INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

JANUARY 2021

IN FOCUS

FACIAL RECOGNITION TECH STORIES AND RIGHTS HARMS FROM AROUND THE WORLD

Contents

Introduction

From Delhi to Detroit, Budapest to Bogota, Facial Recognition Technology (FRT) is being rapidly deployed in public and private spaces across the world.

As of 2019, 64 out of 176 countries[1] were using facial recognition surveillance systems. In the US alone, more than 50 percent of all American adults were in a police recognition database, as of 2016[2].

Law enforcement agencies say they use FRT for law enforcement purposes. For example, the FBI in the US has testified that FRT "produces a potential investigative lead"[3].

Traditionally, FRT surveillance systems work by locating one or more faces in a moving or still image from a camera before determining unique facial features from that image. The system then runs that image, without consent, against an existing database or 'watch list' of images derived from police mugshot databases in the pursuit of a match. Other FRT systems can examine demographic trends or carry out sentiment analysis by scanning crowds, again without consent.

These systems have renowned ethnic, racial and gender biases[4] against people of colour and women. This means that image-matching FRT systems, used by law enforcement agencies, are more likely to misidentify people of colour and females than white males. Such inaccuracies were illustrated in 2019 when the UK's Metropolitan Police FRT system was found to have an error

rate of 81 per cent[5]. One can only contemplate the grave implications of such inaccuracies, and consequent chilling effect on the right to protest, when one considers the indiscriminate screening of crowds during protests. For example, police in India used FRT and driving licence and voter identity databases to 'identify' 1,900 protesters[6] during riots in Delhi in February 2020.

But technology is always improving and serious ethical issues arise no matter how accurate the technology may become. One only needs to consider how surveillance firm Hikvision has come under renowned criticism for allegedly providing FRT equipment in Xinjiang, China, where Uighur Muslims are being forcibly detained[7] in detention centres. Just because a tool is accurate, does not mean it's ethical.

In June 2020, the Association for Computing Machinery's US Technology Policy Committee found these biases to be "scientifically and socially unacceptable"[8]. It found they compromise individuals' fundamental human and legal rights to privacy, employment, justice and personal liberty. The group called for all uses of FRT to be suspended immediately, saying it can cause "profound injury" to the lives, livelihoods and fundamental rights of individuals, particularly the most vulnerable in society.

Pushback against FRT has occurred elsewhere in the world in 2020. In the UK, the Court of Appeal found that the use of automated FRT by the South Wales Police was unlawful[9]. In Canada, Clearview AI, which scrapes images from social media sites[10], builds a database, and offers clients, including law enforcement agencies, access to that database, withdrew[11] from the country. This followed the launch of a probe into the use of the tech by police by the Privacy Commissioner. In Moscow, protesters lodged a complaint[12] with the European Court of Human Rights, over Russia's use of FRT at protests; and in Israel, refusals by the Israel Police and Israel Defence Forces to reveal the use of FRT in both Israel and West Bank has been met with resistance from a civil rights group[13].

This report focuses on the multiple ways in which the growing use of FRT affects the everyday lives of citizens across 13 countries in the Americas, Africa, Europe, Asia and Australia. These stories from 13 member organisations of the International Network of Civil Liberties Organisations (INCLO) outline how this surveillance can harmfully discriminate and infringe on a plethora of rights including people's right to privacy and their freedoms of expression, and association and assembly.

Each story is unique to each member country but, considered together, they reveal how this harmful surveillance has become pervasive and entrenched in private and public spheres across the world. They also collectively illustrate the need for public, democratic debate about the use of this technology and for robust laws to safeguard citizens around the same.

FRT &

The right to freedom of expression

01

FRT and the right to freedom of expression

Olga Cronin, Irish Council for Civil Liberties

FRT systems and algorithms traditionally scan crowds indiscriminately in the pursuit of capturing and detecting[14] the facial characteristics of as many people as possible, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics.

Given FRT systems' blanket collection of this most sensitive of personal data at specific locations and events - including protests, demonstrations and religious events - it's clear that this practice has the potential to discourage people to publicly express their opinion or, in countries with autocratic rulers, it could lead to the apprehension or prosecution of those who choose to do so.

The right to freedom of expression is asserted in Article 19 of the Universal Declaration of Human Rights[15]; Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[16]; Article 9 (2) of the African Charter on Human and People's Rights[17]; Article 10.1 of the European Convention on Human Rights[18], Article 13.1 of the American Convention on Human Rights[19]; and principle 23 of the Human Rights Declaration[20] adopted by the Association of Southeast Asian Nations (ASEAN).

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression David Kaye in 2019 highlighted[21] that the intrusiveness of FRT is probably no more demonstrable than in China where FRT is reportedly used to track and control some 11 million Uighurs[22], a largely Muslim minority and one million of whom are believed to be in detention camps.

FRT and its potential to infringe on the right to freedom of expression was something that was referred to in the landmark Ed Bridges/Liberty case in the UK. In this case, a protester took action against the South Wales Police after his face was scanned while Christmas shopping and, separately, while at a protest.

Mr Bridges and INCLO member organisation Liberty criticised the police's Data Protection Impact Assessment (DPIA) of the technology, arguing that the DPIA carried out by the police was silent as to the risks to some rights that the technology would infringe, including the right to freedom of expression. The UK Court of Appeal ultimately found that the DPIA did not adequately consider the risks[23].

To ignore the risks that FRT pose to the right to freedom of expression is to ignore them at our peril.

As Mr Kaye determined in his report to the Human Rights Council: "Interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression."[24]

UK Court of Appeal finds face scanning to be unlawful

Hannah Couchman, Liberty

What

The UK Court of Appeal ruled in favour of civil liberties campaigner Ed Bridges when it found that the use of automated FRT by the South Wales Police was unlawful. It followed Mr Bridges, who was represented in court by Liberty, taking action against the police after he had his face scanned on two occasions by the technology, while Christmas shopping in Cardiff city centre on December 21, 2017, and while at a peaceful anti-arms protest at the Motorpoint Arena in Cardiff on March 27, 2018.

> This technology is an intrusive and discriminatory mass surveillance tool. For three years now South Wales Police has been using it against hundreds of thousands of us, without our consent and often without our knowledge. We should all be able to use our public spaces without being subjected to oppressive surveillance.
>
> • ED BRIDGES, CIVIL LIBERTIES CAMPAIGNER[25]

WHERE CARDIFF, WALES
WHEN DECEMBER 21, 2017 AND MARCH 27, 2018

Further details

Police in South Wales scanned approximately 500,000 faces while using automated FRT in a pilot project known as AFR Locate on about 50 occasions between May 2017 and April 2019 at different public events. Mr Bridges brought a claim for judicial review on the basis that the technology, among other things, was not compatible with the right to respect for private life under Article 8 of the European Convention on Human Rights or data protection legislation.

