially much broader scope since 'it can be applied to all footage obtained from a city-wide 24/7 surveillance camera network, or indeed to footage from multiple networks. Equally, it does not require a visible police presence meaning that its use gives rise to significantly less resource implications. RFR can, in effect, run unseen in the background'.[21]

Potential further applications of FRT at an early stage of development include the application of algorithmic decision-making tools to FRT for purposes beyond identification, purportedly to infer an individual's emotions or intentions.[22] This type of application – sometimes called 'facial emotion recognition' ('FER') – is reportedly used in certain contexts[23] but is in its infancy globally. Like all FRT, however, FER is subject to rapid experimentation and can be expected to be applied with increasing frequency. As an example, an EU-funded border security project known as 'IBorderCtrl' from 2016 to 2019 sought to develop an automated polygraph-style 'deception detector' by applying FER to real-time video of individuals so as to draw conclusions about the honesty of their responses to interview questions.[24]

Whatever the mode of FRT, the facial recognition process involves a number of complex steps.[25] First is the phase of enrolling images into a reference dataset, which lays the groundwork for all of the subsequent operations of the system. Such a dataset may be specific and bounded, such as the faces on a domestic or international terrorism or criminal watchlist, or broad and expansive, such as the 40 billion images which US company Clearview AI acknowledged had been scraped in bulk from the Internet, without consent, as a reference dataset.[26] Clearview AI was fined £7.5 million by the UK Information Commissioner's Office in 2022 for that scraping exercise, but the fine was set aside on appeal on the basis that the FRT services were provided to non-UK law enforcement and national security agencies, whose activities fell outside UK data protection law.[27] The process of building the dataset, and programming an algorithm to subsequently detect and match faces, can encode biases into FRT and render it prone to false positives from the outset.

Once an FRT system is applied to verify or identify a person from a new image, the system initially undertakes 'face detection' to identifying whether, and if so where, the image presented contains a face. In contexts where there are multiple individuals close together, whether in a crowd at a protest or in a queue at an airport, the 'face detection' stage also involves isolating which face will be analysed. The system, instructed by its algorithm, picks out general features such as overall shape and presence of nose and eyes. Then it undertakes 'face normalization'[28] or 'face alignment', which seeks to eliminate the effect of different face poses and expressions by identifying 'facial landmarks' (nose shape, pupils of the eye, corners of the mouth, jawline, eyebrows, etc) and relocating those features to a presumed standard or 'canonical' pose.

The final stage is the extraction from the 'canonical' face of the discriminating features, such as the measurements between the different facial landmarks and their relative orientation. That information is then compared with the reference set of images available to the system. At that final stage there will be a specific level (or 'confidence threshold') of accuracy tolerance identified. The objective of the commercially-developed FRT systems marketed to law enforcement and security agencies is to provide a number of matches which comes within that accuracy tolerance. The higher the confidence threshold imposed, the lower the likelihood of a match being returned, and vice versa: low confidence thresholds return higher error rates.

Each of OIFR, LFR, and RFR are used habitually in law enforcement and national security contexts. OIFR is increasingly standard as a border management tool and is used by some police forces as a way of verifying the identity of a detained person without recourse to lengthy arrest procedures. Police forces worldwide use LFR as a tool to increase preventive monitoring of target or watch-listed individuals, and RFR to investigate suspects after an incident.

Examples of the use of the three main FRT methods

Publicizing use of all three FRT methods of FRT by UK police forces, the UK Home Office has given examples of each form, facilitating arrests where ordinary physical policing would likely have failed to identify the suspects. The examples include:[29]

OIFR: 'OIFR is a mobile App that allows officers, after engaging with a person of interest, to photograph them and check their identity where they are not sure, without having to arrest them and tak[e] them into custody. It is at the early trial stage but has been showing positive results'.

LFR: 'The technology uses live video footage of crowds passing a camera and compares their images to a specific list of people wanted by the police'; 'At the Arsenal v Tottenham north London [football] derby on 24 September 2023, it led to three arrests, including a suspected sex offender'; and '[o]ver two busy Friday nights in Soho in August 2023 the Metropolitan Police used [LFR] to help find high harm offenders. Across the two deployments there were six accurate alerts and no false alerts. It led to the police engaging with six people, five of whom were arrested including a man wanted for possession of a bladed article and a woman wanted for breach of bail in relation to robbery'.

RFR: 'RFR is used after an event or incident as part of a criminal investigation. Images are typically supplied from CCTV, mobile phone footage, dashcam or doorbell footage or social media. These images are then compared against images taken on arrest to identify a suspect'; '[An individual] was jailed for life in 2021 after attacking a woman he followed off a bus. He was arrested within 48 hours of the incident thanks to South Wales Police using facial recognition on images captured by CCTV, including on the bus'; and 'Multiple burglars have been caught thanks to doorbells with cameras, the modern equivalent of a thief leaving his fingerprint on a windowsill. A man was jailed for burgling the home of a vulnerable pensioner. Using RFR on a CCTV image from the pensioner's home, officers identified the suspect, arrested him the following day, and he later pleaded guilty to burglary'.

The extent of the use of FRT by law enforcement and security authorities worldwide is unclear given a lack of transparency. A 2022 survey of 99 countries estimated that 70 percent of police forces had access to some form of FRT.[30] In China, FRT is widely deployed in different settings, supported by 560 million security cameras (half of the global total).[31] In the US, the Government Audit Office identified in 2021 that 42 federal law enforcement agencies used FRT in some form.[32] Local and state/provincial police forces make wide use of FRT: Clearview AI claimed in 2023 that US police forces had used the system for 1 million searches.[33]

In the UK, in 2026 the Government announced that LFR would be used by all police services in England and Wales, and all forces already have access to RFR through the Police National Database.[34] In Russia, FRT is used by State agencies across the country. The *Glukhin v Russia* case before the European Court of Human Rights revealed that all of the more than 220,000 CCTV cameras in Moscow are equipped with LFR technology.[35] In 2021, the Canadian Office of the Privacy Commissioner revealed that the Royal Canadian Mounted Police (which is responsible for federal and the vast majority of provincial policing in the country) had been using FRT without public knowledge (and had falsely represented to the Privacy Commissioner that it was not).[36] Cities in Brazil,[37] North Africa,[38] and elsewhere[39] have been rolling out FRT-enabled camera networks for public safety and law enforcement purposes. The rapid expansion of FRT capacities worldwide is clearly set to continue.

II Previous UN and multilateral work on FRT

A International standard setting

The binding Security Council measures in 2017 drove the rapid wider adoption of FRT as a counter-terrorism and law enforcement tool. Subsequently, various UN and multilateral agencies have promoted the international development and implementation of such systems. The General Assembly has consistently reaffirmed, in reviews of the UN Global Counter-Terrorism Strategy since 2018, the collection and sharing of biometric data (including face data) as a means to address terrorist travel and border management.[40] A key practical part of global FRT capacity is the Interpol Facial Recognition System ('IFRS') – a global reference database launched in late 2016 and populated with images received from a wide range of member countries.[41] The IFRS database has, since late 2023, been brought together with Interpol's fingerprint database and an automated matching functionality developed by Interpol's tech partner to create Interpol's new Biometric Hub,[42] available to law enforcement agencies in 196 States.[43] As already noted, a UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism was published in 2018.

There is no binding international legal framework specifically regulating FRT, or its use in conjunction with AI. Various entities have been at the forefront of reviewing the compliance of FRT with international human rights law, urging caution against its increasingly broad application. The international community, including UN human rights mechanisms, have predominantly focused on the indiscriminate application of FRT in public settings, in particular the risks posed to the freedoms of expression and assembly. In 2019, the Special Rapporteur on the rights to freedom of peaceful assembly and association identified that '[f]ace recognition technology deployed at large cultural events, major sporting events, music festivals and political gatherings … raises proportionality concerns'[44] and that FRT systems 'violate the individual's anonymity in public spaces and exert significant "chilling effects" on decisions to participate in public gatherings'.[45] As a result, the Special Rapporteur recommended a blanket prohibition on the use of 'surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association'.[46] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his 2019 report on surveillance similarly called for an immediate moratorium on the sale, transfer, and use of surveillance tools including FRT until robust human rights safeguards were in place to regulate such practices.[47]

The 2020 report of the UN High Commissioner for Human Rights on the impact of new technologies considered the risks posed by the use of FRT to the rights to freedom of peaceful assembly, privacy, and freedom of expression, and urged that authorities should generally refrain from using FRT in peaceful assembly contexts.[48] The same year, the Special Rapporteur for the promotion and protection of human rights and fundamental freedoms while countering terrorism released a report on the use of biometric data to identify terrorists which noted that the potential for the discriminatory impact of FRT was exceptionally high and called for action particularly with respect to transparency and accountability of automated FRT processes.[49]

Then in 2021, the UN High Commissioner for Human Rights, in the 'Right to Privacy in the Digital Age' report, reiterated that States ought to impose a moratorium on the use in public spaces of remote biometric recognition technologies, including FRT, at least until authorities are able to demonstrate compliance with privacy and data protection standards and that

significant concerns regarding accuracy and discriminatory impacts have been addressed.[50] The same year, the Human Rights Council convened a panel discussion on the promotion and protection of human rights in the context of peaceful protests, involving the Special Rapporteur on the rights to freedom of peaceful assembly and association, the former chair of the Human Rights Committee, civil society, and contributions from 20 States and the European Union.[51]

In 2021, the Consultative Committee of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted Guidelines on facial recognition.[52] These Guidelines proceeded on the basis that FRT may lawfully be employed for law enforcement purposes, but urged agencies using FRT to, among other things: (a) do so with transparency (limiting covert use to where 'strictly necessary and proportionate in order to prevent an imminent and substantial risk to public safety');[53] (b) do so in compliance with data protection rules (limiting the purposes for which biometrics may be used and the time period for which it can be retained, and imposing requirements for the deletion of that data);[54] and (c) ensure the accuracy of the data and take reasonable steps to correct false matches.[55]

In 2022, the Human Rights Council adopted a resolution which expressed concern about the arbitrary and unlawful surveillance of individuals engaged in peaceful protests including via facial and purported emotional recognition technologies, and again urged States to refrain from such use.[56] The UN High Commissioner for Human Rights further warned that FRT may create mass surveillance of public spaces in violation of privacy rights, and suggested the need for an international advisory body to align regulatory standards with human rights.[57] In 2023, the Secretary-General proposed the establishment of a digital human rights advisory body.[58] Although such a body has not been established, multilateral interest in digital governance more generally has been pursued through a temporary High-level Advisory Body on Artificial Intelligence, which reported to the Summit of the Future in September 2024, leading to the adoption of the Global Digital Compact, and the later the General Assembly-driven processes on global governance of AI, discussed below.

Reference to FRT was included in the Special Rapporteur on the rights to freedom of peaceful assembly and association's 2024 Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests,[59] developed in collaboration with the UN Office of Drugs and Crime ('UNODC') and the High Commissioner for Human Rights. Building on previous international work,[60] the Model Protocol reiterates the obligations of law enforcement under international human rights law, focusing on the need to minimize unnecessary and disproportionate interferences with protesters' exercise of their freedoms. Accordingly, the Model Protocol urges law enforcement to '[e]nsure that the overall approach guiding any use of digital technologies in the context of protests is premised on a limiting principle to circumscribe the use of such technologies, rather than an authorizing principle intended to expand their use'.[61] In relation to digital surveillance including FRT, the Model Protocol provides as follows:[62]

> Law enforcement officials should:
>
> Employ the least intrusive methods while gathering information, conducting assessments and collecting evidence during a protest, which should be done in full compliance with protections against arbitrary or unlawful infringement of participants' rights;
>
> Ensure that any decision to utilize surveillance strategies and/or to record participants is exceptional and limited to distinct law enforcement purposes, such as directly aiding the prevention, investigation and prosecution of a specific criminal offence occurring within the

context of the protests. Facial recognition technologies and other biometric systems must not be utilized to identify individuals who are peacefully participating in a protest;[63]

Apply strict law enforcement protocols to govern the collection, retention and use of data collected during a protest, in accordance with a commitment to safeguard the rights and privacy of individuals;[64]

Refrain from interpreting with suspicion any tactics utilized by an individual or group of individuals during a protest with the ostensible intention of preserving their anonymity. Individuals have a legitimate expectation of a degree of anonymity in online and offline spaces.[65]

Further, non-binding guidance on FRT been provided by the Global Privacy Assembly, comprised over 130 public data protection and privacy authorities, in its 2022 Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology.[66] The standards emphasize legality; reasonableness, necessity, and proportionality; protection of human rights, including in relation to impact assessments, bias, chilling effects and marginalized groups; transparency; accountability; and data protection (including privacy by design; purpose specification and use limitation; data minimization, retention and deletion; safeguards; and data quality).

At a technical level, there have also been international developments that can potentially enhance the human rights compliance of FRT. In 2025, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) adopted a number of new International Standards, including ISO/IEC 29794-5:2025 on biometric sample quality for face image data (to reduce errors due to face image quality and improve both algorithmic and human assessment), and ISO/IEC 19795-10:2024 on biometric performance testing across demographic groups. This supplements other ISO standards on FRT,[67] and further standards are being developed or revised.[68] Meanwhile the first global standard on AI management systems, ISO/IEC 42001, adopted in 2023, applies to AI connected with FRT, and addresses ethical use, data privacy and governance, risk management, bias, accountability, and transparency. While these standards are voluntary, as industry 'soft law' they increasingly function as quasi-mandatory due to their incorporation into procurement, certification and regulatory processes, outpacing formal global regulation and often also national regulation.

The convergence of FRT with AI is transforming potential surveillance capabilities, by improving scale, accuracy and speed. These advances have precipitated widespread deployment of AI-driven surveillance systems in public spaces, on public transport, and at borders, with profound implications for human rights. Efforts towards international regulation are currently being channelled through the Global Digital Compact (2024) and the establishment in 2025 of the Independent International Scientific Panel on AI and the Global Dialogue on AI Governance, with a strong emphasis on human rights (including equality and non-discrimination), transparency, accountability and robust human oversight.

In a 2025 Position Paper, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism highlighted concerns regarding persisting algorithmic bias affecting certain demographic groups, stemming from unrepresentative datasets; data protection gaps; and transparency and explainability deficits that impede the right to effective remedy and accountability for resulting human rights violations.[69] The Paper called for explicit and enforceable legal regulation, including of law enforcement, border management and national security applications; prohibitions on uses that

cannot comply with human rights law or that pose unacceptable risks; rigorous human rights due diligence; data testing, validation, security and protection; transparency and explainability; and effective export and transfer controls.

B European Union: Biometric data protection

Biometric data generally is covered by the general prohibition on the processing of highly sensitive special categories of personal data under Article 9(1) of the European Union's General Data Protection Regulation,[70] first adopted in 2016, with exceptions for 'substantial public interest' purposes under Article 9(2). However, it is not intended to apply in relation to criminal offences and safeguarding public security (recital 19) or national security (recital 16). Instead, the Law Enforcement Directive (LED) (Directive 2016/680) applies to police, prosecutors, and criminal justice authorities, and provides more tailored (and permissive) regulation of data processing and data protection in that context. Where the General Data Protection Regulation does apply, it can also limit data subject rights on grounds of public or national security, defence or prevention of crime (Article 23). National security generally (including intelligence, counter-terrorism and military activities) is the responsibility of member States, not the EU.

