JULY 2021

Facing the Risk

Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology

AUTHORS
Amy K. Lehr
William Crumpler

A Report of the CSIS Strategic Technologies Program and the Human Rights Initiative

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JULY 2021

Facing the Risk

Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition Technology

AUTHORS
Amy K. Lehr
William Crumpler

A Report of the CSIS Strategic Technologies Program and the Human Rights Initiative

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

CSIS thanks William Carter, Mariefaye Bechrakis, Anna Lehman-Ludwig, and Luiza Parolin for their research and administrative support during the drafting of this report. CSIS also thanks the nearly 100 individuals who participated in interviews and workshops over the course of this project.

This report was made possible through a grant from the U.S. State Department Bureau of Democracy, Human Rights, and Labor.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Contents

Executive Summary

Facial recognition technology (FRT) refers to the practice of using software to determine the similarity between two face images in order to evaluate a claim. Most facial recognition technologies are used for one of two purposes: verification or identification.

- **Verification** (also known as 1:1 matching) involves using facial recognition to confirm whether a person is connected to a specific identity record, such as when a person uses facial recognition to unlock their phone.
- **Identification** (also known as 1:N or 1:many matching) involves using facial recognition to compare a target individual to a larger database of known faces, such as when police use the technology to identify a suspect from footage of a crime.
- A distinct but related process is facial characterization, where the purpose is not to compare the similarity of two faces but instead to classify a single face according to its gender, age, emotion, or other characteristics. Face characterization is sometimes combined with facial recognition, but it can also be used on its own without identifying the individuals being analyzed. Facial characterization poses significant risks due to its discriminatory potential but lies beyond the scope of this paper.

A wide variety of organizations in both the public and private sectors have begun to deploy facial recognition to support their operations. These deployments can be classified into five categories based on the use case:

- **Law Enforcement:** Police deployments of facial recognition can take one of two forms: live monitoring and retroactive identification. Live monitoring involves comparing individuals against

a watchlist in real time as they pass within the range of facial recognition-enabled cameras. Live monitoring is often deployed during major events for added security or in major public areas as a passive way to generate alerts for suspects. Retroactive identification involves applying facial recognition to captured images or video to identify persons of interest. Retroactive identification can be used to develop leads for criminal investigations and to identify missing persons or deceased individuals. Law enforcement use of facial recognition poses significant risks due to the way it could enable government surveillance or create chilling effects on fundamental freedoms.

- **Border Control:** Governments around the world are expanding their use of facial recognition as a way of processing immigrants and travelers at their border. Authorities hope that facial recognition will improve the security and convenience of border management, but there are risks that some governments could track and monitor travelers in ways that violate their privacy and share that information with other agencies or governments in opaque and unaccountable ways.

- **Identity Verification:** Facial recognition can allow individuals to biometrically authenticate themselves when accessing services provided by public and private actors. This could improve convenience and expand access to services ranging from mobile banking to social security and public transportation. This use carries privacy risks due to the possibility that sensitive data will be collected, processed, and shared beyond what is necessary, proportional, or consented to by the user. Errors occurring during the verification process also risk shutting people out of these services if there is no readily available mechanism for appealing and reviewing match decisions.

- **Access Management:** Facial recognition can be used to automate the process of letting authorized individuals into restricted areas, taking the attendance of workers and students, and even tracking people as they move through an area. These systems are already in use in offices, factories, residence complexes, and schools around the world. Depending on how data is collected and shared, these systems can pose privacy risks by revealing sensitive information about those who have been enrolled. This risk is particularly significant in the case of school deployments, which implicate the rights of children. Access management systems can also risk restricting individuals' access either due to errors or because of chilling effects.

- **Private Security:** Private actors are increasingly turning to facial recognition systems as a way of providing security at retail locations, event venues, and even residential neighborhoods. These systems pose substantial risks to the right to privacy due to the potential for individuals to be monitored and tracked without their awareness or consent and can have chilling effects on movement, expression, assembly, and association. Depending on the source of images for the watchlist and the justification used to decide who to include, private security systems could also risk arbitrarily denying individuals the right to access essential services, such as grocery stores.

A variety of fundamental rights and freedoms can be impacted through FRT deployments. While in a few instances FRT may be used to help protect and promote certain human rights, for the most part the technology tends to have a negative impact on fundamental rights and freedoms. This report highlights 15 rights and freedoms that could be significantly affected by FRT deployments and discusses these impacts in the context of the five use cases outlined above.

- **Right to Privacy:** Facial recognition is uniquely capable of allowing for the remote identification and surveillance of individuals and thus carries significant privacy risks even when deployed

with strong safeguards. Governments can exploit FRT to track and target activists and dissidents or form databases revealing sensitive information about people's lives and activities. Border authorities can use facial recognition to collect and share information about the movements of travelers as well as vulnerable populations such as migrants and asylum seekers. Private operators using facial recognition for identity verification, access management, or private security can also violate subjects' rights depending on whether individuals are made aware of when FRT is being used, whether they offer free and informed consent to the data processing, and how collected data is shared or sold to other organizations.