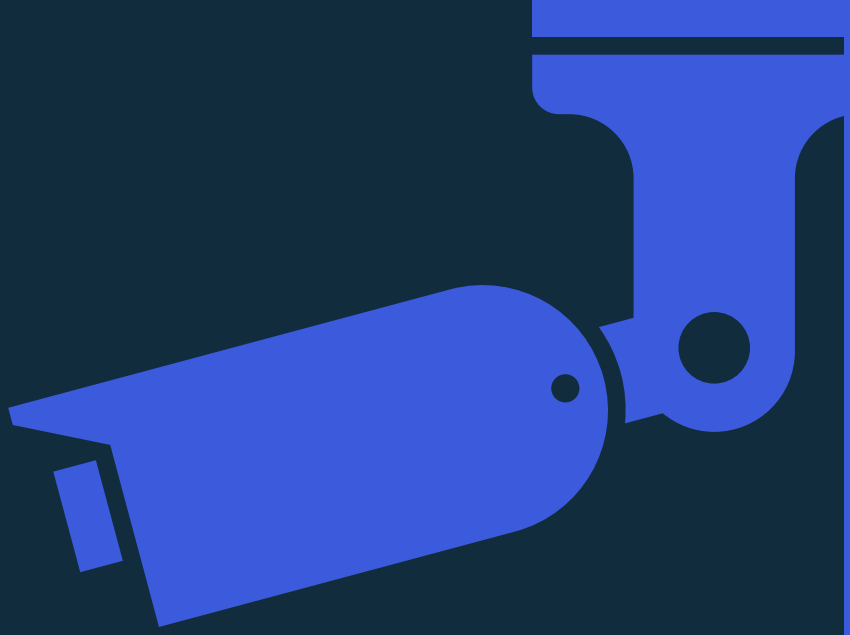
The type of technology at the heart of this case extracted faces captured in a live feed from a camera and then automatically compared them with faces on a police watchlist. If no match is detected, the software automatically deletes the facial image captured from the live feed. However, if a match is detected, a police officer would be alerted and would review the images to determine if action is necessary.

Harm to rights and freedoms

In its judgment[26], the Court of Appeal found that the police use of this technology was unlawful and in breach of privacy rights and data protection law. It also found that the police did not independently investigate whether the technology discriminated on racial or sex grounds and equality law. Specifically, it found there was an insufficient legal framework to make the violation of privacy rights under Article 8 of the European Convention on Human Rights "in accordance with law". The court also found that the Data Protection Impact Assessment carried out by the police did not comply with the law.

Legal and campaign action

Liberty acted for Mr Bridges in court. Liberty lawyer Megan Goulding said[27]: "The court has agreed that this dystopian surveillance tool violates our rights and threatens our liberties... It is time for the [UK] Government to recognise the serious dangers of this intrusive technology. Facial recognition is a threat to our freedom – it needs to be banned." A petition by Liberty[28] calling for a ban on the use of FRT in public has been signed by more than 50,000 people.



FRT &

The right to equality and non-discrimination

02

FRT and discrimination

Gil Gan-Mor and Avner Pinchuck, Association for Civil Rights in Israel

The use of FRT has real and significant potential to strengthen structural inequalities and discrimination and/or exacerbate existing inequalities. These harms may be predominantly caused by failures in the technology's algorithms.

Research to date indicates that FRT is biased against people of colour and women. In 2018, a study by MIT and Stanford University tested commercially released facial-analysis programs from three different manufacturers of FRT. It determined errors in gender classification in more than 20% of the cases related to faces of dark-skinned women. In contrast, the error rate among light-skinned men was less than 1%.[29].

Another comprehensive study conducted in the US by the National Institute of Standards and Technology[30] found that face-recognition technology suffers from a significant bias that leads to misidentifications of people of African and Asian descent.

It found that false positive rates are highest among West and East African, and East Asian people, and lowest among Eastern European individuals; that false positive rates are higher among women than men; and there are elevated false positives among the elderly and children.

When technology forms the basis of a police investigation, the bias is likely to lead to disproportionate incrimination and wrongful indictment among minority groups.

Another concern is the use of technology to govern and monitor different minority groups, and to over-police them, by placing cameras connected to the technology in areas identified with those minority groups.

Wrongful arrest and detention in the USA

Ben Wizner, American Civil Liberties Union

What

Detroit resident Robert Williams was arrested after FRT used by the Michigan State Police erroneously matched him with a wanted watch thief. Attempts by Mr Williams and the American Civil Liberties Union to get details about the events leading to his arrest have been stonewalled[31]. The Detroit Police Department has since admitted the FRT it uses has a 96 per cent[32] error rate.

> I never thought I'd have to explain to my daughters why Daddy got arrested. How does one explain to two little girls that a computer got it wrong, but the police listened to it anyway?
>
> • ROBERT WILLIAMS

WHERE MICHIGAN, USA
WHEN JANUARY 9, 2020

Further details

In October 2018, someone shoplifted five watches, worth $3,800, from a Shinola store in Detroit. Over a year later, FRT later mismatched a grainy still of the baseball cap-wearing thief from CCTV footage captured at the store with Mr Williams' driver's licence. The grave error resulted in Mr Williams getting handcuffed and arrested at his home in front of his wife and two daughters[33] before being detained for 30 hours. He was subsequently arraigned on a first-degree theft charge and received a $1,000 bond. After his arrest, Mr Williams was brought to a detention centre where police took his mug shot, fingerprints and DNA before he was held overnight. While being interrogated the following day, it became obvious that he was arrested based on a false FRT match. The charges were later dropped[34].

Harm to rights and freedoms

What occurred to Mr Williams shows how FRT can lead to misidentification, result in serious invasion of privacy, lead to wrongful arrests and/or detentions, and obstruct the principles and requirements of due process and procedural fairness, i.e. where individuals are treated fairly.

Legal/campaign action

ACLU of Michigan filed a complaint[35] with the city of Detroit stating that the wrongful arrest of Mr Williams "disrupted his family life, resulted in his unjustified jailing, and violated all norms of reasonable policing and investigation". The letter specifically called for the case against Mr Williams to be outright dismissed without prejudice; that he should receive a public apology; that the Detroit Police Department stop using FRT as an investigatory tool; that any photographs of Mr Williams be removed from any police FRT database; and that Mr Williams' mugshot taken after his arrest be expunged from all police and state records. In addition, ACLU is helping to lead a broad coalition which is pushing for greater community oversight[36] and control over police use of surveillance technologies in Detroit[37].

For years the ACLU has been advocating against police use of FRT. Multiple locations, such as San Francisco, Berkeley and Oakland in California, as well as Cambridge, Springfield, and Somerville in Massachusetts, have since banned police from using FRT. Amazon and Microsoft have recently announced they will not sell FRT to police for some time but they have yet to clarify[38] their positions on the sale of the technology to federal law enforcement agencies like the FBI and the DEA.

Surveillance in the West Bank

Gil Gan-Mor, Association for Civil Rights in Israel

What

Palestinians in the West Bank who seek permits to enter Israel must get photographed and fingerprinted at an Israeli military office. These photographs are stored in a biometric database and are also connected to electronic ID cards that Palestinians scan at checkpoints when they enter Israel. As of August 2019, 450,000 Palestinians, out of the approximate 2.7million Palestinians living in the West Bank, had electronic ID cards and their photographs stored in the biometric database. FRT software at the checkpoints scan their faces and this is compared to the photographs held on Israel's biometric database.