In 2023 and 2024, European Union organs considered FRT in detail. European Data Protection Board guidelines consider the impact of the use of FRT by law enforcement on the rights to privacy and the standards required by EU data protection legislation.[71] The Board noted that it

> understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, such tools should be used in strict compliance with the applicable legal framework and only in cases when they satisfy the requirements of necessity and proportionality.[72]

The Board considered that certain uses could never be justified: 'In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society, as by its nature, it entails mass surveillance'.[73] Further, the Board considered that the use of FRT for profiling or prediction or inference about future conduct should be generally prohibited.[74] In addition, the Board indicated that FRT programs 'that would rely on a database populated by collection of personal data on a mass scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law'.[75]

C European Union: Biometrics and artificial intelligence

The EU has emerged as the key normative standard setter on the use of FRT in connection with AI. In 2024 the European Union adopted its Artificial Intelligence Act (Regulation 2024/1689) ('AI Act'), which lays down harmonized rules for a large number of AI applications.[76] FRT is addressed in four important ways, including certain prohibitions that came into force in February 2025. First, echoing the Board's recommendation, the AI Act prohibits the sale or use of FRT systems which build their reference image databased by means of untargeted scraping of facial images from the Internet or CCTV footage.[77] European Commission Guidelines of 2025 clarified that targeted scraping is permissible, as where it relates to specific criminals or groups of victims; and that the prohibition on untargeted scraping only applies if AI is used.[78]

Secondly, again in line with the Board's view, the AI Act prohibits the use of any 'real-time' biometric identification system (including LFR, but not RFR) in public for the purposes of law enforcement except insofar as such use is strictly necessary for the purposes of the: (a) targeted search for specific victims of abduction or trafficking, or missing persons; (b) prevention of a 'specific, substantial, and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack'; or (c) identification of a person suspected of having committed a serious criminal offence (meaning offences punishable by at least four years imprisonment).[79]

Thirdly, the AI Act prohibits biometric systems that categorize individuals based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation, subject to a law enforcement exception for labelling or filtering of lawfully acquired datasets.[80]

Fourthly, each use of 'real-time' biometric identification systems (including LFR, but not RFR), even for the limited purposes above, requires specific authorization that it is 'necessary and proportionate' from a judicial authority or independent administrative body (except in cases of urgency, in which case ex post authorization must be obtained within 24 hours).[81]

From August 2026, full compliance obligations under Annex III of the AI Act come into force for high-risk biometric systems, which include many FRT applications (such as remote identification and emotion recognition). These require conformity assessments, quality management systems, risk management and human oversight frameworks, registration in an EU database, and comprehensive technical documentation. Remote biometric identification requires audit logs to be maintained, and verification by two qualified individuals (but with exceptions for law enforcement, migration, border control or asylum).

Fines of up to €35 million or seven percent of global turnover are available for breaches of the AI Act, but enforcement is difficult against companies without a European presence. The EU established an AI Office and AI Board in 2025 to coordinate implementation and interpretation.

Notably, the Council of Europe also governs AI (including relevant FRT systems) through the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024), imposing binding human rights obligations, but again with exemptions for national defence and national security (article 3).

III Absence of explicit national legal regulation of FRT

Moving to the national level, despite the widespread adoption of FRT systems in law enforcement and security contexts worldwide, a common feature is the lack of prior specific legislative authority for their use. While some jurisdictions are in the process of enacting specific legislation authorizing the use of FRT,[82] many prominent law enforcement agencies, such as the London Metropolitan Police Service ('MPS') and the US Federal Bureau of Investigation ('FBI'), have tended to rely upon claims as to general or inherent authority to deploy whatever tactics are deemed necessary for public protection,[83] or to treat FRT as simply an example of generally-authorized evidence-gathering powers. In the US, federal, state, and local police forces operate FRT on an ad hoc basis: such technology comprises a range of off-the-shelf commercial products[84] deployed as a mere instrument by analogy with any other tool or technique and without any prior unique legislative consideration or statutory authority.

As an independent legal review of FRT use by UK police noted, there is no explicit legal basis for the practice,[85] despite calls by a UK parliamentary committee in 2024 to legislate for its use.[86] Instead, UK forces rely upon general common law policing powers to detect crime and protect public safety, asserting that FRT is simply another exercise of those legitimate powers and does not require explicit authorization, a position endorsed by the UK courts.[87] The courts have further accepted that legality and foreseeability, as required by human rights law, are also enabled by data protection legislation and police and surveillance codes, policies and procedures, such that the overall framework and safeguards are sufficient.

In many places, such as in China[88] and under the EU's Law Enforcement Directive and AI Act, legislation refers to official use of FRT as an allowable exception to restrictions upon non-official deployment of biometric identification technology. Even in the case of jurisdictions considering specific legislative authority for the use of FRT – such as the amendments proposed to the Irish legislation governing police use of CCTV and body-worn cameras[89] – the reference to FRT or biometric data is in general terms and does not go into any detail regarding the capabilities, vulnerabilities, record-keeping, or other features of the systems envisaged.

The upshot of the current lack of detailed legislative interrogation of FRT systems in use by law enforcement and security agencies is a fundamental failure to engage with the complex implications of various FRT systems for human rights protection across the different contexts in which those systems are deployed. Human rights experts and regional courts have emphasized that FRT should only be deployed under more specific domestic legal authority. According to the European Court of Human Rights in *Glukhin v Russia*, such authority prescribes limitations on, inter alia, 'the nature of situations which may give rise to the use of [FRT], the intended purposes, the categories of people who may be targeted, … processing of sensitive personal data' and 'procedural safeguards … such as the authorization procedures, the procedures to be followed for examining, using and storing the data obtained, supervisory control mechanisms and available remedies'.[90] The absence of specific legislation also necessarily means an absence of the dedicated human rights analysis and scrutiny that often accompanies proposed legislation in many parliamentary systems, including consultation with relevant stakeholders such as technical and legal experts, national human rights institutions, data protection and corporate regulators and civil society organizations.

FRT is a descriptive label, rather than a monolithic thing. Different commercially-available programs, used for different functions (such as OIFR for verification of identity at the border, LFR on protest or non-protest crowds to identify watch-listed individuals, RFR on CCTV to track down suspects) give rise to human rights considerations of different natures and intensity. Each merits specific consideration, and bespoke safeguards, through proper legislative scrutiny involving consultation with technical and legal experts. As a result, the keystone of any human rights-respecting regime of FRT regulation should be a requirement that parliaments (or equivalent law-makers) consider and authorize of each proposed use of FRT in law enforcement and security contexts, so that the necessary and context-specific limitations and safeguards on such use may be adequately addressed.

IV Common human rights critiques of FRT

Since the emergence of FRT as a law enforcement and security tool, extensive work by human rights bodies, civil society, and academia has considered the risks it poses to human rights. A consistent critique has focused on how the LFR and RFR applications of FRT potentially

interfere in the rights of privacy, freedom of expression, freedom of peaceful assembly and freedom of association. Part III of this Paper summarizes these critiques, before Part IV examines the wider human rights implications of FRT, including whether the purported 'fixes' for the mainstream human rights concerns are adequate.

A Right to privacy

Under human rights law, everyone enjoys the right to private and family life without undue interference.[91] Both the General Assembly[92] and the Human Rights Council have stressed[93] that the right to privacy serves as one of the foundations of democratic societies and, as such, plays an important role in the realization of a host of other rights, including the rights to freedom of opinion and expression,[94] religion,[95] peaceful assembly,[96] and association.[97]

In both LFR and RFR, footage of large numbers of people is analysed to identify, and then allow the further tracking or apprehension of, certain individuals. Such uses necessarily require the analysis and review of the biometrics of a very large number of people who are not of interest to law enforcement, but whose data is nonetheless collected and assessed, even if only to be discounted as irrelevant. This process is well-recognized as representing a clear interference with individuals' rights to privacy.[98] As the European Court of Human Rights put it in *Glukhin v Russia*,

> [a] person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one of the essential components of personal development and presupposes the right to control the use of that image. While in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person.[99] …
>
> Where the personal data of a person's face is accessed in a context where it reveals political opinions or other affiliations, it can be viewed as especially sensitive and demanding of a heightened level of protection.[100]

The impact of biometric monitoring technologies upon privacy is particularly acute given that a typical legislative safeguard against privacy infringement – domestic data protection regimes – will generally be either ousted or heavily restricted by counter-terrorism or criminal justice powers. Data protection regimes grant data subjects the opportunity to obtain and, where appropriate, request rectification or removal of inaccurate or unnecessarily held personal information. For example, the EU's governing data protection framework – the General Data Protection Regulation,[101] on which much data protection legislation worldwide is modelled – does not apply to data processing by law enforcement and criminal justice authorities, and even the weaker data processing rules that apply (the so-called Law Enforcement Directive)[102] do not regulate data collection, retention, processing, and/or sharing to the extent that such sharing occurs for national security purposes.

B Freedoms of expression, peaceful assembly, and association

FRT (particularly LFR) is frequently deployed in crowds of people, often brought together for purposes of assembly, including in respect of political demonstrations or religious observance. These contexts place the rights of freedom of expression, association, and peaceful assembly

at special risk. Freedom of expression – which includes the right both to impart and to receive information without undue restriction[103] – is protected worldwide as a fundamental right,[104] and is of particular importance, since it provides a platform upon which other rights, including political participation[105] and freedom of peaceful assembly,[106] association,[107] and religion[108] may be exercised. As the Human Rights Committee stated in General Comment No. 34:

> Freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society … Freedom of expression is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights.[109]

The right applies broadly, and includes 'political discourse, commentary on one's own and public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse'.[110] As regional courts have made clear, opinion and expression does not lose protection merely by virtue of being untrue, shocking, offensive, disturbing, or even by challenging the democratic principles by reference to which its protection is justified.[111]

The freedoms of peaceful assembly and association are in turn 'essential pillars for democracy and for facilitating public participation and as enablers of civil, political, social, economic and cultural rights'.[112] As the Human Rights Council has repeatedly recognized, peaceful assembly and protests 'can make a positive contribution to the development, strengthening and effectiveness of democratic systems and to democratic processes, including elections and referendums' and that protests 'have historically played a constructive social and political role in the development of more just, equal and accountable societies, and that such protests can continue to make a positive contribution to human development and to the full enjoyment of civil, political, economic, social and cultural rights'.[113]

The significance of the impact on FRT in the context of protest and assembly has been highlighted by the UN High Commissioner for Human Rights, who noted that '[a]ssemblies traditionally have allowed participants a certain level of protection against being singled out or identified'.[114] Indeed, the Human Rights Committee in General Comment No. 37 has emphasized that:

> The wearing of face coverings or other disguises by assembly participants, such as hoods or masks, or taking other steps to participate anonymously may form part of the expressive element of a peaceful assembly or serve to counter reprisals or to protect privacy, including in the context of new surveillance technologies. The anonymity of participants should be allowed unless their conduct presents reasonable grounds for arrest, or there are other similarly compelling reasons, such as the fact that the face covering forms part of a symbol that is, exceptionally, restricted for the reasons referred to above…. The use of disguises should not in itself be deemed to signify violent intent.[115]

The UN High Commissioner warned, however, that FRT has led to 'a paradigm shift' which 'dramatically increases the capacity to identify all or many participants in an assembly in an automated fashion'.[116] The Human Rights Committee, in its concluding observations on the 2024 periodic report of the UK, noted with concern the 'increased use by police forces of facial recognition technology to monitor peaceful gatherings'[117] and called upon the State to halt such use at protests 'to safeguard privacy, non-discrimination, freedom of expression, association, and assembly rights for protesters'.[118] Authorities in certain States have used FRT in blatant

disregard of the rights of protesters. In the Russian Federation, for instance, FRT has been used to identify, locate, and arrest participants in rallies in support of Russia's deceased opposition leader.[119] FRT can also be used on conjunction with other restrictions that facilitate it, such as bans on face coverings at normal protests, such as those imposed in many European States, Russia, and some US states.

Interferences with the rights to privacy, freedom of expression and assembly, and other associated rights are only permissible in limited circumstances where (a) such interferences are precisely authorized by law; (b) serve a legitimate objective, which may include public safety and national security;[120] and (c) are strictly necessary and proportionate, and non-discriminatory, in their effect. As discussed in Part III of this Paper, a dominant human rights criticism of the adoption of FRT systems by law enforcement and security agencies worldwide has been the absence of specific statutory or regulatory authority.

A bona fide application of FRT for the purpose of preventing crime is generally accepted as meeting the 'legitimate objective' criterion.[121] However, the degree of interference must be considered in light of the necessity of the measure to achieve the aim and the actual benefit it yields.[122] The Human Rights Committee has clarified that proportionality requires that the infringement is the 'least intrusive instrument amongst those which might achieve their protective functions,'[123] and has counselled that

> [i]n adopting laws providing for restrictions permitted [for legitimate aims], States should always be guided by the principle that the restrictions must not impair the essence of the right … the relation between the right and the restriction, between norm and exception, must not be reversed. The laws authorising the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution.[124]

An FRT system which reviews the biometric data of a large number of persons without any prior distinction between potential suspects and those raising no legitimate law enforcement concern inevitably casts its net too wide, and appears incapable of complying with the 'least intrusive instrument' proportionality criterion. That is why the Special Rapporteur on the rights to freedom of peaceful assembly and association has stated that surveillance against individuals should 'only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality, and providing for close judicial supervision'.[125] Similarly, the UN High Commissioner for Human Rights has recommended that States should '[r]efrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards'.[126] The African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression and Access to Information in Africa has made the same point, noting that generalized surveillance, including via FRT, is prima facie unlawful and targeted surveillance must be authorized by law and premised on specific and reasonable grounds.[127]

In addition to the interference which FRT appears inevitably to entail for those subject to monitoring, human rights more broadly are affected by the introduction of ever-greater surveillance capabilities in civic space. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has observed,[128] disproportionate use of surveillance powers per se undermines freedom of expression, particularly through a chilling effect whereby people self-censor to avoid State scrutiny. That concern is particularly

keenly felt by people who already perceive themselves as disproportionately targeted by State authorities, including members of racial, religious, ethnic or other minorities.[129] Further,

> chilling effects are not binary, but are nuanced in their impacts. That is, a chilling effect does not necessarily mean that a person will not engage in political activities when ordinarily they would have; of course they may choose not to engage, but they may also choose to modify the nature of that engagement. Chilling effects can therefore impact on the process by which individuals develop their identity/personality, which can in turn impact on their political participation.[130]

This has not only individual but collective impacts, since it impedes the ability of people to associate and express themselves in groups, and undermines the dynamic development of society and democracy. As has been observed, '[w]hen there is protection from surveillance, new ideas can be entertained, even when they might be deeply subversive or threatening to conventional or orthodox views. If we value a pluralistic society or the cognitive processes that produce new ideas, then some measure of intellectual privacy, some respite from cognitive surveillance, is essential'.[131] Further, the 'chilling effect is best understood as an act of compliance with, or conforming to, social norms'.[132]

One of the most challenging aspects of the chilling impact of FRT surveillance on individual and societal development and progress is the difficulty of effectively identifying, specifying, and remediating such effects. The harm is 'different to [that] typically addressed by human rights law' in that, while 'violations of the prohibition of torture, the right to life, or the right to a fair trial are relatively easy to identify as there is immediately observable harm', chilling effects 'are more complex, and more difficult to identify'.[133] That is because the effect may be to vary rather than prevent affected persons' behaviour, and so the causative impact is more nuanced. Further, 'while certain chilling effects may be discernible in the short term, the true impact is only likely to manifest over the medium to long term'.[134] In addition, the chilling effect of diffuse digital surveillance by FRT may impair individuals' willingness to take legal steps to remedy violations and to vindicate their rights. Generalized surveillance through FRT can discourage individuals' participation in civil society, including in the protection of their own and others' rights, with the net effect being an environment of State dominance of civic space and social life and mass conformity and compliance.