- **Freedom of Expression, Assembly, and Association:** Facial recognition can threaten these freedoms by enabling government authorities to identify and retaliate against those engaging in acts of dissent. There is already evidence of this occurring in countries such as India, Russia, Uganda, and Indonesia, and it is likely that many other cases have occurred but are not yet known. Even in cases where FRT is not used this way, if the public perceives facial recognition monitoring to be a risk, they will begin to self-censor, leading to chilling effects. Private FRT deployments also contribute to these chilling effects and can have direct impacts on these rights if operators cooperate with government authorities in monitoring certain individuals.

- **Freedom from Arbitrary Arrest and Detention:** While facial recognition continues to improve, the large majority of systems still experience very high error rates during real-world deployments. This creates a risk that law enforcement or border authorities that are overconfident in a system's accuracy may detain innocent individuals on the basis of an erroneous match. FRT systems used for identity verification or private security can also create risks for arbitrary arrest if they are repurposed by government authorities to support unlawful surveillance activities.

- **Right to Non-Discrimination:** A majority of facial recognition systems have been shown to have different accuracy rates for different demographic groups, raising the risk that some groups may be disproportionately impacted by errors. Even when there is no bias in an algorithm's accuracy, FRT can have discriminatory effects if it is used in a way that disproportionately targets certain groups. Further, some operators may decide to combine facial recognition with facial characterization systems in ways that allow authorities to single out members of particular groups for surveillance and monitoring.

- **Right to Effective Remedy:** Depending on the procedures put in place by operators, there are significant risks that individuals whose rights are impacted by FRT may be unable to seek remedy for violations. This can occur if individuals are never made aware that they are being subjected to facial recognition or if they are denied information about the scope, purposes, and policies surrounding the technology's use. This would make it impossible to determine whether and how one's rights were impacted—a necessary prerequisite to seeking remedy. Remedy may also be made more difficult in cases where remote, facial recognition-based authentication methods become the standard for accessing essential public goods and services, such as social welfare. A lack of human oversight could make it more difficult for individuals to rectify instances where they are denied entitlements due to facial recognition error.

- **Freedom of Religion:** The use of FRT by government authorities may have chilling effects on the freedom of religion if certain groups suspect that the technology may be used to monitor or harass them. Facial recognition may also be used as an excuse to deny individuals the right to practice

their religion if it is used to justify forcing people to shave their facial hair or remove head and face coverings.

- **Freedom of Movement:** Facial recognition can have direct impacts on freedom of movement to the extent that it is used by public or private operators to enforce unlawful restrictions on individuals' movements both within and between countries. The technology can also have chilling effects if people decide to avoid certain locations out of concern that they may be monitored by the technology.
- **Rights of the Child:** Facial recognition has been successfully used by law enforcement around the world to identify missing children and combat trafficking and exploitation. However, there are important questions as to the value and efficacy of some of these deployments, especially in light of the mission creep that has sometimes resulted. FRT can also restrict the rights of children when minors are included in security watchlists or when schools implement FRT systems for attendance or security.
- **Right to Life, Liberty, and Security:** Facial recognition can be used by law enforcement officers to apprehend criminals, by border officials to improve terrorist screening processes, and by private operators to identify guests who have engaged in dangerous or unlawful activity in the past. However, these deployments also create substantial risks to other fundamental rights and freedoms, and as such must meet high standards of necessity and proportionality to justify such intrusive security measures.
- **Right to an Adequate Standard of Living:** Facial recognition can help improve living standards by enabling mobile banking services that promote financial inclusion for underserved populations, such as in rural areas. However, FRT could also negatively impact people's right to adequate living standards if access management systems shut individuals out of residential complexes, workplaces, and other locations or if private security systems prevent individuals from being able to access essential commercial activities, such as grocery stores.
- **Right to Own Land:** Facial recognition can help promote land ownership and support land management reforms by enabling mobile apps where users can register and transact their properties. These apps reduce the friction associated with the registration and sale of property and make the process more attractive to owners by tying property ownership to expanded credit, loan opportunities, and other financial services.
- **Right to Social Security:** Facial recognition can be used as a way of verifying the identities of those collecting welfare benefits, making it easier for individuals in remote areas or those who have jobs or medical conditions that make it difficult for them to physically claim their benefits. However, if adequate safeguards are not in place, errors in authentication could lead to some being denied their rights to government benefits.
- **Right to Just and Favorable Conditions of Work:** Biometrics can help protect the rights of laborers by enabling systems of accountability in dangerous workplaces. In industries such as fishing, biometric worker check-in procedures could help authorities ensure that laborers are not sold and rotated to other ships or lost overboard and not reported. FRT can jeopardize this right, however, if facial recognition systems are expanded to support broader workplace surveillance practices.

While some rights, such as the right to non-discrimination, cannot be restricted under any circumstances under international human rights law, other rights and freedoms are not absolute and can be restricted under certain conditions. Restrictions on the right to privacy, freedom of assembly, freedom of expression, and freedom of movement are allowed, provided they meet the following tests:

- **Lawfulness:** Proposed restrictions to individuals' rights and freedoms must be provided by law. This legal basis for the use of technologies such as facial recognition must be public, capable of being challenged through democratic processes, and specific as to the conditions and safeguards associated with deployments.
- **Necessity:** The restriction of fundamental rights and freedoms must be the only way or least intrusive way to achieve the aim being sought. In the context of facial recognition, this includes demonstrating that alternative biometrics or non-biometric tools are inadequate for the given purpose. Necessity must be demonstrated in a specific and individualized fashion.
- **Legitimacy:** Restrictions may only take place if they are necessary in the pursuit of a legitimate aim, including the protection of others' rights, national security, public order, or public health. Because so many facial recognition operators will likely argue that their deployments are necessary for national security or public order, it is important that legitimacy not be taken as the only test required to justify a deployment.
- **Proportionality:** Restrictions must be proportionate in scope and effect to the aim being sought and the risks created by the deployment. The proportionality of facial recognition systems is affected by the geographic and temporal scope of deployment, the enrollment policies used to create matching lists, the existence of alternative methods or tools, and the safeguards put in place by the operator.