> "This is a technology that, by its nature, allows tracking of massive numbers of people, not just criminals, and has the potential to harm everyone.
>
> • GIL GAN-MOR, DIRECTOR OF THE CIVIL AND SOCIAL RIGHTS UNITS, THE ASSOCIATION FOR CIVIL RIGHTS ISRAEL (ACRI) [39]

Further details

Since 2018 Israel has been using FRT at West Bank checkpoints[40] to verify Palestinians' identities[41] as they enter Israel. FRT is not used at checkpoints for Israeli settlers or other Israeli commuters moving between the West Bank and Israel. The FRT software used was developed by Israeli tech company AnyVision who has previously received significant investment from Microsoft. In October 2019, Microsoft hired[42] former US Attorney General Eric Holder to examine how AnyVision's technology was being used and to find out if AnyVision complied with Microsoft's own ethical principles[43] on how biometric surveillance technology should be used. It followed reports that AnyVision was carrying out mass surveillance in the West Bank.

In March 2020, Microsoft pulled its financial support for AnyVision even though Microsoft and AnyVision jointly announced that Mr Holder's audit did not substantiate[44] any breach of Microsoft's principles. The audit also found[45] AnyVision's technology "has not previously and does not currently power a mass surveillance program in the West Bank that has been alleged in media reports". There are also concerns that the Israel Defence Forces (IDF) or police also use live FRT to track the movements of Palestinans in the West Bank

WHERE WEST BANK
WHEN SINCE 2018

as demonstrated in an AnyVision demonstration video[46] obtained by NBC news.

Harm to rights and freedoms

The rights to privacy, assembly, associate and the freedom of movement are all engaged by this biometric ID system of which Palestinians, seeking to enter or work in Israel, appear to have little or no means to opt out. Such a system also lends to the creation of police visual databases for future use which could lead to potential misidentification, wrongful arrest and detention.

Legal action/Campaign action

The Association for Civil Rights in Israel (ACRI) filed a petition[47] to the Administrative Court in Jerusalem in September 2020 after the IDF refused to answer a Freedom of Information request about the use of in FRT in the West Bank. The IDF claims that revealing this information would possibly expose methods of operation and infringe on the security of the state. An additional petition was filed by ACRI against Israel Police who also refused to reveal any information about its use of FRT.

Fears of AI-powered apartheid in South Africa

Edwin Makwati, Legal Resources Centre

What

The ongoing roll-out of 15,000 artificial intelligence-powered CCTV cameras across Johannesburg in South Africa has prompted fears that, if not properly regulated, it will drive AI-powered apartheid[48], discrimination, security threats and privacy infringements. It's feared that as more areas install these Vumacam cameras, with in-built bias problems against people of colour and women, it will lead to racial profiling and a further normalisation of mass surveillance.

> South Africa's Constitution is founded on the values of human dignity, the achievement of equality and freedoms and takes due cognisance of the inequalities occasioned by the country's repressive past. The installation of FRT without appropriate safeguards is a threat to these shared values, as these unfettered infringements have no regard for the privacy of persons and their freedom of expression.
>
> • EDWIN MAKWATI, ATTORNEY AND LEGAL RESEARCHER, LEGAL RESOURCES CENTRE (LRC)

Further details

Vumacam is a privately owned company. The network is privately funded and vetted security companies pay to access the feed in their areas. Overview and licence plate recognition cameras are streamed via a fibre network to a data centre that records or queries databases of vehicles of interest, such as vehicles that might be stolen. Machine learning systems perform video analytics to recognise things in the video, such as objects or behaviours. With enough cameras, computers could intelligently "watch" the neighborhood and notify private security forces in real-time when the algorithm detects something it deems suspicious. Security companies enter into a contractual agreement with Vumacam, which grants them access to the feed. In the event they need footage, they have to approach Vumacam with official documentation from the SAPS (South African Police Service).

WHERE JOHANNESBURG, SOUTH AFRICA

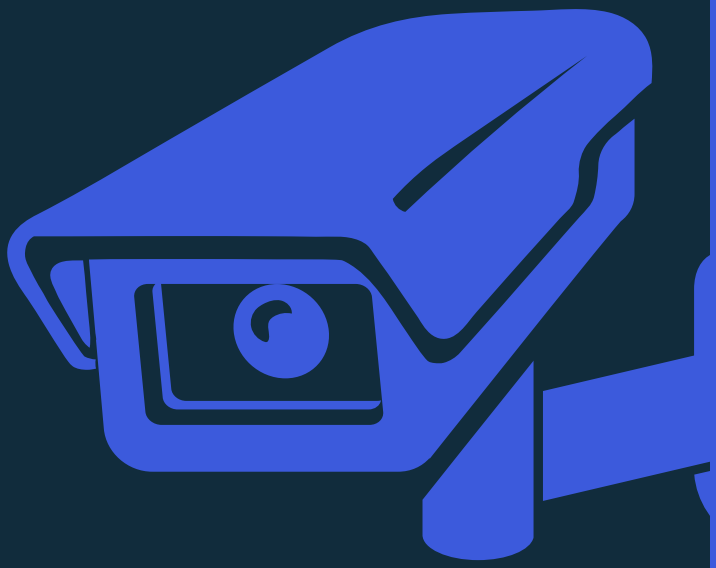
WHEN SINCE 2019

Harm to rights and freedoms

Vumacam has categorically stated its cameras do not enable[49] FRT. However, these cameras still engage the South African constitutional right to privacy, the notion of presumed consent, cybersecurity and the potential harm of hacking when the data stored, can be leaked, altered or stolen if not sufficiently secured. More importantly, in a country where racial inequality is high, there are concerns the Vumacam system will reinforce that inequality, by inaccurately identifying people or colour.

Legal/Campaign action

South African civil rights and liberties organisations have pushed back against the Vumacam project, claiming it is not compliant with South Africa's Protection of Personal Information Act, an act which aims to protect people from harm by protecting their personal information in an effort to mitigate the unintended consequences of emerging technologies. The groups claim that, as per POPIA, Vumacam needs individuals' consent to collect personal information such as their licence plate numbers. However, Vumacam says it is compliant with the POPIA. The LRC has taken legal action against the government and mobile service providers in regards to general surveillance and challenged surveillance legislation.



FRT &

The right to freedom of assembly and association

03

FRT and the right to freedom of assembly and association

Ádam Remport, Hungarian Civil Liberties Union

New technologies can be powerful tools for facilitating assemblies, such as protests, sit-ins and strikes, by allowing participants to organise their gatherings more efficiently. However, some can pose new threats to fundamental rights. Most alarmingly, FRT can enable governments to identify, track and create databases of citizens taking part in peaceful protests, practices which can potentially suppress dissent directly or by a consequential chilling effect. INCLO's member organisations have taken legal action in several countries to protect people's right to freedom of assembly and association.

The right to freedom of peaceful assembly and to freedom of association is enshrined in several fundamental international treaties and conventions, including the Universal Declaration of Human Rights and the European Convention on Human Rights. It is a right that serves as a cornerstone in any democratic system. However, FRT directly infringes on this right because it allows for a specifically invasive type of surveillance which, in and of itself, can serve to discourage individuals from participating in peaceful protests. The risk posed by FRT to the freedom of assembly has been universally acknowledged, prompting several international organisations including, among others, the UN High Commissioner for Human Rights and the EU's Fundamental Rights Agency, to call for the implementation of safeguards in national legislation.

INCLO member organisations have been at the forefront of taking action against the illicit use of FRT. In July 2020, Russian INCLO member organisation Agora International Human Rights Group lodged a complaint with the European Court of Human Rights about the use of FRT against protestors in Moscow. This is the first time a complaint concerning FRT has been lodged with the ECHR about FRT. Agora is representing a civil activist and a politician for the alleged violation of their right to peaceful assembly due to the collection of their biometric data prior to a political rally. Agora's clients, as well as at least 20,000 other participants, could only access the site of a demonstration by passing through metal detectors equipped with FRT-enabled CCTV cameras at eye-level.