One 'fix' for these adverse impacts on freedoms of expression, peaceful assembly, and association is simply to ban the use FRT as a surveillance tool, as advocated by many human rights activists and some cities. Another 'fix' acknowledges that FRT is likely to be used, but recommends human rights safeguards, such as that the use of FRT should be: (a) generally prohibited in the context of live application to peaceful protests; and (b) when used in other contexts, either made subject to explicit transparency requirements, such as signposting to the public that FRT is being used for live crowd monitoring, or limited to retrospective rather than live use. When used in a live capacity to search a large crowd for specific persons already on a watch-list, the conventional human rights critique proposes that the biometrics of persons who are not identified as a match must be automatically deleted. According to such proposals, FRT may be acceptable when applied to gatherings outside the formal context of a protest, say, to a crowd at a non-political public event like a football game or a busy public space to search for watch-listed individuals, so long as its use is publicized and the biometrics of persons not matched against the list are deleted. FRT is also considered acceptable when applied after the fact by means of RFR to supplement traditional methods of identification, like fingerprinting and eyewitnesses, of those already suspected of involvement in a criminal incident.

C Non-discrimination and equality

A further element in the dominant human rights critique of FRT focuses on its disproportionate rates of inaccuracy in identifying persons other than white males, and thus its potential to violate the rights to non-discrimination and equality in international human rights law.[135] This issue came to prominence following a 2018 blogpost providing the results of a test conducted by the American Civil Liberties Union, using one FRT system, Amazon Rekognition, to compare images of members of the US Congress with a reference set of 25,000 mugshots of persons arrested for crimes. The test falsely identified 28 members of Congress as matching the mugshots, with disproportionately high false identification of non-white members.[136] That test has been roundly criticized by figures from the FRT industry,[137] but the apparent bias of FRT systems has been revealed in a range of contexts.

Examples of discriminatory FRT identification

A number of examples have been prominently reported in the US where black men have been arrested and detained on serious charges on the basis solely of FRT misidentification.

- In 2019, a man in New Jersey was identified from LFR video as matching an image on a fake identification card left at a crime scene. He was arrested on serious charges of assault, theft, and evading arrest which would have borne a maximum sentence of 25 years' imprisonment.[138] He was finally exonerated when separate evidence proved he was elsewhere at the time of the crime.

- Also in 2019, a man was detained at a routine traffic stop in Detroit and then arrested on the basis of an RFR match against a screenshot taken during a violent altercation some months earlier. Upon rudimentary human review of the image, the obvious differences – including prominent tattoos – were enough to have the charges dropped.[139]

- In 2020, a man was arrested in Detroit on the basis of his identification via an RFR process which matched a CCTV still of a robbery at a jewellery store against a nation-wide database of 49 million reference images (drawn from driver's licences and other forms of ID). The man's face was identified as one of six probable matches, and was then selected from those six by a witness. Separate evidence established conclusively that the suspect was at work elsewhere when the crime occurred, and charges were eventually dropped and a settlement subsequently agreed.[140]

Racial bias in FRT has been observed worldwide. As the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance has observed,

> [t]he facial recognition system used by the Delhi Police was reported to be accurate in only 2 per cent of cases and to put minority communities at a disproportionate risk of misidentification and false arrest. Brazilian law enforcement officials have reportedly falsely accused and arrested individuals on the basis of faulty facial recognition tools. According to a 2019 study, 90 per cent of people arrested in Brazilian cities on the basis of [FRT] are of African descent.[141]

While the inscrutability of FRT's 'black-box' algorithms[142] (including due to a lack of transparency and explainability, coupled with commercial confidentiality) can make it difficult to identify the precise cause of this phenomenon, two explanations have been proposed. First, it is typically explained as a function of skewed proportions of images used in the training sets of the first broadly-available FRT algorithms, apparently due to limited access to representative and broad image sample sets, which appear to have failed to train the systems sufficiently well on features found in female and non-white faces.[143] Alternatively, some have pointed to at least unconscious bias on the part of predominantly white software engineers, potentially by instructing the software to place prominence on features which may be more readily recognizable by white male observers rather than on the features that are objectively useful in distinguishing other faces.[144]

As FRT systems have continued to be tested and refined, the gaps between identification rates, at least in the optimal conditions under which testing occurs, appear to have closed, at least according to the peak testing body, the US National Institute of Standards and Technology. As mentioned, ISO/IEC technical standards have also continued to be refined. This may tend to suggest that the critique focused on machine-learning errors may fade in significance over time. That does not mean, however, that FRT systems – like any law enforcement or counter-terrorism tool – would be immune from discriminatory effects, since those tools may continue to be deployed in contexts where discrimination persists in the application of those tools.

Indeed, the supposed solution to apparently discriminatory FRT errors – namely access to more diverse datasets of reference images – does not necessarily guarantee non-discrimination. That is because the enrolment of reference datasets contributes to the calibration of the FRT system in a way which, while it may increase the accuracy of recognition of non-white faces, also increases the frequency of those results. If datasets of faces which are disproportionately non-white – including disproportionately non-white image databases held by police forces in the US, where many FRT algorithms are developed – are used to train FRT systems, the inevitable conclusion will be an ever-greater proportion of positive matches to non-white suspects. Since non-white individuals are disproportionately likely to be arrested by police forces in the US,[145] or have their image held even without arrest or suspicion (such as under the NY Police Department database of suspected 'gang affiliates', which does not depend upon proof),[146] the presence of non-white individuals in police databases is vastly out of proportion to their prominence as serious criminal offenders in society. FRT systems increasingly trained on non-white faces can thus be expected to replace one error which has a relatively simple technological fix (inaccurate identification) with another, the reasons for which are systemic, long-standing, and much more difficult to remedy (disproportionate targeting and over-policing of certain demographic groups). In addition, given the international export market for FRT databases, even datasets that might be relatively representative in one State (or part of it) may not be reliable in foreign jurisdictions with quite different demography.

D Right to effective remedy

The use of FRT as a remote and covert surveillance technology has also raised substantial concerns concerning the right to effective remedies,[147] which is central to effectively protecting human rights.[148] For a remedy to be 'effective', it must be: prompt;[149] practical rather than theoretical;[150] determined by a competent independent authority,[151] with the possibility of judicial remedy; and accessible (without undue practical barriers).[152] It also entails a right of reparation, including compensation as appropriate.

Surveillance technology poses specific challenges for access to effective remedies. Surveillance and the use of FRT is often concealed and, even if revealed in relation to a specific person, may be unknown to the large number of others affected. The UN High Commissioner for Human Rights has previously identified that effective remedies require '[n]otice (that either a general surveillance regime or specific surveillance measures is in place) and standing (to challenge such measures)', but that in practice, notification obligations in criminal cases appear 'to be regularly ignored'.[153] Notice should be adequately publicized, comprehensible, and accessible to diverse groups, including as regards language and disability, and include information concerning how to seek remedies.

In the absence of proper notice of the extent to which FRT has been used in a particular context, affected individuals may have limited access to the evidence necessary to vindicate their right to a remedy. Further, where a person has not had notice, there may be delays in the person learning that their rights were violated and the person may thus not be able to obtain a 'prompt' remedy. The 'black box' nature of FRT algorithms can pose a further barrier at a later stage, since it prevents an affected person from scrutinizing flawed datasets and matching methods.

Again, it is typically proposed that the right to effective remedy may thus be enabled prior notification requirements, so that affected persons may be forearmed. They may then be able to vindicate their rights if they can demonstrate that the use of FRT monitoring of the crowd of which they formed a part was not for a legitimate purpose, was not necessary or proportionate to pursue that purpose, extended beyond a justifiable time, or was otherwise unlawful. Ensuring the explainability and transparency of FRT algorithms is also aimed at reducing barriers.

E Implications of common human rights critiques

Judged on the basis of common human rights critiques of FRT, there is a temptation to consider that such systems may be acceptable in law enforcement and security contexts so long as:

- Their databases are built on images provided voluntarily and not obtained via indiscriminate, non-consensual internet scraping; and there is a process to ensure demographic diversity in the pool of images used to build the reference database;
- Their use is prohibited in the context of monitoring peaceful protest, given the particular risks of infringement and chilling effects;
- Their use as a law enforcement tool is typically restricted to RFR, rather than LFR, since that minimizes the chance of disproportionate and unnecessary bulk surveillance of individuals not involved in crime or terrorism;
- Where LFR is contemplated, the use of the technology is judicially authorized and/or notified to the public;
- Biometric information obtained via FRT is subject to robust data protection standards, particularly in respect of the security of storage and the requirement to delete such data when no longer required; and
- FRT system algorithms are transparent and explainable.

As considered below, however, the concerns relating to the use of FRT in the law enforcement and security contexts extend significantly wider, in particular concerning the impact of FRT on the integrity of the law enforcement process itself. As such, FRT, even when used outside of

live monitoring of protests, or even when subject to safeguards like pre-authorization and publicity, may continue to entail fundamental challenges to human rights protection and thus necessitate more detailed limitations. Indeed, even the use of FRT which has been largely accepted as an inevitable and positive contribution to law enforcement – namely retrospective use, akin to eyewitness identification supporting ordinary criminal investigations – is not without complex human rights risks.

V FRT reliability and impacts on investigative practices

As set out above, an important strand of human rights critique has considered the deployment by law enforcement of FRT in the context of protests, and highlighted its impact as a particularly intrusive form of bulk surveillance. Such use has disproportionately interfered in the privacy, expression, and peaceful assembly rights of people attending public events, and had a broader chilling effect on civic participation by those concerned about potential exposure.

The human rights impacts of FRT outside of protests are also vital to examine, and how the use of FRT can undermine respect for human rights in law enforcement and national security contexts in ways which cannot readily be remedied or mitigated. Even the sort of measures now widely recommended for adoption at protests, such as prior public notification of FRT use and stricter policies on the handling and deletion of data obtained from FRT, may not adequately remedy or mitigate these impacts. In these respects, this part focuses on LFR and RFR, since OIFR is not routinely employed by law enforcement authorities (though it does raise its own considerations, discussed below). Questions surrounding the reliability of FRT under real-world conditions are first outlined, before turning to three key, inter-related concerns with respect to the increasing reliance upon FRT (LFR and RFR) by law enforcement worldwide. First, there have been detrimental changes in investigative practices which have resulted from assuming the infallibility or reliability of FRT. Secondly, there have been opportunity costs from focusing too narrowly or intensively on technological solutions to complex investigatory problems. Thirdly, the relationship between law enforcement and the public is changing by virtue of the psychological distancing inherent in relying upon technological rather than human investigative methods.

A The reliability of FRT under real-world conditions

Leading figures in State law enforcement and security hierarchies have enthusiastically embraced FRT and highlighted its effectiveness, mirroring how law enforcement generally assumes FRT's accuracy. In 2023, the Commissioner of London's Metropolitan Police strongly endorsed FRT in all its uses, stating that 'live facial recognition is massively effective at picking out wanted offenders from crowds of people'; that '[t]he next step is more exciting: retroactively using facial recognition to identify unknown suspects from CCTV images is showing immense potential'; and that '[t]he results that we're getting are beyond what I expected and I think are going to transform investigative work, potentially, in the way that DNA transformed investigative work 30 years ago'.[154]

Such confidence is not justified by the performance of FRT systems under real-world law enforcement conditions. As previously noted, high reported accuracy rates of over 99 percent for FRT systems are derived from testing of OIFR verification (i.e. matching a single face to a known person's optimal reference image, such as a passport photo) under ideal conditions, with

consistent lighting and positioning, and where facial features are clear and unobscured.[155] The requirement, when undergoing verification, to remove glasses and refrain from smiling, will be familiar to many people: the purpose is to manipulate the face to maximize the FRT system's chance of an accurate return. But accuracy rates drop precipitously outside of OIFR verification. A recent US National Institute of Standards and Technology test of available FRT algorithms found that while 233 of 503 evaluated algorithms could achieve a 99 percent accuracy rate in the optimal verification environment, no algorithms were able to do so when seeking to identify a person from an unposed photo, where the subject was not looking directly at the camera, was in shadow, or was obscured, and the accuracy of some algorithms tested varied by orders of magnitude.[156]

Natural ageing presents a particular problem for FRT, for which many technicians are seeking solutions without clear breakthroughs.[157] It is particularly significant in law enforcement and national security contexts, since the reference database against which an LFR or RFR check is run often comprises images drawn from drivers' licences, police 'mugshots', passport photographs or other situations where individuals periodically interact with a State agency, and which may be many years out of date. Faces can change dramatically over time, and an interval of years between the enrolment of the image and a particular search being carried out has a significant impact on accuracy.

Further, the conditions under which FRT systems are tested are far removed from those in the real world, where pictures captured of individuals will often be imperfect so as to render FRT practically ineffective. This may be intentional – most obviously and easily by wearing a mask, something which has already become a fixture during protests where seasoned attendees presume that FRT will be used.[158] Or it may be unintentional – the reference image or the live image may be of poor resolution, or the weather, clothing, headwear or distance from a camera may inadvertently render a person difficult to identify.

In addition, there is also a significant divergence between the way in which FRT systems are tested in the laboratory and by government regulators – which is typically in respect of a one-to-one image match – and how they are used in everyday contexts by police and security agencies. Commercially-developed FRT systems marketed to law enforcement and security agencies are designed to find multiple plausible matches rather than a single positive match. That is because the system will typically return no matches if the accuracy requirement is made too stringent. Such a system would not be regarded as being so useful, and so system designers are at pains to avoid such an outcome. Depending on the sensitivities programmed into the system, an FRT program may 'purposefully escalate numerous – in some cases, hundreds of – non-matches for human consideration when queried with a probe photo of an unknown suspect, even if there is no true match for the suspect in the database'.[159]

The matches will be generated from the available reference pool, and so the broad subset of lookalikes will replicate any disproportionality in the demographic spread of reference data. This is one reason why the response often suggested to solve apparent racial bias in FRT outputs would not necessarily fix the human rights problem: as one academic has put it

> [e]ven if the software performed perfectly equally across demographic groups, the problem of lookalike false leads would still affect people of color disproportionately. One reason for this is that law enforcement agencies often exercise their authority disproportionality in communities of color. In addition, many agencies' face recognition applications rely on mugshot databases containing more faces of color. This leads to a somewhat higher likelihood that for any given person of color, a lookalike exists in the face recognition database.[160]

For example, the misidentification via FRT of a black community worker and anti-knife crime advocate in London,[161] is one of a number of apparent FRT mistakes in the UK regarding faces of colour.[162] Independent testing by the UK Government's National Physical Laboratory found in December 2025 that facial recognition algorithms more likely to incorrectly include some demographic groups in its search results, particularly Asian and Black people.[163]

Law enforcement analysts are tasked with making selections from the sample of possible matches identified by the FRT system, a task which even those with specific training in face identification will deliver high proportions of false positives. A substantial study in Australia, pitting non-specialists against professional facial examiners in matching persons against pools of images pre-selected by FRT, showed 'very poor face matching performance in a realistic photo-to-photo matching task based on the output of commercial off-the-shelf face recognition software'.[164] This is entirely unsurprising, since telling apart multiple people who have been specifically selected by an algorithm as looking very similar is prone to error. But the most important finding is that analysts also tend to do poorly when the images selected do *not* include the target, namely when the group of images presented are artificially manipulated to exclude an actual match with the target person. Trained facial examiners in the Australian study incorrectly identified a matching person 30 percent of the time even when there was no image of the target presented.[165]

1 Risks of falsification and 'spoofing'

The digital falsification of facial images could further undermine the reliability of FRT. All examinations of the accuracy of FRT algorithms assumes that the images provided on each side of the matching equation – the image from the reference database and the image requiring identification (taken from CCTV, body camera, still camera at a border gate, etc) – are reliable images on their own terms. That assumption relies upon eliding the unique biometric of a face on the one hand and *an image of* a face on the other. But that is not a secure assumption in the era of widespread digital manipulation and 'deepfake' technology by which images – particularly facial images – may be readily edited so that the identities of image subjects become uncertain and unsettled.[166] As the EU Agency for Fundamental Rights has noted, when assessing the supposed 'accuracy' of an FRT system 'questions in relation to how easily a system can be tricked by, for example fake face images (called "spoofing") are important'.[167]

A 'spoofing' strategy could, for instance, involve the creation via AI of thousands of images containing slight facial variations but apparently the same identity, all placed on the internet so as to undermine any reference set created through internet image 'scraping'. Alternatively, spoofing may occur by presenting a fake image (rather than a real face) so as to obtain wrongful verification through an OIFR system.[168] In addition, manipulation of individual images – which may be covert – may compromise the integrity of any of the data relied upon by any FRT system. As a result, even if the FRT approaches perfect accuracy in its capacity to match one image to another, it will never be able to be relied upon as an accurate identification of a real person as the subject who really was, or ought to have been, contained in any particular image. The issue of how to address malicious spoofing of FRT systems is a focus of FRT developers and researchers, and international technical standard setting, given the vulnerability of FRT-based verification tools (using OIFR) to such tactics.[169] As FRT becomes increasingly the norm in criminal and national security investigations, it can be expected that spoofing to avoid identification will similarly increase as a tactic of criminals and terrorists, jeopardizing the utility of FRT systems, however accurate they may become in matching digital images.