The report then proposes a series of recommendations for how facial recognition operators can increase the probability that their systems can be deployed in a manner consistent with international human rights law.

Identifying and Responding to Human Rights Impacts and Risks

1. Conduct a human rights impact assessment (HRIA) prior to deploying a facial recognition system.
2. Institute structures and processes for identifying and escalating potential human rights concerns raised by the operation of facial recognition systems and ensuring that findings are acted on and integrated into decisionmaking.
3. Perform rigorous testing on facial recognition systems prior to deployment to determine their accuracy and ensure they are free from demographic biases.
4. Institute policies to ensure accountability for compliance with these recommendations.
5. Provide individuals with the opportunity to seek remedy for rights violations.

Transparency

1. Release a policy statement outlining the operator's human rights commitments.
2. Provide clear notice when FRT is in use.

3. Be open and transparent about organizational policies and practices relating to how data is collected, used, and shared.

4. Communicate how impacts are addressed.

5. Provide individuals with the opportunity to request access to data about them that was collected using facial recognition and to request correction or erasure as appropriate.

6. Institute record-keeping procedures and release regular transparency reports detailing how FRT has been used.

Operational Rules

1. Limit the collection and use of biometric data to what is necessary to achieve narrowly defined, rights-respecting purposes, and do not share or reuse data in ways incompatible with that original purpose.

2. Practice principles of privacy and data protection by design and default.

3. Ensure staff are trained as to the capabilities, limitations, and proper use of the facial recognition system.

4. Institute policies and practices that ensure for meaningful human oversight or review over any decisions made by facial recognition systems.

5. Implement security measures to protect the data contained in enrollment databases and retain face templates for no longer than necessary.

6. Whenever possible, obtain free and informed consent before enrolling individuals in a program that uses facial recognition.

7. When not based on explicit consent, FRT deployments must include heightened protections, including strict limits on enrollment and data reuse.

Finally, the report proposes a set of recommendations to policymakers for how legal and regulatory regimes can be updated to address the risks posed by facial recognition.

Creating a Legal and Regulatory Regime that Protects Fundamental Rights and Freedoms

1. Clarify impermissible uses of FRT for both public and private sector actors.

2. Set out the legal basis under which different forms and uses of FRT can proceed.

3. Encourage the adoption of common standards of accuracy and non-discrimination.

4. Ensure remedy is available to individuals impacted by FRT deployments.

5. Establish strong privacy and data protection regulations to set limits on the collection and use of data.

6. Create a framework for private sector actors to follow in conducting human rights due diligence.

7. Build an enforcement capacity to ensure that operators are complying with their obligations

under national or human rights law and create penalties for organizations that violate individuals' rights.

Regulating Government Facial Recognition Operators

8. Require public sector agencies to carry out human rights impact assessments (HRIAs) prior to the use of FRT.
9. Create mechanisms for independent oversight over the deployment and use of FRT by government operators.
10. Ensure that the use of FRT by law enforcement is subject to oversight by an independent judiciary.
11. Clarify how evidence derived from FRT may be used in court.
12. Require agencies to conduct scenario or operational tests prior to deployment to gather data about the real-world performance of FRT systems and identify possible risks.
13. Require government operators to adhere to the operational rules and principles listed in the previous section.
14. Require public agencies to publicly release information about their policies and procedures regarding FRT and publish regular transparency reports detailing how their systems have been used.
15. Place clear restrictions on the sharing of data between government agencies and between government and the private sector.
16. Provide resources to support technical capacity building for government agencies.

1

Introduction

After a decade of rapid progress in the field of computer vision, facial recognition technology (FRT) has matured to the point that numerous organizations around the world—from police and border control agencies to banks and retail stores—are now beginning to experiment with its use. If deployed responsibly, proponents hope that facial recognition may support public safety initiatives and improve access to services. However, FRT is still limited in many ways and risks compromising a range of fundamental human rights and freedoms if not deployed in the context of strong operational safeguards and comprehensive legal protections. This is particularly true in the case of nations with weak rule of law.

This report examines current trends in FRT deployment around the world, with the purpose of understanding how FRT will come to be used by different actors, how operators are thinking about the risks the technology poses, and what more can be done to ensure that deployments respect fundamental human rights and freedoms. The current lack of governance for FRT has helped prompt discussions of bans and moratoria on multiple continents. More robust discussions are urgently needed to determine whether there are use cases that are fundamentally incompatible with human rights, as well as how operators and policymakers can craft an appropriate and tailored governance framework that takes into account the full spectrum of potential impacts. This report provides a contribution to that discussion.

A companion report, *Facing the Risk Part 1: Mapping the Human Rights Risks in the Development of Facial Recognition Technology*, provides a complementary analysis of the facial recognition supply chain and how decisions made by FRT developers can affect the risks posed by the technology.

2

What Is Facial Recognition?