In another groundbreaking case concerning the use of FRT by police in South Wales, UK-based INCLO member Liberty was party to a lawsuit that concluded with the court declaring, in August 2020, that the application of FRT by the police had violated the right to privacy under the ECHR[50], the first such decision in the UK. Following the judgment, Liberty has called for the police to stop the use of FRT altogether.

In the meantime, Dejusticia in Colombia requested information from the General Prosecutor concerning a helicopter equipped with FRT cameras which was deployed to monitor specific demonstrations. Far from denying the existence of the technology, the police had in fact previously boasted that the helicopter could identify individuals from a distance of 15km, and that it was capable of recognising covered faces, claims that would have an obvious chilling effect on demonstrators wishing to participate in the demonstrations. The General Prosecutor could not tell Dejusticia, however, how many criminal investigations were opened based on the information gathered by the helicopter cameras, nor did it give a legal view concerning FRT.

INCLO and its members continue to monitor all aspects of the use of facial recognition technology, with a special emphasis on the freedom of assembly and association.

Protesters under watch in Moscow

Damir Gainutdinov, Agora

What

The indiscriminate use of FRT during an anti-government protest in Moscow led to the collection of biometric data of thousands of opposition supporters, including activist Alena Popova and politician Vladimir Milov. The protesters taking part in the demonstration had little or no choice but to have their data collected as they had to pass through metal detectors equipped with CCTV cameras[51] installed at eye level.

> The state should not be able to follow our every step. Facial recognition is one of the first steps towards creating a digital dictatorship. The state is obliged to protect our privacy, but instead it deprives us of this right...Facial recognition systems have no place on our streets.
>
> • ALENA POPOVA, ACTIVIST

WHERE MOSCOW, RUSSIA
WHEN SEPTEMBER 29, 2019

Further details

At least 20,000 people[52], including activist Alena Popova and politician Vladimir Milov, took part in an authorized rally in Moscow in solidarity with those arrested and charged[53] for their participation in peaceful protests. The demonstrations were triggered by the exclusion of independent candidates from the Moscow city legislature elections. In recent years, Russia has emerged as a leading force in the development of FRT with the government defending its expansion of FRT infrastructure as a means to fight crime and maintain order. But rights activists assert it has also been used to identify people who have taken part in rallies and crackdown on activists. Throughout 2019, a network of more than 105,000 cameras were installed across Moscow. The system is currently being used to ensure people are observing Covid-19 quarantine rules but also to continue identifying individuals at rallies and protests.

Harm to rights and freedoms

Agora International Human Rights Group, otherwise known as Agora, argues the collection of protestors' unique biometric data has no legal basis and violates the right to privacy and freedom of assembly. It also says the use of FRT by authorities at protests also amounts to discrimination based on political views.

Legal/campaign action

In January 2020, Ms Popova and Mr Milov filed a domestic complaint[54] against the Moscow government over the use of FRT at protests. In March, the court dismissed[55] the complaint, claiming that the government's use of the technology was legal. In July 2020, they lodged a complaint over Russia's use of FRT during protests with the European Court of Human Rights[56]. Agora is representing them at the ECHR.

Deterring demonstrators in Colombia

Daniel Ospina Celis, Desjusticia

What

Hundreds of thousands of people took part in mass demonstrations[57] against, but not limited to, Colombia's President Iván Duque on November 21, 2019. These protests effectively became known as 21N. They lasted for two weeks while follow-up protests took place in January and February 2020. A day before the protests began on November 21, it emerged that helicopters equipped with FRT would patrol Bogota[58]. The authorities stated the purpose for these FRT patrols was to identify protesters who caused violence. But Dejusticia believes these patrols were used as an attempt to dissuade people from protesting.

> "The public discourse in Colombia strongly supports the implementation of facial recognition technology in almost every aspect of life (including transit tickets). The general discourse surrounding FRT lacks analysis of the impact it has on human rights and especially the right to privacy.
>
> • DANIEL OSPINA CELIS, PRIVACY RESEARCHER, DEJUSTICIA

Further details

Bogotá police told local media that the purpose of using FRT was to identify people who may cause violence during the protests. According to the police, the helicopter equipped with FRT technology had been in use for over three years. Why, then, did the police choose to inform, or remind, the public that it would be used a day before massive public protests were held? It was reported that the FRT cameras would detect facial features from a distance of 15km and detect people who might be hiding from the police. The police also said the tech could even identify covered faces[59]. There is no evidence indicating any effective use of the FRT cameras during the protests in the Colombian criminal system.

WHERE BOGOTA, COLOMBIA

WHEN NOVEMBER, 2019

Harm to rights and freedoms

Invasion of privacy; encroaching on constitutional right to peaceful assembly and association by dissuading people from protesting; creation of police visual databases for future use; potential for misidentification, obstruction to due process, wrongful arrest and detention.

Legal/campaign action

Dejusticia asked the General Prosecutor (Fiscalía General de la Nación) how many criminal investigations were opened as a consequence of the information collected by the helicopter patrols. The General Prosecutor's office said it did not have the information requested. Dejusticia also asked for the legal and constitutional basis for the processing of images by FRT. The answer to Dejusticia's Freedom of Information request indicated that the General Prosecutor could not give a legal view regarding FRT because this could affect judicial impartiality. The police have also not confirmed whether testing has been carried out regarding the use of FRT, in order to determine the possible impact of FRT on citizens' constitutional rights. Dejusticia is continuing to monitor this pressing issue.

FRT &

The right to privacy

04

FRT and the right to privacy

Brenda McPhail, Canadian Civil Liberties Association

Facial surveillance technology has the potential to render our internationally-recognised right to privacy illusory.

While there is a great deal of public concern, and rightfully so, regarding the discriminatory impact raised by the known inability of many facial recognition programs to properly identify faces that are not white and male, privacy advocates warn that if this technology becomes sufficiently accurate that it can reliably identify individuals of skin-colours, the ultimate result is that it will become more dangerous.

Accurate FRT can make it impossible for anyone to move through public spaces and remain just a face in the crowd. Individuals who are identified by default, with no possibility of anonymity, do not only lose privacy; all of the other rights that rely on privacy as a gatekeeper will inevitably be eroded if facial recognition gains widespread acceptance.

Free association, the right to dissent, and free expression often hinge on freedom from surveillance in order for people to feel comfortable exercising them. It is also important to remember that privacy is not just an individual right, but a public good. Equality rights, for example, are more easily eroded when facial analytics enable social sorting.

Different forms of facial surveillance create different privacy deficits or dilemmas, as becomes clear when reading the country-based case studies in this report. Similarly, there are varying levels of risk for individual and group rights depending on whether private sector or state actors are using the technology, although such lines are increasingly blurred as states leverage private sector products and vendors compete for government contracts and commercial market advantage at the same time.

Many INCLO members highlight the severe rights infringements which occur when law enforcement agencies use face surveillance. Whether such uses occur "in the wild" using cameras in public spaces, as described in Liberty's landmark successful legal challenge to FRT by police in South Wales, or as a result of automating the process of matching photos held by, or accessible to, police with crime scene images in the ACLU's story of misidentification, the consequences for individuals caught up in the surveillance net can be consequential.