Among the checklist of features of biometric systems identified in the UN Compendium of recommended practices, while a face is a *universal* and *measurable* feature, the other elements identified are less certain. In marked contrast even to other biometrics, a face, or rather *an image of a face*, is *not permanent* and is capable of significant change. Those changes may be natural (such as from ageing, illness, drug use, or facial injury), artificial (disguise or cosmetic surgery), or present only in the image (the effect of angles, lighting, expression, or digital manipulation). Because of those variations, and because of other inaccuracies, an image of a person is not necessarily *unique* in the sense of being reliably the same as any previous reference image and incapable of being confused with any other person's image.

2 'Facial emotion recognition' and 'behavioural biometrics'

The scope for inaccuracy increases exponentially to the extent that FRT systems come to be supplemented by algorithmic decision-making tools which aim to use faces not only to identify persons but to infer their current or future behaviour or intentions, as in nascent 'facial emotion recognition' (FER) within the wider emerging field of 'behavioural biometrics'. As the European Data Protection Supervisor has explained:[170]

> Analysis of emotions based on facial expressions may not be accurate, as facial expressions can slightly vary among individuals, may mix different emotional states experienced at the same time (e.g. fear and anger, happy and sad) or may not express an emotion at all. On the other hand, there are emotions that may not be expressed on someone's *face*, thus inference based solely on facial expression may lead to wrong impressions. Additional factors can add to the ambiguity of the facial expressions, such as contextual uses (sarcasm), and socio-cultural context. In addition, technical aspects (different angles of the camera, lighting conditions and masking several parts of the face) can affect the quality of a captured facial expression. Furthermore, even in the case of accurate recognition of emotions, the use of the results may lead to wrong inferences about a person, as FER does not explain the trigger of emotions, which may be a thought of a recent or past event. However, the results of FER, regardless of accuracy limitations, are usually treated as facts and are input to processes affecting a data subject's life, instead of triggering an evaluation to discover more about their situation in the specific context.

At a fundamental level, it raises serious concerns for any decision-making carried out by AI systems seeking to draw conclusions about individuals on the basis of patterns identified in a dataset of other individuals' behaviour. It is true that AI systems can be trained on data to make inferences and predictions about individuals based on correlations between their characteristics – in the case of FER, the orientation and positioning of different points of the face in relation to each other – and what the training dataset contains. But what training dataset can truly demonstrate how the range of human emotions, including cross-culturally, are displayed consciously or unconsciously on the face in any manner other than by reliance on the broadest, and thus inevitably misleading, stereotypes? Further, as the UN High Commissioner for Human Rights has noted, 'the scalability of AI solutions can dramatically increase negative effects of seemingly small error rates'.[171]

3 FRT and artificial intelligence

Applying AI systems to biometric datasets raises substantial concerns. Firstly, AI analysis can only function properly when processing vast quantities of personal biometric data – by definition bringing potential risks of data leakage or misuse affecting large numbers of people. Secondly, AI-based decisions can trigger State action even though there is no evidence that a probabilistic pattern-based answer reflects reality – namely, the problem of the inability to

discern emotion identified by the European Data Protection Supervisor above. Thirdly, the opacity of AI-based decisions creates substantial obstacles for effective oversight and remedies, since the detailed functioning of the algorithm is extremely complex and likely incapable of being comprehensibly discerned even by technical experts.

Fourthly, since AI-based decision-making replicates and draws conclusions about correlations from historic data, it is unavoidably bound by the limitations, deficiencies, or biases in that data. If, for instance, a training database of emotions is coded by persons without expertise in recognizing emotions displayed by faces from diverse ethnic, national, or racial groups, the AI system will operate on the basis of an impaired set of instructions and will indefinitely replicate that deficiency. As a result, as the UN High Commissioner for Human Rights notes, AI tools 'carry an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus on policing of certain minorities'.[172]

4 Further risks of assuming reliability

In light of the discussion above, common assumptions as to the technological supremacy and utility of FRT (and/or FER) are misplaced and problematic. It is revealing that optimists compare FRT to DNA, since the experience of past assumptions about the infallibility of DNA technology in criminal investigation holds salutary lessons. Certain studies in the 2000s identified an empirical change in juror expectations that criminal charges should be supported by forensic evidence, particularly DNA.[173] This has been explained as having a dual legacy: on the one hand, jurors appeared to expect to receive detailed DNA evidence and considered cases built on other types of evidence as less compelling;[174] while on the other hand, the presence of any DNA evidence led to excessive deference being granted to that evidence over other matters,[175] despite proven issues with the reliability of DNA evidence.

Such a phenomenon has serious implications for the protection of human rights in law enforcement and security contexts, particularly concerning fair trial rights, the prohibition on discrimination, and the right of victims of human rights violations to effective remedies. A famous wrongful conviction for sexual assault in Australia depended upon a single DNA result (which turned out to be as a result of contamination during testing) to the exclusion of any other supporting witness testimony or circumstantial evidence.[176] A subsequent official investigation noted with concern that 'at virtually every point, and by almost everyone involved, [DNA evidence] was handled with so little insight into the issues which it presented that no need was seen to explore further or conduct research into them'.[177] A long-running investigation in Germany into the so-called 'Phantom of Heilbronn', a hypothesized female serial killer, was exclusively based on DNA samples found at numerous crime scenes across Europe. In 2009 the investigation was abandoned when it was concluded that all of the DNA evidence arose from contamination of collection swabs at their place of manufacture.[178]

Similarly significant errors are likely to arise from the dual implications of excessive faith in FRT: first, the belief that criminal charges that are not supported by FRT outputs are insufficiently evidenced, and secondly, that charges which are supported by FRT are essentially irrebuttable. Indeed, the risks compared with DNA are greater: DNA as a biometric is indelible and reliable (subject to processing errors), whereas the metric of an image of a face is neither indelible nor reliable, yet the deference afforded to it is similar. 'Confidence scores' attached to FRT matches can also be misleading, where results such as a '92 per cent match' can sound highly probative but may not correspond to real-world error probabilities.

Forensic experts tend to be much more cautious in considering the reliability of FRT than in the popular discourse of high-tech infallibility. A 2022 joint report on behalf of Interpol, the UN Interregional Crime and Justice Research Institute, the World Economic Forum, and a range of national police forces[179] noted, for instance, that:

> 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.[180]

Police forces sometimes officially repeat these caveats. The Chief of the Detroit Police Department (the force responsible for the wrongful arrests of two men mentioned in Part IV(C) above) stated in 2020 that '[i]f we were just to use the technology by itself, to identify someone, I would say 96 [percent] of the time it would misidentify'.[181] Chicago and New York police training materials also counsel against over-confidence in FRT match results.[182] The London Metropolitan Police Service ('MPS') requires human review of any FRT match result, albeit in terms which do not suggest any underlying scepticism about potential accuracy of the system. The document 'MPS Live Facial Recognition: Legal Mandate,' published in 2024, records that:

> [a]s a result of having taken reasonable steps to understand the statistical accuracy and demographic performance of the MPS LFR system … the MPS has adopted a "fail-safe" position to ensure that absence there being other lawful grounds to take policing action: no engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own opinion that there is a probable match between the member of the public and the Watchlist image.[183]

The caveats surrounding the published accuracy rates of FRT systems may well be understood by certain policymakers and leaders in law enforcement, namely that those rates are derived from tests under optimal conditions and do not attempt to replicate the poor quality of the majority of images which police officers will meet in practice. But it cannot be assumed that, even with appropriate instructions and training, members of law enforcement will always scrupulously apply the necessary scepticism to FRT outputs and treat them solely as directed as 'leads' rather than giving them undue weight. As a recent report into the 2019 arrest in Detroit of one of the men mentioned above put it:

> Detectives who received investigate leads generated by [FRT] may not be aware of any of [the] pitfalls, and may assumed that an AI search has found an exact match rather than, say, a similar-looking person whose picture, taken from social media, does not reflect the person's current appearance. The photograph of [the man] that led to his arrest for robbing the Detroit store came from an old driver's license. The analyst at the Michigan State Police who conducted the search didn't bother to check whether the license had expired – it had. Nor did she appear to consider why more recent pictures of [the man], which were also in the database, didn't turn up as candidates. The dated picture of [the man] 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 a morphological assessment of [the man's] face, including the shape of his nostrils, and found that his was the most similar to the suspect's. Two other algorithms were then run. In one of them, which returned two hundred and forty-three results, [the man] wasn't even on the candidate list. In the other – of an FBI database – the probe photograph generated no results at all.[184]

FRT matches could also reinforce 'confirmation bias' where there is an existing pattern of discriminatory over-policing of certain groups. The understandable reality is that busy law enforcement officers, bequeathed a supposedly accurate high-tech system, will be tempted to defer to the outputs generated by that system, and use it as a substitute for alternative investigative strategies, rather than simply as an additional investigative tool to be afforded no special status and only appropriate weight.

B Wider influence in justice and security systems

Beyond law enforcement professionals, the perception of FRT systems as accurate is likely to influence others involved in criminal justice decision-making. Firstly, law enforcement use of FRT is likely to increase the rate at which eyewitnesses inaccurately identify suspects. In law enforcement practice there is a well-known problem with eyewitnesses to crimes identifying individuals in a physical or photographic 'line-up' as the culprit, even when the culprit is not in the line-up. Reviews of eyewitness selection have found that, even when they are informed that the target individual may not be present in the line-up, and even when the culprit is not present, eyewitnesses still select somebody out of the line-up in 48 percent of cases.[185] Eyewitnesses, likely intending to assist an investigation and trusting that there is a real chance of the culprit being present, act with overconfidence to misidentify persons as perpetrators, resulting in a significant risk of wrongful convictions. Cross-racial identification errors are particularly pronounced.

Eyewitnesses are likely not familiar with the complexities and deficiencies inherent in FRT systems or in how they are typically used by law enforcement agencies. As such, it can be anticipated that they will be even more prone to assume that FRT-generated 'line-ups' accurately contain the perpetrator, and so will continue to misidentify persons who they simply recall (at whatever temporal interval) as looking like that person. The tendency of lay individuals to attribute greater accuracy to technology and computer outputs has a long history: it is often termed 'automation bias' and 'effectively turns a computer program's suggested answer into a trusted final decision'.[186] When coupled with a layperson's general deference to law enforcement and authority, the potential for errors to multiply and compound is clear. In the words of one review:

> Consider a scenario involving a law enforcement user as trained in facial examination as the best-performing group in the [Australian study]. If the user searched for a perpetrator who was captured on surveillance camera and the match did not appear in the candidate list, the … study indicates that the user might nevertheless erroneously select another candidate as an investigate lead as much as 30% of the time. If the user then asked an eyewitness to identify the candidate in a showup type procedure conducted just a few hours later … [studies] suggests that there is a greater than 50% chance the witness would erroneously say yes. Factoring these together, there could be as much as a 15% chance that when a perpetrator is not present or otherwise not found in a face recognition database used by law enforcement, a lookalike would be misidentified by law enforcement and then against by an eyewitness.[187]

Further, other decision-makers in the criminal justice system, particularly jurors, may be prone to deferring to the assumed integrity of FRT decision-making when assessing the likelihood that a selected individual was or was not involved in an incident. Appropriate judicial instructions to jurors are vital, along with stringent evidentiary rules to ensure that FRT evidence may be considered as probative and corroborative but not as conclusive, and that expert explanation of error rates and limitations can be provided. Even so, given the closed nature of the jury room, the effectiveness of such guidance on juries is not entirely clear.

The use of FRT in counter-terrorism and national security contexts is not limited to the criminal justice system. It may also form the basis of intelligence assessments and actions that do not involve criminal charges, but instead lead to covert surveillance, or administrative security measures imposed by executive authorities or the civil courts – such as terrorist listings, restrictive orders, administrative detention, or other preventive interventions. The human rights risks of such measures were examined in a 2025 report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[188] Particularly where such measures are imposed directly by executive authorities, there may be a lack of transparency about how police, intelligence and security agencies internally evaluate the probative value of FRT evidence, including by considering and weighting its limitations. Subjects of surveillance deriving from faulty FRT matches may not know that their privacy has been violated. A person notified of administrative measures may face barriers to obtaining disclosure of the FRT evidence from security agencies in order to effectively challenge it, while disclosure of evidence can also be heavily restricted in administrative tribunal or civil court proceedings that lack the full safeguards of criminal trials.

C Opportunity costs

The errors arising from the use of FRT in law enforcement contexts – and the risk of uncritical acceptance of such systems – are concerning per se. But the adverse impacts are exacerbated because FRT-based decision-making can displace other investigative methods which could contribute to more accurate outcomes. One opportunity cost arises from allocating financial resources to FRT systems instead of other policing demands. Across the world, investments in law enforcement are increasingly directed towards FRT. For instance, India's National Crime Records Bureau called for tenders to develop a centralized FRT system for Indian law enforcement – the Automated Facial Recognition System – at a cost of US$37 million.[189] Investment in state and city-level FRT projects in India has also occurred, in Bihar, Chennai, Chandigarh, Dharamsala, Delhi, Haryana, Hyderabad, Jammu and Kashmir, Odisha, Rourkela, Uttar Pradesh, and Uttarakhand. In 2024, the UK announced £55.5 million in funding for police FRT systems, comprising over 20 percent of its entire package of police funding proposals.[190]

Even if FRT investments supplement, rather than replace, human resources, experience suggests that officials will rely ever more on FRT systems in preference to traditional, more costly, and more labour- and time-intensive investigative methods. Longstanding police techniques like neighbourhood canvassing – the painstaking door-to-door process of asking potential witnesses what they may have seen – risks disappearing among police forces who routinely run FRT checks as the first step in an investigation. Indeed, the FRT industry has explicitly promoted FRT as a replacement for physical canvassing where agencies do not have sufficient human resources.[191] In the above-mentioned examples from the US in 2019 and 2020, basic checks of alibis, the presence or absence of any other biometrics like fingerprints, or apparent motives, appear not to have been conducted, and FRT was resorted to as the first – and presumptive – determination of guilt.