Facial recognition is a subfield of artificial intelligence (AI) research focused on using deep learning to build software systems that can identify faces in images and video. Facial recognition programs work by transforming face images into numerical expressions that can be compared to determine their similarity.

One of the most common uses of FRT is *verification* (also known as 1:1 matching), where the technology is used to confirm whether a person is connected to a specific identity record. Examples of verification include when a person uses their face to unlock their smartphone, sign into a banking app, or verify their identity when passing through airport security. When a person attempts to log in, the system takes a picture of their face and then compares it with the image on record for that person. If the two faces are deemed a match, the person is then granted access. Comparison photos are usually either taken when a person first signs up for the service or drawn from a trusted source such as a passport or national identity registry.

Identification (also known as 1:N or 1:many matching) is when facial recognition is used to determine whether a target individual exists in a larger database of known faces. Some police agencies use identification to generate suspect lineups based on images or footage of a crime, as well as to search for missing persons and identify deceased individuals or non-cooperative suspects in custody. Identification can also be used by the private sector to enforce blacklists (i.e., when a store monitors its customers to detect for the presence of known shoplifters) or whitelists (i.e., when a building's management wants to automate the process of granting access to employees or residents).

Identification does not necessarily supply any information about who a person is. That is, FRT can be used in ways that do not actually involve collecting or linking any personal data about the person

in question. For example, some retail stores may assign unique persistent identifiers to individuals that allow the store to recognize them as return customers and track in-store behavior for marketing analysis, but not link that identifier to any biographic information, such as a name, address, or purchasing history. Similar systems can also be used in the opposite way—to identify when a person has not been seen before. An example of this is the Beijing park that was experiencing issues with visitors taking too much toilet paper and decided to install toilet paper dispensers with FRT that first check to ensure that a person had not been encountered by the system in the past nine minutes.[1]

Importantly, facial recognition is different from facial *characterization* (also sometimes referred to as facial analysis). In facial recognition, algorithms are used to compare the similarity of two faces. In facial characterization, algorithms are used to classify a single face according to its gender, age, emotion, or other characteristics. Facial characterization can sometimes be paired with facial recognition systems, but it can also be used on its own to anonymously profile individuals for purposes such as counting the number of men and women entering a particular store or providing data about how different demographic groups respond to a product or advertisement.

For the purpose of this paper, the term facial recognition should be taken as only referring to systems that compare two or more faces to determine their similarity. There are important conversations to be had about the use and governance of characterization systems—especially given recent attempts to use the technology for highly questionable and discriminatory purposes such as classifying people by ethnicity or "detecting" an individual's sexuality, political orientation, or criminality—but these should be undertaken with an awareness that facial characterization and facial recognition are distinct technologies.[2]

3

How Is Facial Recognition Being Used?

Facial recognition is being adopted by an increasing variety of organizations across both the public and private sectors. Outlined below are five of the most common use cases for the technology, along with an overview of the fundamental human rights and freedoms most affected by each type of deployment.

Law Enforcement

Law enforcement agencies around the world are using FRT in a variety of different ways.[3] Some uses, such as identifying deceased individuals or de-duplicating databases, raise few issues. Others, such as passively scanning public areas for wanted criminals or identifying dissidents from footage of protests, warrant greater concern.

In general, the law enforcement deployments that generate the most significant risks with respect to human rights can be divided into two categories: live monitoring and retroactive identification. Interviews for this report indicate that developing countries appear to be more interested in expanding their capacity to conduct live monitoring and surveillance than developed nations, which seem to be more focused on expanding retroactive identification capabilities.

LIVE MONITORING

Live monitoring refers to the practice of using facial recognition to compare individuals against a watchlist in real time as they pass within the range of facial recognition-enabled cameras. The primary risk of live monitoring is that governments will use it to persistently track and surveil their citizens, as Chinese authorities have done in Xinjiang.[4] However, live monitoring can also take place in more constrained ways that nevertheless carry significant risks. In general, the impacts of live monitoring

systems are determined by the geographic scope and length of the deployment, the number and profile of the individuals included on the watchlist, and the legal and institutional safeguards defining when and how the technology is used.

Many law enforcement agencies around the world are piloting live facial recognition systems, but there is wide variance in the scale, organization, and protections involved. In many nations, live monitoring is first piloted as a way for police forces to provide security at specific events. Indonesia, for example, has used live facial recognition on several occasions for major gatherings such as the 2018 Asian Games and IMF-World Bank annual meeting,[5] while Brazil has used it to monitor crowds during Carnival and at major football games.[6] In many countries, these types of deployments serve as the proof-of-concept that is then used to justify more expansive installations.

Many nations have also conducted pilots and trials of more open-ended deployments in public areas. In the United Kingdom, for example, the Metropolitan and South Wales police services have deployed temporary, van-based facial recognition systems in major cities.[7] In Germany, federal police trialed live facial recognition in a major train station but ceased after deciding they lacked the legal authorities to continue.[8] The city of Buenos Aires has begun to use facial recognition on the subway system to scan crowds for individuals wanted by Argentina's legal system, including minors,[9] and interviews indicate that similar subway deployments have also been proposed in Brazil. In Mexico, interviews indicate that the capital has trialed a deployment of 50 cameras placed in a major central market, while the state of Coahuila recently purchased 1,100 cameras from the Chinese firm Dahua that will match people to the country's criminal database and national identity registry.[10] This represents only a slice of what is happening around the world.