Despite the potential harms, there are few jurisdictions that provide appropriate privacy safeguards in existing legal instruments, and fewer still that have enacted specific regulation for this invasive technology. The tendency for it to roll out in secret, with no public transparency and accountability, further exacerbates privacy concerns, as the CCLA lays out in their case, describing the behind-the-scenes use of Clearview AI technology by police forces across the country, without any scrutiny by regulators that would have identified that the images in Clearview's database would likely be considered unlawfully obtained under Canadian law.

Privacy is a human right, and it is a first line of defence for many other rights. The impact of face surveillance technologies on individual and group rights, to move through public spaces without undue state scrutiny, risks eroding civil liberties and human rights, in a manner inconsistent with democratic freedoms and values.

Covert use by police in Canada

Brenda McPhail, Canadian Civil Liberties Association

What

Covert use of FRT revealed in Canada speaks to concerns about the possible wider use of FRT in the country. In 2020, police forces across Canada reluctantly admitted[60] they had been testing Clearview AI's controversial FRT, many after initially denying[61] they had done so. In May 2019[62] it emerged the Toronto Police Service had been using FRT to compare images of potential suspects captured on public or private cameras with its internal database of 1.5 million mugshots for more than a year[63]. Until 2017, the public were also unaware that Cadillac Fairview was using FRT at shopping centres in Calgary (and likely other locations) to monitor foot traffic and the age and gender of shoppers, a practice since suspended[64].

> FRT is both too powerful, and too flawed, to be used before we have the necessary societal conversations asking if this technology can ever be used without undermining fundamental freedoms.
>
> • BRENDA MCPHAIL, DIRECTOR OF PRIVACY, TECHNOLOGY AND SURVEILLANCE PROJECT, CANADIAN CIVIL LIBERTIES ASSOCIATION (CCLA)[65]

WHERE UNKNOWN NUMBER OF MUNICIPALITIES ACROSS CANADA, INCLUDING TORONTO, ONTARIO & CALGARY, ALBERTA.

WHEN 2019-2020

Further details

Clearview AI FRT was being used by the Royal Canadian Mounted Police, and regional or municipal forces across Canada, all without public disclosure, in many cases apparently on the initiative of individual units within a force, without authorisation from their chiefs of police. Public outrage ensued and an investigation into the tech by the Privacy Commissioner of Canada contributed to Clearview AI withdrawing its services from the country. That investigation is ongoing and it is anticipated that the way in which Clearview attained images for its database, by scraping social media and other internet sites for photographs without consent, will be found to be in violation of Canadian privacy laws. Hundreds of thousands, if not millions of Canadians, may have been included in searches of the database. Many forces only admitted their use of the tech after media investigations and a data breach[66] came to light.

Harm to rights and freedoms

FRT has the potential to eliminate our ability to be a face in the crowd, and the risk is exacerbated when the technology is used covertly. Both private and public sector actors seem to conduct their own secret and often controversial interpretations of privacy law or exploit gaps in Canada's aging privacy regulatory regime. Meaningful consent is illusory or, more often, impossible. Discrimination, misidentification, obstruction to due process, wrongful arrest and wrongful detention may occur, yet little public scrutiny of such harms is possible.

Legal/campaign action

CCLA has initiated a series of access to information requests into the uses of Clearview's products; the number of cases it was used during investigations; the number of accused identified; and the relationship between the use of the tech and charges being laid. It is researching how the Toronto Police Service FRT program impacts people accused who have been identified via FRT in subsequent court actions. CCLA has called for a moratorium on the use of FRT pending public debate and improved regulation, and has participated in a study being conducted on FRT by the Office of the Privacy Commissioner of Canada.

Illegally arrested over an invalid warrant in Argentina

Margarita Trovato, Centro de Estudios Legales y Sociales

What

A woman identified by an FRT camera in Buenos Aires was intercepted by police officers and detained in 2019, several years after the expiration of an arrest warrant that had been issued against her. The order had originally been issued in 2006 for the woman's failure to testify in court as a witness because she had not been duly notified of her obligation. By the time she was detained in 2019, the warrant she knew nothing about had long expired, making her arrest illegal.

> In the city of Buenos Aires, mass facial recognition did not pass through the legislature or involve any type of political discussion. The software, how it was acquired, who implements it or under what regulations or control mechanisms are not known.
>
> • CELS ANNUAL REPORT 2019[67]

WHERE BUENOS AIRES, ARGENTINA
WHEN FROM APRIL 2019

Further details

Authorities in Buenos Aires started to use 10,000 FRT cameras[68] in Argentina in April 2019, with the aim of detecting people against whom an arrest warrant had been issued[69]. However, the use of FRT cameras in the city's subway system has led to the detentions of innocent people who were delayed for hours before being released. Despite civil society's cries, the City of Buenos Aires adopted in October 2020 an overly superficial legal and regulatory framework on FRT, after an abbreviated debate that lacked a proper analysis of the technology's impact on human rights. To this day, the software used, how it was acquired, and who implements it are matters still unknown.

Harm to rights and freedoms

An outdated police database of images and false positives have led to wrongful arrests, casting suspicion over innocent people and putting them in the invidious position of having to prove their innocence. The principles of due process and procedural fairness are harmfully engaged, while a severe lack of political discussion about the use and roll-out of this technology goes against the principles of democracy. The rights to privacy, the protection of personal information, and citizens' right to know what information has been compiled about them are also engaged.

Legal/campaign action

CELS assisted the woman who was arrested in Buenos Aires after her detention. It has also been campaigning that not only are there problems with the privacy violation of facial recognition cameras, there is also a problem of accuracy. It seems clear that the information supplied to the system has not been updated while no judicial or police authority appears to be checking who is being detected, detained and the reason for the same.

Hikvision cameras in a children's hospital in Ireland

Olga Cronin, Irish Council for Civil Liberties

What

Ireland's new National Children's Hospital may use Hikvision CCTV cameras with end-to-end FRT as part of its security system. These cameras, linked to human rights abuses in China, can map facial features caught on camera or video and compare the caught images to a separate database of images in order to confirm the identity of a person.

> To protect everyone's rights, including children's, the State should not install these face surveillance systems in hospitals in the first instance, and certainly not in cooperation with private surveillance companies with controversial rights track records.
>
> • ELIZABETH FARRIES, ASSISTANT PROFESSOR, UNIVERSITY COLLEGE DUBLIN DIGITAL POLICY PROGRAMME

Further details

Hikvision has been widely condemned for monitoring[70] Muslim minorities in China. The surveillance outfit came under huge criticism for allegedly providing the equipment in Xinjiang where Uighur Muslims are being forcibly detained[71] in detention centres. A law ordering all federal government bodies in the US to stop buying Hikvision cameras[72] went into effect in August 2019. The revelation that Ireland's new National Children's Hospital may use Hikvision FRT cameras was first reported[73] in December 2019. Ireland's Minister for Health subsequently told the Irish parliament: "Less than 3%[74] of the cameras procured for the new children's hospital have the potential for high definition facial recognition capabilities." Meanwhile, Dublin City Council has backtracked[75] on its plans to use these cameras in a community centre setting.