D Distancing from communities

The opportunity cost of attributing outsized prominence to FRT as an investigative tool is not limited to the investigative outcome of an individual case. The traditional methods of policing – manifested through on-the-ground strategies such as in-person interviews, site visits, and door-to-door canvassing – perform a dual function in policing practice. Human interaction between police officers and members of the public is traditionally considered, in theories of policing, to be a crucial building block of the public trust which conditions members of the public to cooperate and share information with law enforcement, rendering police information-gathering more efficient.[192] Crime prevention strategy has traditionally sought to cultivate community relationships through measures such as the Police Athletic League in the USA,[193] the Neighbourhood Watch movement,[194] the creation of volunteer Special Constables in the UK,[195] and similar engagement strategies internationally. 'Community policing' is expanding in various African States, including in areas heavily affected by terrorist groups. A broader risk of an FRT-led approach is that police may increasingly operate behind a digital screen of anonymity and at an increasing physical and psychological distance from the community, thus reducing face-to-face evidence gathering, the building of community relationships and information-sharing, and public trust.

The rapid adoption of FRT by law enforcement internationally, and in particular its deployment in the very settings where empathy and personal engagement is most challenging, such as crowd and protest settings, poses significant challenges from the perspective of police psychology. A gradual retreat of law enforcement professionals behind technological methods of investigation which reduce or sever community ties risks hardening police psychologies and removing the aversion to violence that comes from instinct, experience and training. iIn the same way, technological mediation in conflict settings (including in drone warfare) has been shown to reduce participants' natural aversion to violence, by removing the immediacy of human consequences.[196] As one leading criminologist puts it, 'distance has a long history of being seen as socially conducive to the infliction of pain'.[197] The psychological distancing which FRT-centred investigation entails risks increasing excessive police violence.

E Implications for human rights: Liberty and fair trial

The adverse impacts for criminal investigation set out above are also of concern because they jeopardize fundamental human rights, including the prohibition against arbitrary arrest[198] and the right to fair trial.[199] These concerns have received little consideration in the FRT debate.

1 Right to liberty

As the Human Rights Committee made clear in its General Comment on the right to liberty under Article 9 of the International Covenant on Civil and Political Rights (ICCPR), an arrest or detention may be technically authorized by domestic law but nonetheless arbitrary, since 'the notion of "arbitrariness" is not to be equated with "against the law", but must be interpreted more broadly to include elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality'.[200] Inaccurate FRT identification, coupled with a lack of rigorous alternative investigative methods to corroborate identification, may mean that there is an objective absence of reasonable suspicion to substantiate an arrest, resulting in arbitrary detention and a violation of the right to liberty. Further, Article 9(2) of the ICCPR requires law enforcement to inform an arrested person at the time of the arrest of the nature of the reasons for the arrest, and to promptly inform

the person of any charges. In respect of reasons, as the Human Rights Committee has set out, '[o]ne major purpose of requiring that all arrested persons be informed of the reasons for the arrest is to enable them to seek release if they believe that the reasons given are invalid or unfounded. The reasons must include not only the general legal basis of the arrest, but also enough factual specifics to indicate the substance of the complaint, such as the wrongful act and the identity of an alleged victim'.[201]

Police services using FRT systems as primary investigative aids may not be able to provide fully sufficient reasons or explanation as to why a particular person has been identified as a suspect, due to the 'black box' nature and proprietary algorithms of FRT systems.[202] In many circumstances, at the time of arrest law enforcement may realistically only be able to inform the suspect of the existence of the LFR or RFR image and that they were selected by the FRT system (and, if applicable, that there was confirmation by a human analyst or eyewitness from a subset of FRT results). The suspect and their legal representatives are unlikely to be able to effectively challenge the arrest and charges as contemplated by Article 9 of the ICCPR unless there is also disclosure of the tolerances of the FRT system, the particularities of how the system conducts the stages of face detection, face alignment, and face matching, and the images of the other persons suggested by the system but not selected as a positive match. In a proceeding challenging detention under Article 9, where liberty is at stake, it would be time-consuming, costly, and procedurally challenging to petition the court to compel the disclosure of such information, and for the person and their lawyer to acquire the necessary expert technical evidence to challenge the reliability of the FRT system and its use in the case.

2 Right to a fair trial

The same opacity behind investigative decisions based on FRT matches could also compromise the right to a fair criminal trial under Article 14 of the ICCPR. Article 14(3)(a) relevantly provides that, in all cases of criminal charges (whether or not the subject has been detained), the suspect has the right to be informed of the charge promptly and in detail, with a statement of both the law and the alleged general facts on which the charge is based.[203] Further, as the Human Rights Committee observed in General Comment No. 32, a fair hearing requires, among other things, that all parties have a real opportunity to review, examine, and contest all arguments and evidence.[204] With respect to digital evidence, what is required is that the evidence is intelligible, capable of interrogation, and has not been subject to interference or manipulation. Article 14 thus requires the authorities to arm wrongly accused persons (including through their lawyers) with the means to protect themselves and vindicate their rights, since the deficiencies in the case against them can be discovered and exposed in a fair hearing before an impartial tribunal.

Dominant reliance upon complex digital evidence can undermine these elements of a fair trial. If a person has been identified as a perpetrator on the basis of a FRT system, but the internal operating metrics of the system are either not fully disclosed or (just as likely) are not fully understood by the investigating authorities, the accused and their lawyers face insuperable obstacles to challenging that evidence. Information on the confidence threshold used in the selection of a match is crucial, but may be hidden in the code of a system and not obvious to users or targets. Detail on the size and integrity of the reference database may similarly be crucial for calculation of likely error rates, but may not be accessible by operators of the system, and indeed may be a proprietary secret of the software developer. Any history of data breaches or database vulnerabilities to spoofing, manipulation, systematic error, or other problems may be commercially sensitive and never revealed to authorities, despite the significance in order

to challenge the reliability of the FRT results. In addition, to ensure that law enforcement officers, lawyers and judges understand these matters, extensive training is required on how FRT systems work, what their limitations are, and how their results ought to be understood.

Uncertainty about the integrity of FRT evidence not only affects fair trial, it also calls into question the safety of convictions involving FRT generally, casting doubt on the integrity of proceedings and undermining investigations relying upon it, and potentially leading to costly compensation awards for wrongful convictions. The risk of undetected false positives at the investigative stage, and at trial, can also tie up scarce law enforcement resources and divert the authorities from focusing on the actual perpetrators and delivering justice for their victims.

3 Stronger guardrails on using FRT

The procedures governing the use of FRT in law enforcement and security contexts necessitate much more detailed examination than they have attracted to date because of the inherent vulnerability of FRT to error and/or manipulation, coupled with the complexity of understanding the extent and causes of those faults. Human rights-compliant deployment of FRT will, at a minimum, require that the FRT system is capable of disclosing, upon request, detailed information regarding the data upon which it has based its decisions, the confidence thresholds and accuracy sensitivities applied, and the data safety measures used. An acceptable auditable record might, for instance, explain precisely how the system has come to its conclusion, setting out, say, that the suspect's face was identified as a match with X percent of confidence against Y number of faces, allowing for the calculation of a percentage accuracy rate against population size. The demographic representativeness and any known biases in underlying datasets should also be disclosed. The use of FRT systems which are incapable of providing granular, and interrogable, information of this kind is unlikely to be compatible with human rights, regardless of other safeguards such as notice requirements, judicial authorization, proportionality assessments, and the like.

At the same time, State authorities should avoid disproportionate reallocation of resources to FRT systems as a substitute for other, perhaps more costly and time-consuming, investigative methods. The integrity of criminal investigation and the presumption of innocence (under Article 14(2) of the ICCPR) suggest that law enforcement should exhaust multiple fact-finding strategies, using electronic, human, and forensic means, in partnership with robust interrogation of potential alibis and motives, before arrest and criminal charges are pursued. Increasing reliance upon purportedly efficient impersonal techniques such as FRT risks eroding the proper investigative practices which underpin due process, and prevent wrongful convictions, injustice, and violations of human rights.

F Border management concerns

One use of FRT which deserves greater human rights analysis is its role in verifying traveller identity at international borders. The OIFR function of seeking to match a traveller's face to their passport image at an electronic border gate has become increasingly common as an alternative to border agent interviews.[205] It holds the promise of automating and rendering more efficient the border screening process, which represents a key choke point for international travel and which is also traditionally human resource-intensive.

The control of movements at international borders touches on a range of fundamental rights, including the right to freedom of movement (including to leave any country and to return to

one's own country),[206] the right to seek and enjoy asylum overseas,[207] the freedoms from arbitrary detention and arbitrary expulsion, and family rights, among others. The importance of protecting such rights can hardly be overstated: the ability to travel across borders is often the most immediate remedy for those persecuted in another country. Violations of the rights of freedom of movement and asylum often lead to further violations, including: arbitrary detention at the border; violence and reprisals against those denied asylum in countries to which they are returned; separation of family members, including children from their parents; and interference with the rights to health, education, work, and freedoms of association and peaceful assembly.

The General Assembly has urged States to 'adopt concrete measures to prevent the violation of the human rights of migrants while in transit, including in ports and airports and at borders and migration checkpoints'.[208] The Security Council, General Assembly and Human Rights Council have repeatedly reaffirmed that States must respect international human rights law and international refugee law while countering terrorism, including at borders. As the UNOCT Handbook on Human Rights and Screening in Border Security and Management acknowledges, States 'must have particular regard to the right of all persons to leave any country, including their own' since '[d]enial of boarding may put an individual at risk, and may deprive them of the opportunity to seek asylum' in another country.[209] OHCHR has made recommendations for digital border governance, emphasizing the need for human rights assessments of border technologies, including their cumulative impacts, along with oversight and remedies; banning the use and transfer technologies that cannot be used in compliance with human rights; and embedding use of technologies in a human rights-based approach to migration generally, including providing safe and regular migration pathways.[210]

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has emphasized in particular that terrorist 'watch-lists' must respect human rights, including the requirements of necessity, proportionality and non-discrimination, data protection, due process (including access to information), administrative and judicial review, and cooperation to ensure delistings are recognized in other jurisdictions.[211] In addition, where travel bans flow from counter-terrorism sanctions designations, the Special Rapporteur has identified essential best practices regarding the permissible grounds for listing (including a sufficiently high standard of proof); due process (including sufficient disclosure of the information supporting the listing to enable the person to effectively challenge it, instruct their lawyer and enjoy equality of arms in proceedings); and effective judicial safeguards.[212]

The stakes for human rights protection in border management are extremely high. The margin for error must accordingly be minimal, and any system to assist in border management must build in fail-safe mechanisms to ensure both accuracy of decision-making and adequate avenues for independent review. The increasing reliance upon automation via FRT as either an absolute precondition for, or the sole determinant of, border approval, places these rights in jeopardy. Mistakes are made as a result of the inherent vulnerabilities of FRT systems when operating at scale and speed, even in the relatively 'closed' verification environment of OIFR. In 2023, it was widely reported that the FRT function in the US Customs and Border Protection mobile 'app' for asylum claims ('CBP One') systematically failed to recognize thousands of (mostly Haitian or African) applicants due to apparent racial bias.[213] Further, CBP One – and all FRT-enabled border management programs – displays the familiar downsides of all complex software programs, including: unexplained outages or freezing;[214] inaccessibility to those without mobile phone access or with older mobile phones that cannot run a certain app; and vulnerability of stored data to leaks both inadvertent (as occurred with the leak of asylum seeker

details between two States)[215] and malicious (as occurred with a subcontractor's theft of 100,000 travellers' images and their sale on the dark web in 2019).[216]

As FRT-dependent border management systems proliferate, the frequency of errors will increase, including legitimate migrants and asylum seekers being denied their rights of movement and safety, and illegitimate entrants – potentially including threats to security – being wrongly allowed across borders. Protecting human rights in border management demands that FRT systems ought to never be the sole, or dominant, mechanism for traveller verification and decision-making about granting or refusing entry. The stakes are too high to outsource human rights-compliant decision-making to an automated system. State border agencies are unlikely to be able to comply with their human rights obligations if they excessively rely on automated FRT systems, given the acute need to carefully consider individual situations and to preserve access to effective remedies for adverse decisions. States must necessarily sacrifice a measure of technological efficiency in the interests of ensuring sufficiently robust human rights protection at the border.

OHCHR has urged Member States 'to provide effective remedies for violations of human rights at international borders, to provide reparation to victims and to bring State and private actors to account for such violations and abuses'.[217] The need for particular sensitivity to human rights in border management is amplified due to the many barriers to effective remedies. The liminal space of the border creates distinct legal and practical complexities for the vindication of rights, so States must be proactive in considering and mitigating human rights risks rather than relying upon victims to bring post facto claims for redress via the courts. One legal obstacle is the uncertainty about the jurisdiction within which a particular border management decision may be challenged. In the modern world of provision of biometric and biographical information prior to departure, a refusal of entry by State A may well take effect when the prospective traveller has not yet boarded their flight or ship, and so has not yet left State B. Technically, individuals subject to such a refusal should be regarded as being under the jurisdiction of the State responsible for screening (State A), regardless of their physical location in State B.[218] In other cases, a person arriving in one State may be denied entry based on their inclusion by another State in a terrorist watchlist that has been shared with the State of arrival, with no practical possibility to challenging the original listing decision in the foreign source country.

States typically have some formal judicial or administrative mechanism for challenging border or immigration decisions. But in real life, individuals will face considerable obstacles to accessing those remedies. They may lack knowledge of and practical access to the foreign State's judicial or administrative processes, as well as legal representation (especially since legal aid is likely not extended to foreign would-be arrivals outside the jurisdiction); there may be considerable language and financial barriers; and they may not be able to access remedies *promptly* so as to safeguard essential interests such as seeking refugee or humanitarian protection; and challenging the validity of biometric decisions in a timely manner at the border may be unrealistic. Further, if a person is fleeing their home country, they can hardly seek assistance from home authorities in challenging a travel refusal by foreign authorities.

VI Export/transfer of FRT

The global proliferation of FRT systems through exports and transfers is of considerable concern. The two leading States for corporate FRT exports are the US and China,[219] with other leading corporate exporters from Israel, Russia, and the European Union. The standard

framework that can assist in reducing the potential human rights harms flowing from technology exports is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ('the Wassenaar Arrangement'). (The binding Arms Trade Treaty does not apply to FRT.) The Wassenaar Arrangement is a multilateral export control regime involving political commitments by 42 participating States, including key States with thriving surveillance technology industries, including the US, UK, France, Germany, Russia, and Italy.[220]

The Wassenaar Arrangement maintains a regularly-updated list of conventional arms and dual-use goods and technologies agreed by consensus of the member States. 'Dual-use' goods or technologies are those not exclusively designed for, but that are capable of, military and security applications. States should restrict the export of these goods and technologies to other States where they may be misused by State or non-State entities. Each State undertakes to operate an export control regime covering the listed goods and technologies, and share information on export approvals and denials so that trends in their trade can be monitored. The Arrangement aims to promote transparency, responsibility and accountability in trade and to avoid the destabilizing accumulation of arms.

The Wassenaar Arrangement is not without its limitations. It is non-binding and implemented through voluntary domestic export control laws and standards.[221] Companies can 'offshore' operations – 'judicial arbitrage' – to avoid controls. A number of significant arms and technology exporting States, including China and Israel, are not members. Nevertheless, it represents the high point of integrating concern for human rights protection into international trade in certain harmful technologies. It has influenced controls in non-member States, including to an extent major exporters such as Israel and China. Importantly, its 'best practice guidelines' encourage States to avoid authorizing exports where, among other things, there is a clear risk of the violation of human rights, humanitarian law, sanctions, arms control; or of threats to peace or national security, terrorism, organized crime, or repression.[222]

FRT systems are not, however, within the scope of the Wassenaar Arrangement, not having been included in the last rounds of amendments to the dual-use list in 2012 and 2013, which added certain cyber and digital technologies, including intrusion software, IP network surveillance, and mobile device interception technologies (so-called 'IMSI-catchers').[223] As a result, the trade in FRT systems is not subject to any coherent global regulation of even the 'soft' kind under the Wassenaar Arrangement.