While most deployments of live monitoring to date have been on relatively small scales, there is clear interest from many governments in building on these pilots and tests by integrating facial recognition into new and existing surveillance camera infrastructure, and even by piggybacking off of private surveillance camera networks. However, there is little evidence so far of agencies successfully accomplishing this in a large-scale, coordinated way. Many agencies—particularly those in developing nations—face significant barriers to scaling up live facial recognition due to constraints in technical infrastructure and organizational capacity. Several interviews with stakeholders in developing nations revealed that officials unfamiliar with the technical specifications of the systems will frequently install new surveillance cameras at heights and positions that make them nearly useless for live monitoring. And even when the technical infrastructure can be deployed correctly (sometimes with the help of foreign engineers or by outsourcing the management to private firms), many nations may lack the organizational coherence to take advantage of the technology. However, while these barriers may slow the development and impacts of a full-scale facial recognition-based surveillance infrastructure in many countries, it will not prevent them.

RETROACTIVE IDENTIFICATION

Retroactive identification refers to the practice of applying facial recognition software to captured images or video to quickly identify persons of interest. Retroactive identification is quickly gaining widespread adoption around the world due to its growing availability, relative ease of use, and value in generating leads for law enforcement investigations. Retroactive identification can have benefits insofar as it helps address violent crime and identify exploited or missing persons, but it has also been used by governments to target dissidents and protesters. Countries such as India, Russia, and Uganda have already employed facial recognition to identify protesters from surveillance footage, and many

other countries are suspected to have done the same.[11] Through interviews, the authors received reports that Indonesia used facial recognition on surveillance camera footage to identify and arrest those involved in protests following the country's 2019 presidential election, and that Serbia may have used facial recognition to identify protesters and arrest them for misdemeanor offenses. Recent reports indicate that the government of Myanmar installed 335 facial recognition-enabled cameras in the capital, which are presumed to now be in use for the purpose of identifying anti-coup protesters.[12]

Similar to live monitoring, the risks of retroactive identification capabilities are dependent on multiple factors, including the number and profile of individuals included on the watchlist and the legal and institutional safeguards defining when and how the technology is used. But retroactive identification differs in that it does not depend on the same kind of dedicated infrastructure as live monitoring. Retroactive analysis can be used to identify people not just from surveillance camera footage but also from social media posts, third-party recordings, body cameras, mobile devices, and any other source of images. This means that the potential impact of law enforcement gaining access to these tools is also dependent on their ability and authority to access images from a broad range of sources.

Retroactive identification can have benefits insofar as it helps address violent crime and identify exploited or missing persons, but it has also been used by governments to target dissidents and protesters.

Border Control

Many nations are beginning to use facial recognition at their borders to process immigrants and travelers. This is likely to be among the fastest-growing uses of facial recognition and carries risks due to the possibility that governments could use collected data to track and monitor individuals and their movements. Facial recognition systems are becoming increasingly common at airports as ways of checking passengers in before flights and at land borders and other entry points where immigration officials in many nations are using it to keep records of people who enter the country. Examples include the United States, European Union, Japan, Kenya, Brazil, and the United Arab Emirates, in addition to many others.[13] In some cases, the UN has been a key driver of uptake for these solutions. The UN Security Council, for example, has directed all nations to implement biometric border control systems to identify terrorist suspects, while the International Organization for Migration (IOM) has been working with countries like Kenya to install facial recognition systems at border checkpoints and expand biometric data analysis in ways that include few human rights safeguards.[14]

The primary justifications for these deployments tend to be convenience and security, as facial recognition processing could allow for travelers to make their way through checkpoints much more quickly and in a way that allows officials to more effectively monitor for known threats. However, these deployments can also create risks depending on how the collected data is used and shared. Governments may use FRT to create logs of people's movements or pass information along to other agencies or even other countries to enable surveillance by other actors. FRT could also be used to

enforce unlawful restrictions on people's freedom of movement and lead to arbitrary detention if erroneous matches are acted on. The exact risks and impacts of this application of facial recognition remain unclear, however, as few governments are fully transparent about their border control practices.

Identity Verification

Both governments and private sector entities are exploring the use of facial recognition as a way to allow individuals to authenticate their identity when accessing services. In the private sector, this authentication can be for purposes such as unlocking a mobile device, logging into a banking app, or paying at a store by scanning your face.[15] On the government side, citizens may use facial recognition as a way to access public transit, retrieve welfare benefits, or even vote.[16] In Singapore, a global leader in FRT adoption, citizens can already use facial recognition to access more than 500 government and commercial services through government-run digital identity infrastructure.[17]

In general, identity verification systems can be thought of as either centralized or decentralized. In a centralized system, a single entity—which can be either a government agency or private firm—serves as a trusted authority issuing identity credentials to users. In the case of the government, this most commonly takes the form of a national registry containing basic information about every citizen. Service providers interested in integrating FRT into their services (e.g., a bank wanting to allow its users to authenticate themselves through its mobile app using a selfie) can enter into an agreement with this central authority. When a user submits a face image during a login attempt, the provider sends that data to the centralized authority for analysis. The authority conducts a check to determine whether the scan matches the file on record for the user in question and then lets the provider know whether the user is a match or not. In decentralized verification systems, each provider would independently collect an image of their users when signing them up. Later, whenever the user tried to log in, their face would be compared against that initial image to verify their identity.