A Department of Health spokesperson told ICCL that an evaluation of all aspects of the security systems to be installed at the hospital would be undertaken. They also said a Data Protection Impact Assessment would be carried out and that the chosen system will be compliant with Ireland's Data Protection Act 2018 and the EU's General Data Protection Regulation (GRPR) rules.

WHERE NATIONAL CHILDREN'S HOSPITAL, DUBLIN, IRELAND

WHEN THE HOSPITAL IS DUE TO BE OPENED IN 2022 AT THE EARLIEST

Harm to rights and freedoms

FRT is expensive, inaccurate and discriminatory. Given Ireland is subject to the GDPR rules, the use of FRT is likely to be unlawful. The use of FRT for children accessing medical care would be incredibly invasive. Children are afforded enhanced personal data protections under the law. Deploying this tech in this manner would run afoul of those protections.

Legal/campaign action

ICCL has advocated against[76] the use of these cameras at the hospital while Ireland's Data Protection Commissioner has warned the hospital[77] if it intends to use this FRT, it must carry out a DPIA because the data processing could involve new technologies, children's data, special category[78] data as defined in Article 9 of the GDPR, and large scale processing in a publicly accessible area.

At the discretion of the secret service in Hungary

Ádam Remport, Hungarian Civil Liberties Union

What

In Hungary, the deployment of FRT is sporadic and most often used to identify wanted or missing persons, although the true extent of the FRT use in Hungary is largely unknown. So far, the existing legal framework on data collection and access to personal data has no FRT provisions. A recent report reveals that the main state institution authorised to collect and control confidential information with facial recognition technology (FRT) is the Special Service for National Security (secret service).

> This is new technology to the extent that we don't even have the established legal terms in Hungarian to describe all the notions related to it. At this point, the use of FRT is at the discretion of the secret service, which means that its proper use depends on the common sense and good intentions of secret service agents.
>
> • ADAM REMPORT, LEGAL OFFICER, PRIVACY PROJECT, HUNGARIAN CIVIL LIBERTIES UNION (HCLU)

Further details

An HCLU inquiry sent to the Hungarian Data Protection Authority (DPA) in 2019 regarding the government's use of FRT triggered an investigation which revealed that the secret service, authorised to use facial recognition software, carries out identification requests from different branches of government. From the DPA report we learn that in 2018 the FRT has been used sporadically in relatively few instances (6000 times), leading to 209 police requests for individual identification and four arrests. One other authority using facial recognition capabilities is the national immigration office. The latter compares images with the portraits of wanted persons on lists published by the Hungarian police and also by Interpol, Europol and the FBI on their public forums.

Another development worthy of attention is the establishment, by the Ministry of Interior in early 2019, of a centralized system of image data continuously collected from many locations via a nationwide network of 35,000 CCTVs. This technology is installed by city councils and the police in public places, including motorways, banks and public transport and offers the possibility of storing and linking the collected data with each other and with data from other sources.

WHERE HUNGARY
WHEN 2018 - 2019

Harm to rights and freedoms

The concern is that the existing legal framework on data collection and access to personal data makes no specific reference to FRT and allows for the widest possible interpretation about how such data is handled and, as such, it cannot guarantee the protection of privacy rights. Moreover, the HCLU flags the concern that at any given time the FRT could be used in conjunction with the existing CCTV network, spreading further the threat to privacy.

Legal/campaign action

No legal action has been taken so far. While the use of FRT seems sporadic and limited, HCLU emphasises the necessity to develop at this stage a precise legal framework with specific reference to FRT.

A system that sees through Covid-19 masks in India

Siddharth Seem, Human Rights Law Network

What

In early 2020, India's central government approved the deployment of an Automated Facial Recognition System (AFRS) across the country beginning early 2021. The system will reportedly allow facial biometrics to be extracted from video and CCTV which will be matched with images of individuals whose photographs are maintained in criminal databases held by the National Crime Records Bureau (NCRB). It will reportedly be the world's largest government-operated facial recognition system. In September 2020, it emerged that the NCRB wants an AFRS that can identify people wearing face masks. Due to Covid-19, 300 million people[79] in India's largest cities and states currently must wear a mask or risk time in prison.

> The NCRB's plans violate every legal principle governing the right to privacy and data protection. The lack of a data protection law in India further exacerbates the privacy risks of any program, where law enforcement agencies can collect, use and control data whichever way they please. Moreover, the inaccuracy problems with this technology pose an added threat to religious minorities and socially marginalised groups in India, who are already routinely falsely implicated in alleged crimes.
>
> • SIDDHARTH SEEM, LAW OFFICER, THE HUMAN RIGHTS LAW NETWORK IN DELHI (HRLN)

WHERE THE SYSTEM WILL BE USED BY POLICE ACROSS INDIA.

WHEN THE DEADLINE FOR BIDS WAS OCTOBER 8, 2020 AFTER IT WAS EXTENDED 12 TIMES.

Further details

The NCRB put out a tender calling for bids from vendors to build the national AFRS describing the surveillance tool as a centralised web application which will be the foundation for "a national level searchable platform of facial images"[80]. NCRB plans on police accessing the system via mobile phones and that 2,500 users will be able to use it at the same time. Following queries put to the NCRB about partial face matching because of mask-wearing, the NCRB clarified that prospective bidders would lose points in the bidding competition if their systems could not recognise faces covered with face masks[81]. This is despite some studies showing that tests facial recognition algorithms on faces partially covered by protective masks showed error rates of up to 50 per cent[82] in some cases. The NCRB also said that prospective bidders' systems would also have to generate "comprehensive biometric authentication reports" consisting of a person's face and fingerprints.

Harm to rights and freedoms

The creation of a nationwide automated FRT system, in the absence of robust data protection laws, could lead to a system of mass surveillance for the entire population and lead to discrimination, exclusion and gross violations of fundamental human rights. It is not known how the data collected by this system will be collected and stored and who or what will oversee it in order to safeguard fundamental rights.

Legal/campaign action

Privacy and digital rights experts have raised serious concerns about these plans. While there has been no formal legal action yet, several groups have sent legal notices to the Government to withdraw its proposal.

Plans for FRT 'perpetual line-up' in Australia thwarted

Kieran Pender, Human Rights Law Centre

What

In 2018, the Australian government proposed the creation of a framework for the retention, use and sharing of facial images and other biometric data. The proposed scheme would have established a centralised database of drivers' licence images, which federal, regional and local government agencies could access for use by FRT. This would serve as a 'perpetual line-up': millions of innocent Australians would be subject to dragnet searches, potentially in real-time, with no transparency and minimal safeguards.

> "New capabilities for search and surveillance must be law governed, and existing laws are insufficient to ensure this. However, we have concluded that the proposed Bill is manifestly, and dangerously, insufficient for this purpose.
>
> • HUMAN RIGHTS LAW CENTRE (HRLC)'S SUBMISSION TO PARLIAMENTARY INQUIRY, MAY 2018[83]

WHERE AUSTRALIA

WHEN MAY 2018 – OCTOBER 2019

Further Details

In 2017, Australia's state and federal governments concluded an intergovernmental agreement on "identity matching services". This saw Australia's eight regional governments agree to share drivers' licence images and other biometric data with the federal government, which would establish an "interoperability hub" through which government agencies at all levels could access biometric data. The laws introduced into Australian's parliament in 2018 provided the legal basis for the establishment of the hub and underlying database. Under the draft laws, agencies could search the database without a warrant, on a dragnet basis, in real-time or after-the-fact, with no mechanism for an individual whose biometric data is retrieved to be informed (and hence no potential to challenge to search). No compelling policy purpose was provided for the scheme, beyond the potential for greater efficiency in law enforcement and government administration.