Certainly, some competent bodies have taken steps to address the risk of its international transfer, but the net effect is a patchwork of controls with very substantial gaps in coverage. The EU's Dual-Use Regulation (Regulation (EU) 2021/821), which broadly follows the Wassenaar list, does not specifically include FRT, although FRT that is part of 'cyber-surveillance items' could come within Article 5, thus restricting exports where there is a risk of internal repression, serious human rights violations or breaches of international humanitarian law. The European Union has also enacted piecemeal export control rules which restrict transfers of FRT systems to China and Belarus.[224]

In the US, the Export Administration Regulations also do not specifically address FRT, but it can fall within Commerce Control List restrictions on dual-use surveillance technologies, or restrictions relating to end users (which can include companies or entities that have engaged in repression, surveillance abuses, or targeting minorities or dissidents, including through the use of biometrics) or countries. Since 2024 the US has also been considering proposed rules to

specifically control the export and use of US-developed FRT systems, particularly for mass surveillance and crowd scanning, and to require an export licence for certain countries.[225]

Multilaterally, the Export Controls and Human Rights Initiative has worked since 2021[226] to enhance regulation, with over 20 States (including the US) adopting in 2023 a voluntary, non-binding 'Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights'.[227] It aims to prevent States and non-State actors from 'misusing surveillance tools and other technologies in ways that can lead to serious violations or abuses of human rights, including acts to censor political opposition and track dissidents, journalists, human rights defenders, other members of civil society, or individuals belonging to vulnerable groups'. It politically commits States to use domestic laws and tools to control the export of dual-use goods or technologies to end users that could misuse them for the purposes of serious violations or abuses of human rights. Given that it will operate within existing export control regimes, it does not represent a significant improvement or expansion of controls, and there has been little apparent momentum from additional States to join it since its adoption.

Even where common export control systems are in place, their practical effectiveness has been mixed, as evidenced, for example, by continued exports by some Western States in relation to conflicts in Yemen[228] and Gaza,[229] among others. Since authorizations are made (or withheld) by States authorities, administrative or judicial review by interested third parties can be challenging, particularly in the light of restrictions on disclosure, evidentiary uncertainties relating to past practices and future intentions, standards of review, differing interpretations of human rights and humanitarian law, the margin of discretion accorded to the executive in security- or foreign policy-related decisions, and issues of non-justiciability.

Elsewhere, China's foreign direct investment program is supporting the development of digital infrastructure worldwide, particularly in Africa. For example, its 'Smart Cities' program[230] has assisted cities in at least nine African States, including in Ethiopia, Kenya, Uganda, and Zimbabwe, to obtain a sophisticated 5G digital network supported by the Chinese company Huawei, combined with FRT-enabled CCTV cameras in public spaces provided by Chinese company Hikvision. The provision of 'turn-key' FRT systems worldwide multiplies the potential for harm caused by these mass surveillance technologies unless safeguards are built into such transfers. While China's export control regime, including for dual-use items, addresses security, sovereignty and economic issues, including to protect sensitive Chinese technologies, it does not explicitly address risks of human rights violations by end users.

Conclusion

The commercially-developed FRT systems which are becoming standard tools of law enforcement and national security practice worldwide were never designed with human rights protection in mind. These tools – while extremely sophisticated and increasingly capable – are marked by fundamental problems relating to inaccuracy, susceptibility to deceit and manipulation, and data protection (inadvertent and malicious). Their promise of efficiency and infallibility has been enthusiastically accepted by authorities globally, but their uncritical deployment without essential limitations and safeguards poses serious threats to human rights.

Those threats are manifest in the monitoring of public protests, where the use of FRT is generally considered unacceptable as a disproportionate infringement on privacy and the freedoms of expression, peaceful assembly, and association. Other law enforcement applications of FRT have compromised the rights to liberty, fair trial and effective remedy. In border management, greater sensitivity in individual cases than automated FRT decision-making affords is necessary to protect the rights to freedom of movement, asylum, liberty, due process in expulsion, family unity, and remedies. Effective mitigation of the risks posed by inappropriate uses of FRT confronts additional challenges given the proliferation and spread of the technologies worldwide and in the relative weakness of digital technology export controls.

Recommendations

The Special Rapporteur recommends that States adopt the following best practices to regulate FRT in law enforcement, counter-terrorism and national security contexts.

1 Legality and specific authority

Any proposed use of FRT, whether in the form of OIFR, LFR, or RFR, by law enforcement or security authorities must be specifically and clearly authorized by law, adopted after meaningful public consultation with relevant stakeholders, including technical and human rights experts. Legal authority must take into account the specific features and risks posed by particular uses of FRT systems. Blanket military, national security, law enforcement or border management exemptions must not be permitted; any tailored exceptions must be strictly necessary, proportionate and non-discriminatory, be consistent with human rights law, and must not deprive an individual of their right to an effective remedy.

2 Prohibitions on certain uses of FRT

The use of FRT systems must be prohibited in contexts where they cannot be used in compliance with human rights law or pose an unacceptable risk. This includes: (i) the use of LFR during public protests, as an indiscriminate and disproportionate infringement on the right to privacy, the rights to freedom of expression, peaceful assembly, and association, and the right to take part in public affairs; (ii) FRT databases (including those used to train algorithms as well as operational reference databases) that are sourced from untargeted, non-consensual scraping of images from the internet or surveillance footage; (iii) facial emotion recognition' tools, including polygraphs, since they lack empirical validation; and (iv) fully automated targeting decisions based solely on FRT matches. Where there is uncertainty about the human rights compliance of an FRT system, there must be a moratorium on its use until it is demonstrated that it can be used in a manner compliant with human rights.

3 Human rights due diligence assessments

States must require developers, investors and users to conduct rigorous, comprehensive, and sufficiently resourced human rights due diligence impact assessments of FRT systems, including to identify biases and impacts on vulnerable groups, mitigate potential adverse effects, or refrain from using them, and ensure alignment with international human rights law and national law. Assessments should consider the cumulative impacts of the use of FRT alongside other technologies and their legal frameworks, along with risks of function creep and repurposing.[231] Due diligence processes should engage all relevant stakeholders, including human rights experts and diverse civil society organisations.[232] Initial assessments require periodic review to adjust for performance, and should be subject to external review and validation and be made publicly available.

4 Permissible uses of FRT systems and human oversight

States must only deploy FRT systems where they are necessary and proportionate in pursuit of a legitimate criminal justice, public safety or national security aim. Their use must respect all relevant rights, including equality and non-discrimination, privacy and data protection, freedoms of association, peaceful assembly, expression and religion and belief, the right to information, the right to take part in public affairs, liberty, and rights to effective remedy and reparation.

States should ensure that FRT-based identification in law enforcement contexts is not, of itself, sufficient to designate a person as a criminal suspect or to subject them to further surveillance or restrictive administrative measures; and emphasize the need to continue to also apply conventional human and forensic fact-finding strategies. FRT should support, not replace, human decision-making. Qualified personnel must retain effective oversight of operational uses of FRT, including to safeguard against human rights violations.

Remote biometric identification targeting individuals should be subject to prior judicial authorization, with prompt post-facto authorization permissible in emergencies. In criminal trials, civil proceedings and administrative decision-making in security contexts, FRT systems must be capable of disclosing sufficiently detailed information regarding the data upon which decisions are based (including demographic representativeness and any biases), the confidence thresholds and accuracy sensitivities applied, and the data safety measures used.

5 Border management

Where OIFR is used to verify travellers in managing borders, FRT must not have the sole or determinative role in border decisions, and immediate human oversight and review must be available to prevent violations (including of freedom of movement of nationals, the right to seek asylum, the freedom of non-nationals from arbitrary expulsion or arbitrary denial of entry, family unity, non-discrimination, liberty, freedoms of expression, association and peaceful assembly, and the right to effective remedies). New technologies such as facial emotion recognition should not be used unless their reliability is validated. Border authorities must ensure transparency, explainability, dataset accuracy and non-discrimination in algorithms, and safeguard against inaccuracies and bias across demographic groups. Any use of FRT must provide safeguards for the rights to privacy, data protection and data security. Unnecessary and disproportionate over-collection of data must be avoided, and there must be rigorous safeguards on cross-border data sharing.

6 Transparency and explainability

Developers must design FRT systems to maximise transparency and explainability in how they function, thus enabling their operators to adequately understand and interrogate the functioning of algorithmic processes and their outputs, as well as the sources, currency and weighting of underlying datasets. FRT systems must be able to function in a manner that allows for comprehensible explanations of their operation, inputs and outputs, reasoning processes, limitations, and recommendations. Similarly, users of FRT systems must ensure transparency and explainability, including by notifying the public of their uses and disclosing sufficient information about their operation. Procurement processes for FRT should include assessments of a system's levels of transparency, explainability, record-keeping and auditability.

7 Data quality, testing and validation

FRT system developers and users should ensure that datasets are representative, ethically sourced, accurate, current, and relevant to the intended purpose. FRT systems should be rigorously tested and validated in environments that simulate their operational context, including to assess risks such as automation bias (namely, a deployer's over-reliance on FRT-enabled outputs); and they should be re-tested whenever they are modified or their intended purpose changes. Quality assurance or management systems should be established. Regular algorithmic audits must examine FRT systems for bias, accuracy, adverse impacts and interferences with human rights. Independent oversight bodies should evaluate training data quality, FRT algorithm performance across different groups, and potential discriminatory outcomes and profiling in surveillance and threat assessment.

8 Record keeping and audits

FRT systems must be capable of reliably and automatically recording how results were produced (including through specification of confidence thresholds, and disclosure of the size, source, and integrity of reference databases), and ensure that all records are retained, audited, and disclosed to criminal suspects and their lawyers, and to persons affected by administrative restrictions or potentially unlawful surveillance. Public registers should be maintained of FRT systems used in law enforcement, counter-terrorism and security.

9 Data governance

Legal frameworks must govern and ensure that data collection, access, processing, sharing, transfer, and storage practices are safe, secure and necessary and proportionate for legitimate law enforcement, counter-terrorism and national security purposes, in accordance with international law.[233] Authorities must implement data protection principles including data minimization, purpose limitation requirements, and secure erasure procedures while ensuring compliance with data protection, privacy legislation and adherence to human rights standards that safeguard other interdependent rights. Individuals should be notified when their personal data will become part of a dataset used by an FRT system.[234] As a general rule individuals and groups should also be empowered to consider, give and withdraw their informed consent to the use of their data and to choose how their data is used.[235]

10 Data security

FRT systems in law enforcement and national security settings present attractive targets for adversarial attacks, data poisoning activities such as the corruption of training data, and system manipulation. Multi-layered security architectures must protect against both external threats and internal misuse while maintaining system integrity and operational continuity.

11 Training and expertise

Law enforcement and security personnel likely to use FRT systems should be regularly trained on their legal frameworks, operations, features, limitations, and implications for human rights, including through a contextual and comparative analysis of the reliability of FRT systems and conventional investigative and verification strategies. Training should be available for those involved in oversight and accountability, including legal professionals and judges.

12 Independent oversight

Accountability requires effective independent oversight of FRT in accordance with best practice international standards.[236] Independent review bodies (such as national human rights institutions, privacy and data protection authorities, ombudspersons and courts) should monitor the use of FRT, investigate complaints, and ensure compliance with the law and human rights, while respecting confidentiality. Oversight mechanisms must have guaranteed independence, sufficiently broad powers, and adequate human, financial and technical resources (including FRT expertise). Oversight bodies must be given access to datasets, algorithms, stored data and audit trails, and have the capacity to review data retention and management practices and real-time digital operations, as well as inter-agency and cross-border data sharing.[237]

13 Effective remedies and accountability

State and private actors who use FRT should transparently disclose when and how FRT is used and publicise information about complaints and remedial processes. Companies should establish, maintain and adequately resource accessible and effective complaints mechanisms for remedying violations resulting from their systems. Victims of unlawful actions, including rights violations, must have recourse to an independent institution that can provide a binding, effective remedy, including full reparation. Procedures must ensure due process, including sufficient disclosure concerning algorithms, data sources and potential biases and access to lawyers. Justice must be accessible, including through legal aid in line with international law.

14 Export and transfer

States must not authorize the export or transfer of FRT systems where there is a clear risk that they would be used to violate international human rights law, humanitarian law or refugee law, including by mass or indiscriminate surveillance of public places or targeting of dissidents, journalists, civil society actors, human rights defenders, or minorities. The transfer of FRT must be subject to rigorous human rights due diligence. Where there is uncertainty about the human rights compliance of an FRT system, it must not be transferred until it is established that it can verifiably comply with human rights. FRT systems should be included in export control lists of dual-use technologies, including under national law and regional and multilateral arrangements. Processes to strengthen global governance of AI should address the high risks of AI-enabled FRT systems in law enforcement, counter-terrorism and security contexts.

15 International cooperation

International cooperation involving FRT, including via information exchange and sharing of evidence through mutual legal assistance, should incorporate binding human rights safeguards, including equal coverage of non-citizens. Data should not be shared where there is risk that it would be used in violating human rights, humanitarian or refugee law. Cross-border data sharing should be subject to independent oversight mechanisms. FRT identification should not be allowed on the basis of foreign terrorist watchlists that do not meet international standards regarding the grounds for listing and due process safeguards.

16 United Nations human rights due diligence

All relevant United Nations entities must assess the potential human rights impacts of providing capacity-building and technical assistance capacity in relation to FRT systems (including in relation to biometrics and border management tools), particularly regarding States with demonstrated records of human rights violations in counter-terrorism,[238] and in accordance with applicable United Nations policies, including on digital technology use.[239] Moratorium and suspension protocols on capacity-building and technical assistance should be established.

17 Military applications of FRT

States should endorse the International Committee of the Red Cross's recommendations on AI-enabled decision support systems (AI DSS),[240] which could include the use of FRT in identifying military targets. States and parties to armed conflicts must ensure that human control and judgement are preserved in decisions that pose risks to life, liberty, and human dignity (ICRC Recommendation 1) and ensure use in compliance with international humanitarian law (R11); systems should maximize transparency and explainability (R2); developers and users should mitigate bias to prevent discrimination (R4); legal reviews should be conducted wherever AI DSS forms part of a weapons system (R7); and users should assess information from all sources reasonably available when drawing on AI DSS outputs (R13). States should urgently negotiate a treaty regulating autonomous weapons systems, as advocated by the Secretary-General and the ICRC,[241] given the risks of FRT integrated into such systems.

• • •

Endnotes

1 See e.g. the 9 August 2024 joint letter to the UK Prime Minister by dozens of UK civil society organizations objecting to proposed 'wider deployment of facial recognition technology', https://www.accessnow.org/wp-content/uploads/2024/08/Joint-letter-to-Keir-Starmer-re-expansion-of-facial-recognition-technology-090824.pdf.

2 https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf.

3 A/69/397, [19].

4 D Coyle and L Hampton, '21st century progress in computing' (2024) 48(1) *Telecommunications Policy* 102649.

5 State agencies have frequently arrogated to themselves largely unchecked powers to intrude into individuals' lives by reference to broad and self-defined counter-terrorism objectives, as the mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has often noted: see A/76/261, [16]-[19].