Facial recognition-based identity systems could help support financial inclusion efforts and improve access to welfare, public services, land rights, and trusted digital identities. However, the centralized collection of biometric data could lead to privacy abuses if repurposed for surveillance and could create data protection risks for any information stored with or linked to those identifiers. If made a requirement for accessing essential public services such as welfare, error-prone systems may result in some individuals consistently facing denied access and limited opportunities to seek remedy. Additionally, depending on the quality of the system used, some identify verification systems can be fooled by a photograph, which could lead to identity theft that would then affect access to government benefits or other rights or services.

Facial recognition-based identity systems could help support financial inclusion efforts and improve access to welfare, public services, land rights, and trusted digital identities. However, the centralized collection of biometric data could lead to privacy abuses if repurposed for surveillance.

FRT and Covid-19

Covid-19 has given some governments justification to expand their use of facial recognition systems in the name of public health. In China and Russia, for example, FRT has already been used as a way of enforcing Covid-19 quarantine measures.[18] Facial recognition is also being used to create records of people's movement to support contact-tracing efforts.[19] In Japan, for example, authorities are considering using FRT to register people who attend large-scale events so they can be contacted later if they are found to have close contact with virus carriers.[20]

In countries that do not already have a roust facial recognition infrastructure, the pandemic could catalyze a rush to deploy health monitoring systems that could eventually lead to more expansive forms of surveillance. In Africa and Latin America, for example, interviews for this report indicated that Chinese companies were taking advantage of Covid-19 concerns to donate or sell health monitoring systems to companies and government offices, including cameras that could be used for FRT. Once these systems are established, it will become easier to justify the deployment of additional surveillance systems that combine their data together in ways that could create substantial privacy risks.

Covid-19 also risks driving the adoption of facial recognition if economic pressures and unrest create instability that could be used as a justification for an expanded security infrastructure.

Access Management

One of the most common applications of FRT today is to help automate the process of letting authorized individuals into restricted areas, taking the attendance of workers and students, and even tracking people as they move through an area. In workplaces and residential complexes, these systems are seen as a way to modernize and improve security checks.[21] Instead of using badges or some other non-biometric credential, building managers can set up face registries containing everyone who works in the building and allow people to scan themselves at entry gates to automatically be let into the complex. These systems may also be used to alert building security if unauthorized people enter restricted areas. In schools, factories, and offices, administrators see FRT as an opportunity to replace manual attendance systems that are considered either inefficient or too prone to manipulation.[22] Retailers may use FRT systems to identify and track VIP customers or those who have signed up for loyalty programs as they move through the store, gathering data to inform marketing efforts.[23]

Because these systems require relatively small investments to set up and are deployed in ways that make them easy to integrate into existing processes, access management will likely be one of the fastest-growing FRT use cases—and, along with identity verification, the most likely to become a daily part of people's lives in the near future.

The risks of FRT access management systems primarily stem from the way data may be collected and shared about individuals without their knowledge or consent, in violation of their right to privacy. The most acute risks apply to children in cases where FRT is deployed in a school setting for attendance taking or security. Experimentation inspired by these FRT systems may lead to employers and educators instituting even more technology to keep track of the way their workers and students are acting during the day, further eroding their privacy. FRT access management systems may also impact individuals' freedom of movement both indirectly, through chilling effects, and directly, if errors cause some individuals to be arbitrarily denied access to workplaces, residences, or other locations. The

technology can have benefits, however, in situations where biometric attendance may help vulnerable workers who otherwise would be at risk of abusive work conditions.

FRT access management systems may impact individuals' freedom of movement both indirectly, through chilling effects, and directly, if errors cause some individuals to be arbitrarily denied access to workplaces, residences, or other locations.

Private Security

While much attention has been paid to the ambitions of government agencies to use FRT to monitor for criminal and security threats, comparatively less attention has gone to the growing trend of FRT security systems deployed by private actors. These types of systems are being used for a range of tasks, including detecting known shoplifters at retail stores, identifying trespassers at industrial complexes, preventing people who have caused trouble at past sporting events from entering stadiums, stopping gambling addicts from entering casinos, and identifying stalkers at concerts.[24] Adding FRT capabilities to existing security camera infrastructure allows private operators to automate the process of monitoring for known or suspected threats that have been identified by the operator. This monitoring can be done by the operator themselves or by specialized private security firms contracted by a property's management. Private security systems may be paired in some cases with the access management systems described above.

While the use of these systems may have security benefits in some situations, they carry substantial privacy risks that can only be justified if operators are able to pass a high bar of proving the necessity and proportionality of the system in use. Beyond these risks, private FRT security systems could also lead to risks to children's rights to privacy and education if deployed at schools; endanger the right to an adequate standard of living for individuals cut off from essential services, such as grocery stores, due to inclusion in FRT shoplifter watchlists; and increase both direct and indirect restrictions on people's rights to freedom of movement, expression, and assembly. The risks of private security systems also intersect strongly with the risks associated with law enforcement use if data sharing arrangements are put in place that allow the government to access footage or data derived from private deployments. Such arrangements could lead to an opaque and unlawful extension of government surveillance powers.