Harm to rights and freedoms

The proposed scheme would have significantly eroded privacy protections enjoyed by all Australians. Ordinarily, Australian privacy law would require individuals to provide current, specific, voluntary and informed consent to the collection, use and disclosure of biometric data; the scheme provided no such requirements. It also posed a significant threat to freedoms of expression, association and assembly enjoyed by Australians – the draft laws contained no safeguards for the unimpeded exercise of these freedoms. There were also grave concerns about the potential for the scheme, if established, to disproportionately burden marginalised or vulnerable groups.

Legal/campaign action

The Human Rights Law Centre's Democratic Freedoms Unit were at the forefront of resistance to the proposed laws. The HRLC provided exhaustive initial, subsequent and oral submissions to an inquiry by Australia's Parliamentary Joint Committee on Intelligence and Security (PJCIS). The HRLC simultaneously undertook a substantial media and advocacy campaign, highlighting concerns with the draft laws articulated by HRLC and other civil society stakeholders.

In October 2019, the influential PJCIS accepted the submissions of the HRLC and other civil society stakeholders, recommending that the draft laws be redrafted on the basis that the proposed regime be "built around privacy, transparency and subject to robust safeguards"[84]. The HRLC's submissions were cited extensively in the PJCIS's ultimate report. As of January 2021, revised laws have not yet been put to Parliament.

Unregulated FRT across Kenya

Martin Mavenjina, Kenya Human Rights Commission

What

In September 2018, the National Police Service launched an FRT system[85] involving the installation of thousands of cameras, which also use licence plate recognition technology, along major roads and highways as part of its Integrated Command and Control System. FRT is also being used at Kenya's borders[86] while 1,800 cameras with FRT capabilities were deployed all over Nairobi and Mombasa in 2014, a figure which grew to 2,100 by 2019. But the unregulated use of FRT by law enforcement agencies has resulted in the infringement of privacy rights, freedom of expression and the undermining of the protection of fundamental rights and freedoms.

> The continued use of FRT by law enforcement agencies in Kenya will give them unfettered discretion to conduct mass surveillance, stifle voices of decent, restrict freedom of expression and also commit various human rights violations such as assaults, crackdown on peaceful demonstrations and/or even commit extrajudicial executions.
>
> • MARTIN MAVENJINA, CONSTITUTIONAL AND HUMAN RIGHTS LAWYER, THE KENYAN HUMAN RIGHTS COMMISSION (KHRC)

WHERE NAIROBI AND MOMBASA IN KENYA, AND KENYA'S BORDERS

WHEN FROM 2014

Further details

The cameras with FRT capabilities in Nairobi and Mombasa were deployed as part of a surveillance system involving a live camera feed beamed to the National Police Service headquarters. The police claim the system has led to the recovery of over 4,000 stolen vehicles. However, increasing crime level statistics belie the idea that the system helps to reduce crime. According to Kenya National Bureau of Statistics, Nairobi saw 7,434 crimes reported in 2017 versus 6,732 in 2014. The rape of a woman in broad[87] daylight in Nairobi's Business Center in 2018 has led many to question the efficacy of the system. Further questions arose in July 2019 when it emerged[88] that the cameras lacked basic components to avert crime and had limited data storage capacity.

Harm to rights and freedoms

The unregulated use of FRT by law enforcement agencies in Kenya has raised key fundamental concerns specifically around the right to privacy, under Article 31 of the Constitution of Kenya, and data protection. There are also concerns about due process as the police neither have to seek judicial authorisation nor consent from any individual while conducting surveillance. The Data Protection Act 2019[89] provides for a robust framework on the handling and protection of personal data but the government has been slow to implement the Act. These cameras have been used to conduct mass surveillance on peaceful protestors within Nairobi and may explain why after, or during, peaceful demonstrations, some human rights defenders have been unlawfully arrested or detained by the police[90].

Legal/campaign action

The Kenya Human Rights Commission has continued to engage relevant state actors on the negative implications of FRT and the fundamental human rights concerns that arise as a result of continued use of the same with a view of ensuring that the government enacts legislation and policy to develop a framework for regulation. KHRC has previously, through strategic impact litigation, challenged the surveillance technologies that have been deployed by the state[91].

Conclusion

As our report illustrates, the indiscriminate use of FRT is in widespread use by law enforcement and other government agencies across the world. The full harmful impacts and effects of FRT on people's lives are only beginning to emerge. But it can already be said, without hesitation, that the global roll-out of this blanket surveillance tool is dangerously normalising surveillance.

As this technology allows for the tracking of people in real-time and the identification of who we are, where we go and who we meet, it threatens to create a world where people are watched and identified when they attend a protest, take part in religious events, visit a doctor or just go about their daily lives.

The proliferation of this discriminatory and deeply invasive technology, often with no or little public debate, means that not only do we risk losing all privacy in public spaces but it also puts our rights to freedom of expression, protest and equality in jeopardy.

In many countries, the use of FRT is grounded in little or no legislation. Without rigorous legal frameworks for this technology to ensure transparency, accountability, and proper security, FRT may be subject to misuse and, worse, abuse.

The wholesale collection of personal data, without consent, urgently calls into question the necessity and proportionality of this technology, as it contributes to the ever-increasing databases that collect our personal data. Most worryingly, this method of surveillance flies in the face of the legal principle of the presumption of innocence, an international human right under the UN's Universal Declaration of Human Rights[92]. Innocent people don't belong on criminal databases[93].

End Notes

1. The Global Expansion of AI Surveillance Carnegie Endowment for International Peace, Steven Feldstein, September 2019
2. Half of All American Adults are in a Police Face Recognition Database, New Report Finds, Center on Privacy & Technology at Georgetown Law, October 2016
3. FBI, Facial Recognition Technology: Ensuring Transparency in Government Use, Statement Before the House Oversight and Reform Committee, Washington, DC, June 2019
4. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification Joy Buolamwini and Timnit Gebru, 2018
5. 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says, Sky News, July 2019
6. Delhi violence: Over 1900 faces recognised through facial recognition, says Amit Shah, The Economic Times, March 2020
7. China: facial recognition and state control, The Economist, October 2018
8. Statement on principles and prerequisites for the development, evaluation and use of unbiased facial recognition technologies, ACM U.S. Technology Policy Committee, June 2020
9. Ed Bridges V South Wales Police, UK Court of Appeal, Bailii
10. The Secretive Company That Might End Privacy as We Know It, New York Times, Kashmir Hill, January 2020
11. Clearview AI ceases offering its facial recognition technology in Canada, Office of the Privacy Commissioner of Canada, July 2020
12. Milov filed a lawsuit against the Moscow authorities and the Central Internal Affairs Directorate over face recognition technology, Kommersant, January 2020
13. Police and Military Use of Facial Recognition Technology, ACRI, September 2020
14. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN General Assembly, Human Rights Council, 41st session, 24 June–12 July 2019
15. Universal Declaration of Human Rights
16. International Covenant on Civil and Political Rights
17. African Charter on Human and People's Rights
18. European Convention on Human Rights
19. American Convention on Human Rights
20. ASEAN Human Rights Declaration
21. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN General Assembly, Human Rights Council, 41st session, 24 June–12 July 2019
22. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, New York Times, April, 2019
23. Ed Bridges v South Wales Police, UK Court of Appeal judgment
24. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN General Assembly, Human Rights Council, 41st session, 24 June–12 July 2019
25. Liberty wins ground-breaking victory against facial recognition tech, Liberty, August 2020