6 The first relevant resolution was S/RES/2178 (2014), and the first reference to biometric and biographic information occurred in the follow-up resolution S/RES/2322 (2016), [3].

7 S/RES/2396 (2017), [15].

8 UNOCT, CTED, and Biometrics Institute, 'United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism' (2018) ('UN Compendium'), https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

9 Ibid, 12.

10 The generally-accepted starting point of modern facial recognition research is the work of Woodrow Bledsoe. See e.g. W Bledsoe, *A Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine*, King-Hurley Research Group (30 January 1963); W Bledsoe, *Facial Recognition Project Report*, PR-7, Panoramic Research Inc (6 March 1964); and W Bledsoe, *The Model Method of Facial Recognition*, PRI:15, Panoramic Research Inc (12 August 1964).

11 See T Kanade, *Computer Recognition of Human Faces* (1977).

12 See J Espindola, 'Facial Recognition in War Contexts: Mass Surveillance and Mass Atrocity' (2023) 37(2) *Ethics & International Affairs* 177.

13 For a discussion of the expansion of FRT in response to the Covid-19 pandemic, see K Huszti-Orbán and F Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?', University of Minnesota Human Rights Center, 19-20.

14 P Norstrom, 'Has Covid Increased Faith in Facial Recognition?' (2021) 11 *Biometric Technology Today* 5.

15 L Donohue, 'Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age' (2012) 97 *Minnesota Law Review* 407, 415.

16 H Aniulis, 'Facial Recognition Technology, Privacy and Administrative Law' (2022) 45(4) *UNSW Law Journal* 1513, 1516.

17 M Qandeel, 'Facial Recognition Technology: Regulations, Rights and the Rule of Law' (2024) 7 *Frontiers in Big Data* 1354659.

18 See https://www.unjspf.org/for-clients/digital-certificate-of-entitlement/.

19 An independent legal review of the use of LFR by UK police forces in 2022 recommended that such use be suspended pending the adoption of a legally-binding code of practice and a specific statutory framework: Ada Lovelace Institute, 'Independent legal review of the governance of biometric data in England and Wales: The Ryder Review' (2022), https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf.

20 D Murray, 'Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework' (2023) 87(4) *Modern Law Review* 833.

21 Ibid, 837-838.

22 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Position Paper on Protecting Human Rights while Using Artificial Intelligence to Counter Terrorism' (2025), https://www.ohchr.org/en/documents/position-papers/protecting-human-rights-while-using-artificial-intelligence-counter.

23 Article 19, 'Emotional Entanglement: China's Emotion Recognition Market and its Implications for Human Rights' (2021), https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

24 CORDIS, "iBorderCtrl: Grant Agreement ID: 700626", https://cordis.europa.eu/project/id/700626.

25 See H Du et al., 'The Elements of End-to-end Deep Face Recognition: A Survey of Recent Advances' (2021) arXiv:2009:13290v4.

[26] C Wilson, 'Clearview AI is Still Collecting Photos of Australians for its Facial Recognition Database', *Crikey* (8 February 2024), https://www.crikey.com.au/2024/02/08/clearview-ai-australia-facial-recognition-data/.
[27] See *Clearview AI Inc v Information Commissioner* [2023] UKFTT 819.
[28] M Djamaluddin et al., 'Normalization of Facial Pose and Expression to Increase the Accuracy of Face Recognition System' (2020) 1539 *Journal of Physics: Conference Series* 012035.
[29] See https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/.
[30] See P Bischoff, 'Facial Recognition Technology (FRT): Which Countries Use It?', *Comparitech* (24 January 2022), https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/.
[31] Z Li et al., 'Policy Designs for Adaptive Governance of Disruptive Technologies: The Case of Facial Recognition Technology (FRT) in China' (2023) 6(1) *Policy Design and Practice* 27, 31.
[32] US Government Accountability Office, 'Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used by Employees', GAO-21-105309 (13 July 2021), https://www.gao.gov/assets/gao-21-105309.pdf.
[33] J Clayton and B Derico, 'Clearview AI Used Nearly 1m Times by US police, It Tells The BBC', *BBC* (27 March 2023), https://www.bbc.com/news/technology-65057011.
[34] E Radiya-Dixit, 'A Sociotechnical Audit: Assessing Police Use of Facial Recognition', Minderoo Centre for Technology and Democracy, University of Cambridge (October 2022), Appendix A, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf.
[35] *Glukhin v Russia* [2023] ECHR 540, [5].
[36] Office of the Privacy Commissioner, 'Special Report to Parliament on OPC's Investigation into the RCMP's Use of Clearview AI and Draft Joint Guidance for Law Enforcement Agencies Considering the Use of Facial Recognition Technology' (10 June 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1.
[37] L Belli et al., 'Regulating Facial Recognition in Brazil' in R Matulionyte and M Zalnieriute (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (2024).
[38] S Bergh et al., 'Morocco's Governance of Cities and Borders: AI-Enhanced Surveillance, Facial Recognition, and Human Rights, in Matulionyte and Zalnieriute (eds), ibid.
[39] E Kavioliunaite-Ragauskiene, 'A Central-Eastern Europe Perspective on FRT Regulation: A Case Study of Lithuania' in Matulionyte and Zalnieriute (eds), ibid.
[40] See Eighth Review: A/RES/77/298 (2023), [53]; Seventh Review: A/RES/75/291 (2021), [50]; Sixth Review: A/RES/72/284 (2018), [41]. The use of biometric data complements adjacent UN initiatives such as the UNOCT-led Countering Terrorist Travel ('CT Travel') Programme, including its 'goTravel' software system, which has assisted States to use traveller information data in relation to terrorism database and cross-border information exchange.
[41] https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition.
[42] https://www.interpol.int/en/How-we-work/Forensics/Biometric-Hub.
[43] https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-unveils-new-biometric-screening-tool.
[44] A/HRC/41/41, [56].
[45] Ibid.
[46] A/HRC/41/41, [57].
[47] A/HRC/41/35, [12] and [66(a)].
[48] A/HRC/44/24, [24]-[26] and [30]-[38]. See also A/HRC/51/17, [32], [39], [40], [44], [46], and [49].
[49] K Huszti-Orbán and F Ní Aoláin, above n 13.
[50] A/HRC/48/31, [45] and [59(d)].
[51] The report of the discussion is at A/HRC/50/47 (2022).
[52] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Guidelines on Facial Recognition' (2021) ('Convention 108 Guidelines').
[53] Ibid, 19-21.
[54] Ibid, 21-22.
[55] Ibid, 22.
[56] A/HRC/RES/50/21, [29]. See also the Report of the Special Rapporteur on the rights to freedom of peaceful assembly and association, A/HRC/50/42, [58].
[57] https://www.ohchr.org/en/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner.
[58] UN Secretary-General, 'A Global Digital Compact – An Open, Free and Secure Digital Future for All', Our Common Agenda Policy Brief 5 (May 2023), [15].
[59] A/HRC/55/60.

[60] Such as the Code of Conduct for Law Enforcement Officials (A/RES/34/169) and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (ST/HR/1/Rev.6).
[61] A/HRC/55/60, [62(a)].
[62] A/HRC/55/60, [71].
[63] A/HRC/44/24, [53(f)].
[64] A/HRC/44/24, [53(j)(iii)].
[65] A/HRC/31/66, [77].
[66] https://globalprivacyassembly.com/wp-content/uploads/2022/11/15.1.c.Resolution-on-Principles-and-Expectations-for-the-Appropriate-Use-of-Personal-Information-in-Facial-Recognition-Technolog.pdf.
[67] ISO/IEC 19794-5 (biometric data interchange formats – face image data); ISO/IEC 30137 (biometrics in video surveillance); ISO/IEC 24745 (security and protection techniques); ISO/IEC 30107 (biometric presentation attack detection); ISO/IEC 27553-2 (security and privacy for biometrics on mobile devices); ISO/IEC 20059:2025 (resistance of biometric systems to morphing attacks).
[68] ISO/IEC 24358 (next generation of face-aware cameras); ISO/IEC 25447 (face image capture under less constrained conditions).
[69] Above note 22.
[70] There are exceptions to the prohibition under Article 9(2), including explicit consent of the person and for necessary and proportionate 'substantial public interest' purposes. Where an exception applies, safeguards apply to processing including data minimization (collect only what is necessary), purpose limitation, confidentiality, and the right to deletion. Fines of up to €20 million are available. Data protection impacts assessments are mandatory for biometrics (Article 35) and must document the necessity and proportionality of processing, risks to data subjects, and mitigation measures.
[71] European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement', Version 2.0, Adopted on 26 April 2023 ('EDPB Guidelines'), https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.
[72] Ibid, [105].
[73] Ibid, [107].
[74] Ibid.
[75] Ibid.
[76] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 12 July 2024 ('AI Act').
[77] AI Act, Article 5(1)(e).
[78] Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).
[79] AI Act, Article 5(1)(h)(i)-(iii).
[80] AI Act, Article 5(1)(g).
[81] AI Act, Article 5(3).
[82] Such as the Republic of Ireland. See JOL IRL 3/2022.
[83] See e.g. the basis on which the London Metropolitan Police Services relies: 'LFR for law enforcement purposes is not subject to dedicated legislation. Instead, in line with the way the Metropolitan Police Service (MPS) exercises its well-established common law and statutory powers, LFR is regulated by a number of sources of law': London Metropolitan Police, 'Live Facial Recognition: Legal Mandate' (20 March 2024), https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-legal-mandate-v.3.0-web.pdf, 2.The FBI relies upon its general mandate under the US Code and the Code of Federal Regulations as justification for its FRT system.
[84] Chiefly Clearview AI, InterlCenter, Marinus Analytics, and Thorn. See US Government Accountability Office, 'Facial Recognition Technology: Federal Law Enforcement Agency Efforts Related to Civil Rights and Training', GAO-24-107372 (8 March 2024), https://www.gao.gov/assets/gao-24-107372.pdf.
[85] Ada Lovelace Institute, above n 19.
[86] UK House of Lorde Justice and Home Affairs Committee, Conclusions and recommendations following a short investigation into the use of Live Facial Recognition (LFR) by police forces in England and Wales (2024), https://committees.parliament.uk/publications/43080/documents/214371/default/.
[87] *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 672 (Admin), [75]-[78]; and *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA), [38], [121].
[88] Zhonghua Renmin Gongheguo Geren Xinxi Baohufa [Personal Information Protection Law of the People's Republic of China], Promulgated by the Standing Committee of the National People's Congress on 20 August 2021, effective on 1 November 2021, Article 26.
[89] Garda Síochána (Recording Devices) Act 2023.
[90] *Glukhin v Russia*, above n 35, [83].

[91] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), Article 17; Universal Declaration of Human Rights 1948, Article 12.
[92] A/RES/71/199 and A/RES/73/179.
[93] A/HRC/RES/34/7.
[94] ICCPR, Article 19.
[95] ICCPR, Article 18.
[96] ICCPR, Article 21.
[97] ICCPR, Article 22.
[98] A/HRC/48/31, [27].
[99] *Glukhin v Russia*, above n 35 [66]. See also: *Gaughran v United Kingdom* [2020] ECHR 144, [70]; and *López Ribalda and ors v Spain* [2019] ECHR 752, [89].
[100] *Glukhin v Russia*, ibid, [76]. See also *Catt v United Kingdom* [2019] ECHR 76, [112] and [123]; UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, SHS/BIO/REC-AIETHICS/2021 (24 November 2021), [74].
[101] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 110, 4 May 2016, 1-88.
[102] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, 89-131.
[103] As noted by the Grand Chamber of the European Court of Human Rights: *Magyar Helsinki Bizottság v Hungary* [2016] ECHR 975, [165].
[104] ICCPR, Article 19.
[105] See *Gauthier v Canada*, Human Rights Committee (HRC), CCPR/C/65/D/633/1995, [13.4]; and *Aduayom, Diasso and Dobou v Togo*, HRC, CCPR/C/57/D/422-4/1990, [7.4].
[106] ICCPR, Article 21.
[107] ICCPR, Article 22.
[108] ICCPR, Article 18.
[109] HRC, General Comment No. 34, CCPR/C/GC/34 (2011), [2].
[110] Ibid, [11].
[111] *Handyside v United Kingdom* [1975] ECHR 5; (1976) 1 EHRR 737, [49]; and *Gündüz v Turkey* [2003] ECHR 652, [51].
[112] A/HRC/56/50, [9].
[113] A/HRC/RES/50/21, 2.
[114] The same point has been made by OSCE/ODIHR, 'Guidelines on Freedom of Peaceful Assembly' (3rd edition, 2020), CDL-AD(2019)017rev, [71]; and HRC, General Comment No. 37, CCPR/C/GC/37 (2020), [60].
[115] HRC, General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21), [60].
[116] A/HRC/44/24, [34].
[117] CCPR/C/GBR/CO/8 (28 March 2024), [52].
[118] Ibid, [53].
[119] *Goryunov and ors v Russia* [2024] ECHR 522, [13].
[120] Article 17 of the ICCPR does not expressly set out that interferences may be justified on the basis of a legitimate objective, but the consistent approach of the Human Rights Committee, in common with regional human rights courts, is to read that limitation into the scope of the right. See, for instance, *Van Hulst v Netherlands*, HRC, CCPR/C/82/D/903/1999 (2004), [7.6]-[7.10] and *Roman Zakharov Russia* [2015] ECHR 1065, [227].
[121] *Glukhin v Russia*, above n 35, [84].
[122] A/HRC/27/37, [24].
[123] HRC, General Comment No. 27, CCPR/C/21/Rev.1/Add/9 (1999), [14]; and HRC, General Comment No. 34, CCPR/C/GC/34 (2011), [34].
[124] HRC, General Comment No. 27, [13].
[125] A/HRC/41/41, [57].
[126] A/HRC/44/24, [53(i)].
[127] Special Rapporteur on Freedom of Expression and Access to Information in Africa, Inter-Session Activity Report presented to the 73rd Ordinary Session of the African Commission (20 October to 9 November 2022), https://achpr.au.int/en/intersession-activity-reports/special-rapporteur-freedom-expression-and-access-information-africa-0.