4

The Impact of FRT Deployment on Human Rights

Right to Privacy

LAW ENFORCEMENT

Facial recognition is uniquely capable of allowing for the remote identification and surveillance of individuals. Law enforcement agencies can take advantage of this to track and target activists, dissidents, and ethnic and religious minorities at an unprecedented scale. Live facial recognition presents the clearest privacy risk due to the way it could enable authorities to construct detailed databases revealing sensitive information about people's lives and activities. However, retroactive identification also creates significant risks by increasing law enforcement's capacity to identify and target individuals based on surveillance footage, social media posts, and other image sources. All of these uses would deeply interfere with respect for individuals' private lives. Even when used in more restrained ways, the capture and processing of biometric information without an individual's consent qualifies as an invasion of their privacy which must be justified as a necessary and proportional intervention.

The privacy impacts of law enforcement FRTs are affected by the number, profile, and source of images included on the match list and the legal and institutional safeguards defining when, where, and how FRTs can be used. The privacy risks of law enforcement FRT deployments is particularly acute because of the possibility that people may never realize they are being monitored. And even when individuals are aware that FRT is being used, law enforcement FRT systems usually provide no means of opting out and are often deployed in public areas that people may not be able to avoid. Importantly, the fact that surveillance is taking place in a public space does not remove the potential for privacy impacts. The Human Rights Committee has found that the right to privacy protects individuals from being identified by facial recognition even during public assemblies.[25]

BORDER CONTROL

The collection of biometric data at border checkpoints can create potential privacy risks depending on how the information is used and who it is shared with. The greatest risk is that governments will use FRT to create logs of people's movements—including vulnerable populations such as migrants—in ways that cannot be justified as necessary or proportionate to any legitimate state aim. Biometric information collected from travelers also risks being passed on to other government and law enforcement agencies within the country that could maintain surveillance on individuals after they have crossed the border.

In Indonesia, for example, interviews with the Directorate General of Immigration indicate that authorities have used facial recognition to help them track immigrants when they enter the country and as they pass through internal checkpoints. One of the primary motivations of the system is tracking illegal migrants transiting through Indonesia to seek asylum in Australia or New Zealand. Authorities use FRT to keep records of when people pass through, screen immigrants against lists of known terrorists, and ban certain individuals from re-entry. Depending on how this information is handled, this processing may constitute a violation of those travelers' privacy rights. Officials also confirmed that they had used biometrics taken from undocumented immigrants to identify suspected criminals in the country, raising questions around the safeguards involved in data sharing between border and law enforcement authorities.

There are also risks that data could be shared between different countries in ways that would allow individuals to be tracked internationally without their awareness. Indonesia, for example, confirmed that the biometrics they were taking from immigrants were being shared with other countries through bilateral cooperation agreements. The UN Security Council itself has encouraged the international sharing of biometric data as a way to identify terrorists and foreign terrorist fighters.[26] However, the mandate of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has found that this mandate contains inadequate guidance for how its provisions can be adopted in ways that avoid compromising human rights, creating risks that states may design systems that lead to the overbroad sharing of data without adequate safeguards.[27]

IDENTITY VERIFICATION

Identity verification systems allow greater opportunity for subject consent than those used for remote verification and therefore have a better opportunity to mitigate some of the technology's associated privacy risks. Users of face verification services are almost always aware when facial recognition is being used and have agreed to the terms of data processing. The primary exception to this is when FRT is used to authenticate individuals who are trying to access public services such as welfare or public transit. If the government does not provide any other option for authentication and the user feels they have no choice except to use the system, consent cannot necessarily be considered valid. This is also the case when users have not been provided clear information about how their data will be collected and processed.

Even if the user is willing and able to freely give their informed consent, there are still privacy risks stemming from the way that collected data is reprocessed and shared. These risks are strongly affected by whether the identity system in question is centralized or decentralized. Centralized setups minimize the number of organizations that have access to sensitive biometric data, in contrast to decentralized systems, where each individual service provider is responsible for maintaining their own

database of user credentials. So long as service providers do not store the data they collect during login attempts—something that many choose not to do in order to avoid regulatory scrutiny under privacy and data protection laws—the central authority should be the only entity to hold users' biometrics, reducing privacy risks.

However, the use of centralized authorities can create new privacy risks if providers send not just a biometric scan but also details about users' activities. If a single entity is involved in approving individuals' logins for everything from welfare and public transit to financial services and retail, there are substantial risks that the authority could be able to compile profiles of individual users that could include enough information to offer an extremely invasive view into their private lives. Many authorities and operators take steps to ensure that no data of this sort is transmitted during the check, but these protections are not always guaranteed.

There are also risks of the reverse happening. In the process of authenticating a user, the central authority may send back more information than is necessary to the service provider, exposing personal data. In Indonesia, for example, the Ministry of Home Affairs has recently begun working with over 1,000 companies to provide face-based authentication of their customers. The ministry says that they do not provide those operators with any data other than the verification decision. However, in interviews, civil society organizations highlighted that a previous government program offering verification services to telecoms for SIM card registration was rumored to have resulted in telecom operators gaining access to the full government identity database after the ministry responsible became overwhelmed with requests.

Decentralized verification systems reduce some of these concerns by avoiding the need for a single entity to be involved in such a broad cross section of individuals' lives. Instead, each provider would maintain their own database of user credentials. This would avoid the situation of a single organization having information about multiple different aspects of a person's life (as long as that information was not being shared or sold behind the scenes) but would require users to trust a large number of different institutions with their sensitive biometric data.