26. Ed Bridges V South Wales Police, UK Court of Appeal, Bailii
27. Liberty wins ground-breaking victory against facial recognition tech, Liberty, August 2020
28. Petition: Resist facial recognition, Liberty
29. Study finds gender and skin-type bias in commercial artificial-intelligence systems, MIT News, February 2018
30. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST, December 2019
31. Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart, ACLU, June 2020
32. Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time, Vice, June 2020
33. Wrongfully Arrested Because of Flawed Face Recognition Technology, ACLU, June 2020
34. Detroit police work to expunge record of man wrongfully accused with facial recognition, The Detroit News, June 2020
35. ACLU of Michigan complaint re: use of facial recognition, ACLU, June 2020
36. Community control over police surveillance, ACLU
37. Tell the Detroit City Council: Say No to unchecked government surveillance, ACLU Michigan
38. Despite pausing sales to police, company has not made same commitment for sales to federal law enforcement, ACLU, June 2020
39. Gil-Gan Mor, ACRI, Twitter
40. The Global State of Facial Recognition, Digital Information World, July 2020
41. Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns, NPR, August 2019
42. Microsoft hires Eric Holder to audit AnyVision over use of facial recognition on Palestinians, NBC, November 2019
43. Facial recognition: It's time for action, Microsoft, December 2018
44. Microsoft divests from Israeli facial-recognition startup, AP, March 2020
45. Findings of AnyVision Audit, Covington, March 2020
46. Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?, NBC News, October 2019
47. Police and Military Use of Facial Recognition Technology, ACRI, September 2020
48. Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa, Vice, November 2019
49. Vumacam defends Joburg smart camera network, iWeb, December 2019
50. Ed Bridges v South Wales Police, UK Court of Appeal judgment
51. Activists appealed to the European Court of Human Rights for the use of technology of facial recognition at rallies, Rusbankrot, July 2020
52. Thousands demand protesters freed in Moscow rally, BBC, September 2019
53. The "Moscow Case": What You Need to Know, Human Rights Watch, October 2019
54. Milov filed a lawsuit against the Moscow authorities and the Central Internal Affairs Directorate over face recognition technology, Kommersant, January 2020
55. The court dismissed the claim of Milov and Popova on the illegal use of face recognition technology in the Moscow video surveillance system, MBK, March 2020
56. Moscow's Use of Facial Recognition Technology Challenged, Human Rights Watch, July 2020
57. Student Protester's Death Sparks Fresh Protests in Colombia. Here's What to Know, TIME, November 2019
58. This is the hawk, the helicopter that will monitor... Bogotá using facial recognition, Semana, November 2019
59. Desde helicópteros, Policía haría reconocimiento facial a encapuchados, Public Metro, November

2019
60. Police use of facial recognition program breaks 'trust relationship' with public, privacy expert says, CBC, February 2020
61. Facial recognition app Clearview AI has been used far more widely in Canada than previously known, York Region, February 2020
62. Privacy advocates sound warning on Toronto police use of facial recognition technology, CBC, May 2019
63. Toronto police have been using facial recognition technology for more than a year, The Star, May 2019
64. A quick win for privacy rights: CCLA VS Cadillac, Canadian Civil Liberties Association, October 2018
65. Can your face be your undoing: The perils of facial recognition, Centre For Free Expression, December 2019
66. Clearview AI's entire client list stolen in data breach, CNET, February 2020
67. Secrecy: National security as rationale for an unchecked State, Human Rights in Argentina Report 2019, CELS
68. Ibid
69. From April 15 they will search for fugitives with a facial recognition system, Ámbito, April 2019
70. 'China: facial recognition and state control', The Economist, October 2018
71. China steps up surveillance on Xinjiang Muslims, Financial Times, July 18, 2018
72. Life after the NDAA, Security Info Watch, August 2019
73. Ireland National Children's Hospital Chooses Hikvision End-to-End With Facial Recognition, IPVM, December 2019
74. National Children's Hospital, Irish parliamentary debate, Oireachtas, December 2019
75. DCC to cease using 'blacklisted' CCTV firm, Business Post, May 2020
76. Facial recognition technology, Irish Council for Civil Liberties
77. Watchdog warning over mooted facial recognition cameras at Children's Hospital, Irish Examiner, December 2019
78. See Article 9 of GDPR (Processing of special categories of personal data)
79. Coronavirus: India makes face masks mandatory for more than 300m people, punishable by up to six months in prison, Independent UK, April 2020
80. Exclusive: Concerns around number of active users, and 'backdoors' raised at an NCRB facial recognition meeting, Medianama, July 2020
81. India's NCRB to test automated facial recognition system on 'mask-wearing' faces, Medianama, September 2020
82. NIST Launches Studies into Masks' Effect on Face Recognition Software, NIST, July 2020
83. Human Rights Law Centre: The dangers of unregulated biometrics use: Submission to the Inquiry into the Identity-matching Services Bill 208 and the Australian Passports Amendment (Identity-matching Services Bill) 2018
84. Identity-matching Services Bill 2019, List of Recommendations from Australia's Parliamentary Joint Committee on Intelligence and Security
85. Kenyan police launch facial recognition on urban CCTV network (Biometric Update), September 2018.
86. NEC facial recognition border tech for Kenya as airport biometrics rollouts continue (Biometric Update), October, 2019
87. Police arrest street urchin who raped woman in broad daylight (Nairobi News), April 2018

88. Interior Ministry on the spot over Sh15bn 'faulty' CCTV cameras (The Star), July 2019
89. Data Protection Act
90. Police Arrest Many During #SabaSabaMarchForOurLives in Nairobi (Missing Voices), July 2020
91. Petition 56, 58 & 59 of 2019 (Consolidated), Kenya Law
92. Article 11, United Nations, Universal Declaration of Human Rights
93. Half of All American Adults are in a Police Face Recognition Database, New Report Finds, Center on Privacy & Technology at Georgetown Law, October 2016

Acknowledgments

INCLO is hugely grateful to INCLO Communications Consultant Andreea Anca and graphic designer Taryn McKay for their enormous contribution to the concept, content and artwork of this report.

About INCLO

INCLO is a network of 15 independent, national human rights organisations across the globe. We work together to promote fundamental rights and freedoms. Together we are: the Agora International Human Rights Group (Agora) in Russia, the American Civil Liberties Union (ACLU), the Association for Civil Rights in Israel (ACRI), the Canadian Civil Liberties Association (CCLA), the Centro de Estudios Legales y Sociales (CELS) in Argentina, Dejusticia in Colombia, the Egyptian Initiative for Personal Rights (EIPR), the Hungarian Civil Liberties Union (HCLU), the Human Rights Law Centre (HRLC) in Australia, the Human Rights Law Network (HRLN) in India, the Irish Council for Civil Liberties (ICCL), the Kenya Human Rights Commission (KHRC), the Commission for the Disappeared and Victims of Violence (KontraS) in Indonesia, the Legal Resources Centre (LRC) in South Africa, and Liberty in the United Kingdom.

Learn more at inclo.net.