128 A/HRC/32/38, [57]. See also A/HRC/41/41, [56].
129 Ibid. See also A/HRC/29/32.
130 D Murray, 'Facial Recognition and the End of Human Rights As We Know Them?' (2024) 42(2) *Netherlands Quarterly of Human Rights* 145, 149.
131 N Richards, 'Intellectual Privacy' (2008) 87 *Texas Law Review* 387, 404.
132 J Penney, 'Understanding Chilling Effects' (2022) 106 *Minnesota Law Review* 1451, 1498.
133 Murray, above n 130, 152.
134 Ibid.
135 ICCPR, Articles 2 and 26.
136 See J Snow, 'Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots', *ACLU News & Commentary* (26 July 2018), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28.
137 H Ton-That, 'The Myth of Facial Recognition Bias', *Clearview AI Blog* (28 November 2022), https://www.clearview.ai/post/the-myth-of-facial-recognition-bias; and J Parker et al., 'What Science Really Says About Facial Recognition Accuracy and Bias Concerns', *Security Industry Association Blog* (23 July 2022), https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/.
138 K Johnson, 'How Wrongful Arrests Based on AI Derailed 3 Men's Lives', *Wired* (7 March 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
139 K Hill, 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match', *The New York Times* (29 December 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
140 K Hill, 'Wrongfully Accused by an Algorithm', *The New York Times* (24 June 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; see also K Hill, 'Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes' (29 June 2024), https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html.
141 A/HRC/56/68 (3 June 2024), [27].
142 As observed by Y Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) *Harvard Journal of Law and Technology* 890.
143 See National Institute of Standards and Technology, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software' (19 December 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; and J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', (2018) 81 *Proceedings of Machine Learning Research* 1.
144 See T Johnson and N Johnson, 'Police Facial Recognition Technology Can't Tell Black People Apart', *Scientific American* (18 May 2023), https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/; A Berland, 'How white engineers built racist code – and why it's dangerous for black people', *The Guardian* (4 December 2017), https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police.
145 See e.g. Committee on the Elimination of Racial Discrimination, Concluding Observations on the combined tenth to twelfth reports of the United States of America, CERD/C/USA/CO/10-12 (2022), [18]-[19]; A Beck, 'Race and Ethnicity of Violent Crime Offenders and Arrestees', US Department of Justice: Statistical Brief (January 2021), https://bjs.ojp.gov/content/pub/pdf/revcoa18.pdf.
146 J Blum, 'The NYPD's Gang Database: A New Age of Stop and Frisk', Surveillance Technology Oversight Project (23 July 2019), https://www.stopspying.org/latest-news/2019/7/23/the-nypds-gang-database-a-new-age-of-stop-and-frisk.
147 ICCPR, Article 2(3).
148 See e.g. Report of the Special Representative on Human Rights Defenders, A/56/341, [9].
149 HRC, General Comment No 31, CCPR/C/21/Rev.1/Add.11 (2004), [15]; CEDAW Committee, General Recommendation No. 33, [11]; and Inter-American Court of Human Rights, *Judicial Guarantees in States of Emergency*, Advisory Opinion OC-9/87 (6 October 1987), Series A No. 9, [24].
150 CEDAW Committee, General Recommendation No. 33, [1] and [14].
151 HRC, General Comment No. 31, [15].
152 CEDAW Committee, General Recommendation No. 33, [36]-[37].
153 A/HRC/27/37, [40].
154 M Weaver, 'Facial Recognition Could Transform Policing in Same Way as DNA, Says Met Chief', *The Guardian* (11 September 2023), https://www.theguardian.com/uk-news/2023/sep/11/facial-recognition-could-transform-policing-in-way-dna-testing-did-says-met-chief.

155 W Crumpler, 'How Accurate are Facial Recognition Systems – and Why Does It Matter', Center for Strategic and International Studies (14 April 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it.

156 See NIST, 'Face Recognition Technology Evaluation (FRTE) 1:N Identification' (3 July 2024), https://pages.nist.gov/frvt/html/frvt1N.html.

157 See, for instance: W Yao et al., 'A Study on the Effect of Ageing in Facial Authentication and the Utility of Data Augmentation to Reduce Performance Bias Across Groups' (2023) 11 *IEEE Access* 97118.

158 S Jeffries, 'Invisibility Cloaks and 3D Masks: How to Thwart the Facial Recognition Cameras', *The Guardian* (14 August 2019), https://www.theguardian.com/commentisfree/2019/aug/14/thwart-facial-recognition-cameras-invisibility-cloak-3d-mask.

159 L Moy, 'Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions' (2021) 30 *William & Mary Bill of Rights Journal* 337, 350.

160 Id., 357.

161 C Cuddeford, 'Anti-knife Activist Brings Legal Challenge to Met after he's Detained in Facial Recognition Failure', *MyLondon News* (4 June 2024), https://www.mylondon.news/news/south-london-news/anti-knife-activist-brings-legal-29285138.

162 J Clayton, 'I was Misidentified as Shoplifter by Facial Recognition Tech', *BBC News* (26 May 2024), https://www.bbc.com/news/technology-69055945.

163 www.gov.uk/government/publications/facial-recognition-technology-tests-national-physical-laboratory.

164 D White et al., 'Error Rates in Users of Automatic Face Recognition Software' (2015) 10 *PLoS One* 1, 10.

165 Ibid., 8.

166 M Qandeel, 'Facial Recognition Technology: Regulations, Rights and the Rule of Law', (2024) 7 *Frontiers in Big Data* 1354659, 5.

167 EU Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (2020), 9, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

168 Study of such spoofing of state-of-the-art commercial FRT software, admittedly in 2015, suggested a 70% false positive rate: see D Wen et al., 'Face Spoof Detection with Image Distortion Analysis' (2015) 10(4) *IEEE Transactions on Information Forensics and Security* 746.

169 K Watanabe et al., 'Spoofing Attack Detection in Face Recognition System Using Vision Transformer with Patch-wise Data Augmentation' (2022) *Proceedings of 2022 APSIPA Annual Summit and Conference* 1558; S Kumar et al., 'Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System', (2022) 22(14) *Sensors* 5160; L Li et al., 'Face Recognition under Spoofing Attacks: Countermeasures and Research Directions' (2018) 7(1) *IET Biometrics* 3.

170 European Data Protection Supervisor, 'TechDispatch on Facial Emotion Recognition' (2021), 3.

171 A/HRC/48/31, [18].

172 A/HRC/48/31, [24].

173 D Shelton et al., 'A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the "CSI Effect" Exist?' (2006) 9(2) *Vanderbilt Journal of Entertainment and Technology* 331; R Wheate, 'Australian Juries and Scientific Evidence' (2006) 38 *Australian Journal of Forensic Sciences* 75; and J Goodman-Delahunty and D Tait, 'DNA and the Changing Face of Justice' (2006) 38 *Australian Journal of Forensic Sciences* 97.

174 B Ley et al., 'Investigating CSI: Portrayals of DNA Testing on a Forensic Crime Show and their Potential Effects' (2010) 21(1) *Public Understanding of Science* 51; and M Young, 'Law vs Science: Genomic Evidence, Wrongful Convictions and the Requirement for a Statutory Framework' (2022) 19(1) *Canberra Law Review* 1.

175 H Machado and R Granja, 'DNA Technologies in Criminal Investigation and Courts' in H Machado and R Granja, *Forensic Genetics in the Governance of Crime* 45, 50-51.

176 K Rayment, 'Faith in DNA: The Vincent Report' (2010) 20(1) *Journal of Law, Information and Science* 238.

177 F Vincent, 'Report: Inquiry into the Circumstances that Led to the Convention of Mr Farah Abdulkadir Jama' (2010), 11.

178 C Himmerlreich, 'Germany's Phantom Serial Killer: A DNA Blunder', *Time* (27 March 2019), https://time.com/archive/6946145/germanys-phantom-serial-killer-a-dna-blunder/.

179 Interpol, UN ICRI, Nederlandse Politie, World Economic Forum, 'A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations' (Revised November 2022) ('Joint Policy Framework'), https://unicri.it/sites/default/files/2022-11/A%20Policy%20Framework%20for%20Responsible%20Limits%20on%20Facial%20Recognition.pdf.

180 Joint Policy Framework, 11.

181 J Koebler, 'Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time', *Vice* (29 June 2020), https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time.

182 Moy, above n 159, 354-355.

183 London Metropolitan Police, above n 83, 18.

184 E Press, 'In Front of Their Faces: Does Facial-recognition Technology Lead Police to Ignore Contradictory Evidence?' *The New Yorker* (20 November 2023), 23.

185 S Clark et al., 'Regularities in Eyewitness Identification' (2008) 32 *Law & Human Behaviour* 187, 203.

186 D Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249, 1272.

187 Moy, above n 159, 359.

188 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Best Practices To Protect Human Rights while Using Administrative Measures to Prevent Terrorism: Restrictive Orders, Terrorist Listings, Security Detention and Compulsory Interventions', A/80/284 (2025), https://www.ohchr.org/en/documents/thematic-reports/a80284-report-special-rapporteur-promotion-and-protection-human-rights.

189 See A Agrawal, 'NCRB Invites Bids to Implement Automated Facial Recognition System', *Medianama* (8 July 2019), https://www.medianama.com/2019/07/223-ncrb-invites-bids-to-implement-automated-facial-recognition-system/.

190 S Butler, 'Shoplifting Crackdown to Include £55m for Facial Recognition Tools in England and Wales', *The Guardian* (10 April 2024), https://www.theguardian.com/business/2024/apr/10/shoplifting-crackdown-to-include-55m-for-facial-recognition-tools-in-england-and-wales

191 E Hess, 'Top Five Misconceptions About Face Recognition', *Security Magazine* (28 April 2020), https://www.securitymagazine.com/articles/92242-top-five-misconceptions-about-face-recognition.

192 I Loader and A Mulcahy, *Policing and the Condition of England: Memory, Politics, and Culture* (2003), 2.

193 See https://national-pal.org/history-of-pal/.

194 R Yarwood, 'Neighbourhood Watch' in S Smith et al., *International Encyclopedia of Housing and Home, Vol 5* (2012), 90-95.

195 A Crawford, 'The Partnership Approach to Community Crime Prevention: Corporatism at the Local Level?' (1994) 3 *Social and Legal Studies* 497; and A Crawford, 'Appeals to Community and Crime Prevention' (1995) 22 *Crime, Law and Social Change* 97.

196 B Baggiarini, 'Algorithmic War and the Dangers of Invisibility, Anonymity, and Fragmentation', 2024 78(2) *Australian Journal of International Affairs* 257.

197 KF Aas, '(In)security-at-a-distance: Recalling Justice, Risk and Warfare in a Transnational Age', (2012) 13(4) *Global Crime* 235, 253.

198 ICCPR, Article 9(1).

199 ICCPR, Article 14(1).

200 HRC, General Comment No. 35, CCPR/C/GC/35, [12].

201 Ibid, [25].

202 B Garrett, 'Interpretable algorithmic forensics' (2023) 120(41) *Proceedings of the National Academy of Sciences* e2301842120.

203 HRC, General Comment No. 32, CCPR/C/GC/32, [31].

204 Ibid, [13].

205 See J Sanchez del Rio et al., 'Automated border control e-gates and facial recognition systems' (2016) 62 *Computers & Security* 49.

206 ICCPR, Article 12. See also A/RES/76/172 (2022) on the Protection of Migrants.

207 Universal Declaration of Human Rights, Article 14. The right is also contained in regional instruments. See League of Arab States, Arab Charter on Human Rights, Resolution 270, regular session 16 (23 May 2004), Article 28; Organization of African Unity, African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58, Article 12(3); Organization of American States, American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1979) 1144 UNTS 123, Article 22(7); and European Union, Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, 391-407, Article 18.

208 A/RES/76/172.

209 UNOCT UN Counter-Terrorism Centre, 'Handbook on Human Rights and Screening in Border Security and Management' (July 2020) ('UNOCT CTC Handbook'), 16.

210 OHCHR and University of Essex, 'Digital Border Governance: A Human Rights Based Approach' (2023), https://www.ohchr.org/en/documents/tools-and-resources/digital-border-governance-human-rights-based-approach.

211 'Human Rights Principles Applicable to Watchlisting', https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/ApplicablWatchlisting.docx.

212 A/80/284, above n 188, [17]-[39].

213 M del Bosque, 'Facial Recognition Bias Frustrates Black Asylum Applicants to US, Advocates Say', *The Guardian* (8 February 2023), https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias

214 A Kocher, 'Glitches in the Digitization of Asylum: How CBP One Turns Smartphones into Mobile Borders' (2023) 13 *Societies* 149.

215 H Aleaziz, 'DHS Accidentally Informed Cuba that Deportees had Sought Protection in the US', *LA Times* (19 December 2022), https://www.latimes.com/world-nation/story/2022-12-19/cuba-immigrants-deported-asylum-leak.

216 US Department of Homeland Security, Office of the Inspector General, 'Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot', (21 September 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

217 Office of the High Commissioner for Human Rights, 'Recommended Principles and Guidelines on Human Rights at International Borders' (October 2014), 13.

218 UNOCT CTC Handbook, above n 209, 17.

219 W Knight, 'China Is the World's Biggest Face Recognition Dealer', *Wired* (24 January 2023), https://www.wired.com/story/china-is-the-worlds-biggest-face-recognition-dealer/.

220 See generally https://www.wassenaar.org.

221 See e.g. in the USA: the Export Control Reform Act 2018, forming part of the 'John S McCain National Defense Authorization Act for Fiscal Year 2019', 132 STAT. 1636 (§§1741-1793), and the Export Administration Regulations, 15 C.F.R. §730 et seq.; in the EU: Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), OJ L 206, 11 June 2021, 1-461.

222 'Best Practice Guidelines for Exports of Small Arms and Light Weapons', https://www.wassenaar.org/app/uploads/2019/12/Best-practice-guidelines-on-export-of-SALW-web-version.pdf.

223 See Wassenaar Arrangement, 'Dual-Use Goods and Technologies and Munitions List' (2023), https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf.

224 Council Regulation (EU) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destablizing the situation in Ukraine.

225 See https://www.federalregister.gov/documents/2024/07/29/2024-16498/export-administration-regulations-crime-controls-and-expansionupdate-of-us-persons-controls.

226 The governments of Australia, Canada, Denmark, France, the Netherlands, Norway, the United Kingdom, and the United States have expressed support for the Initiative. See 'Joint Statement on the Export Controls and Human Rights Initiative', https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/.

227 https://www.state.gov/wp-content/uploads/2023/03/230303-Updated-ECHRI-Code-of-Conduct-FINAL.pdf.

228 Concerning UK exports to Saudia Arabia in connection with the conflict in Yemen: see *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] 1 WLR 5765 (CA); *R (Campaign Against Arms Trade) v Secretary of State for International Trade* [2023] EWHC 1343 (Admin); [2023] HRLR 11.

229 'Arms Exports to Israel Must Stop Immediately: UN Experts', https://www.ohchr.org/en/press-releases/2024/02/arms-exports-israel-must-stop-immediately-un-experts. Before the International Court of Justice see the pending case of *Alleged Breaches of Certain International Obligations in respect of the Occupied Palestinian Territory (Nicaragua v. Germany)*, https://www.icj-cij.org/case/193.

230 See Ministry of Foreign Affairs of the People's Republic of China, Forum on China-Africa Cooperation Beijing Action Plan (2025-2027), [7.3.3.], https://www.mfa.gov.cn/eng/xw/zyxw/202409/t20240905_11485719.html.

231 A/HRC/51/17, [56(c)].

232 See also Global Digital Compact, A/RES/79/1, Annex, [32(a)].

233 Ibid, [39(c)].

234 A/HRC/48/31, [55].

235 Global Digital Compact, A/RES/79/1, Annex, [39(d)].

236 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies', A/HRC/14/46, 2010; Global Counter-Terrorism Forum, 'Brussels Memorandum on Good Practices for Oversight and Accountability in Mechanisms in Counterterrorism' (2024).

237 See also A/HRC/52/39, [50].

238 See also A/HRC/52/39, [58].

239 Human Rights Due Diligence for Digital Technology Use: Guidance of the Secretary-General (2024), https://www.ohchr.org/sites/default/files/2024-08/digital-technology-use-guidance-sg-1-en.pdf and Practical Guide, https://www.ohchr.org/en/documents/tools-and-resources/human-rights-due-diligence-digital-technology-use-guidance; Human Rights Due Diligence Policy on United Nations support to non-United Nations Security Forces (2013), A/67/775–S/2013/110, https://www.ohchr.org/sites/default/files/Documents/HRBodies/SP/AMeetings/20thsession/IdenticalLetterSG25Feb2013_en.pdf.

240 ICRC, 'Submission to the United Nations Secretary-General on Artificial Intelligence in the Military Domain', 2025, 6, https://www.icrc.org/sites/default/files/2025-04/ICRC_Report_Submission_to_UNSG_on_AI_in_military_domain.pdf.

241 'UN and Red Cross Call for Restrictions on Autonomous Weapon Systems to Protect Humanity', UN News, 5 October 2024, https://news.un.org/en/story/2023/10/1141922.