Facial verification systems could also create privacy risks if FRT allowed providers to collect new kinds of non-biometric data about their users. For example, if a face verification system replaced a formerly anonymous cash- or card-based ticketing system on a bus line, that would create opportunities to collect information about the identities and habits of passengers that previously would have been impossible to collate.

ACCESS MANAGEMENT

Access management systems can pose privacy concerns in workplaces, retail environments, and residential complexes where the data collected by these systems could be shared and repurposed to build profiles of people's behavior. Even if not shared in this way, the collection of sensitive biometric information can only be justified if necessary and proportional to the purpose being served. While keeping unauthorized individuals out of certain complexes may be an important goal, the availability of far less privacy-invasive alternatives such as keys or card badges raises questions over whether the use of FRT may be justified.

PRIVATE SECURITY

Private security FRT systems almost universally require the processing of subjects' biometric information without their consent. The use of these systems therefore almost always qualifies as an invasion of privacy and should be justified as necessary and proportionate.

Some of the most serious privacy risks associated with private security FRT systems relate to how the data being collected is shared with other entities. For example, if private operators were to share their customers' biometric data with one another, it could allow some businesses to monitor individuals who are totally unaware that they have become part of a third party's FRT system. This could occur in the case of retailers sharing customer information, stores sharing the details of known shoplifters, or stadiums and other event venues sharing information about troublemakers they have dealt with. Because of the sensitivity of the biometric data involved and the lack of awareness of the subject, these types of sharing arrangements face a very high bar to be justified. Because of technical constraints, this risk is highest among organizations that use the same vendor to supply their facial recognition systems.

There are also risks associated with sharing the non-biometric data captured as part of FRT operations, such as the purchase history or login details of customers who use a store's loyalty program. If this information were to be shared with other businesses, it may allow third parties to create invasive profiles of individuals' buying habits and movements. This data sharing already happens in many industries, but FRT may make it easier for some businesses to capture an expanded range of non-biometric data that could become a part of these sharing arrangements.

Privacy risks may also come from operators sharing data with law enforcement agencies. In the United Kingdom, for instance, the owner of the 67-acre King's Cross development was revealed to have been using facial recognition for several years to monitor visitors and share information with police forces.[28] In some jurisdictions, there may be an obligation for private CCTV operators to turn over access or footage from their systems to government officials. Interviews for this report found this to be the case in Jakarta, and it is likely that many other jurisdictions have or will soon propose similar rules. Because government agencies have different powers and authorities to take advantage of data collected through FRT systems, these sharing arrangements can raise some of the most serious privacy concerns, especially when governments and private operators are not transparent about their details.

Data sharing already happens in many industries, but FRT may make it easier for some businesses to capture an expanded range of non-biometric data that could become a part of these sharing arrangements.

Freedom of Expression, Assembly, and Association

LAW ENFORCEMENT

Facial recognition can threaten individuals' freedom of expression, assembly, and association by enabling law enforcement authorities to identify and retaliate against those engaging in acts of

dissent. This has already happened in countries such as India, Russia, Uganda, and Indonesia, where protesters were arrested for allegedly committing criminal acts during demonstrations. However, there are also risks that FRT could be used to enable not just the arrest of protesters but also extra-legal intimidation and harassment. In Indonesia, for example, one NGO interviewed for this report revealed that the country's ex-minister of home affairs had threatened to reveal the personal information of a protester who had been identified from footage of a demonstration. While it was not confirmed that this identification was achieved by using FRT, the technology would make this kind of harassment easier to achieve at scale in the future. Similarly, advocates in Zimbabwe expressed concern that the government intended to use FRT to monitor strikes and protests and remove anyone identified in those demonstrations from government payrolls as punishment.

Even if governments do not take these kinds of actions against demonstrators, as long as citizens have reasonable fear that the technology may be used to monitor them, there is a risk that individuals may begin to self-censor and decline opportunities to participate in activities they fear could arouse suspicion from the government.[29] Interviews with stakeholders across Africa, Southeast Asia, and Latin America have revealed that even in countries where facial recognition's use on protesters could not be confirmed, known uses of location tracking and spyware against dissidents and opposition members have led to widespread fears among activists that technologies such as facial recognition may already be used in secret.

Measuring the chilling effects resulting from these concerns is notoriously difficult, but a number of public opinion surveys and studies have consistently demonstrated that individuals change their behavior in response to government surveillance.[30] Notably, even if FRT is inaccurate or not even in active use, those chilling effects can still manifest if the populace believes they will be identified by it. The risk of chilling effects would worsen if more actors deploy FRT in similar areas without adequate safeguards or protections and if data is known to be shared between government agencies—what this report calls "cumulative effects."

As long as citizens have reasonable fear that the technology may be used to monitor them, there is a risk that individuals may begin to self-censor and decline opportunities to participate in activities they fear could arouse suspicion from the government.

PRIVATE SECURITY

The use of FRT by private actors for security purposes can have direct risks to freedom of expression, assembly, and association if law enforcement agencies are able to use images or footage from private networks to identify and retaliate against individuals engaged in protected speech or assembly. As addressed in the previous section on privacy, there is growing risk that opaque public-private data sharing arrangements could allow authorities to gain access to footage or facial recognition-derived data they may not otherwise be able to obtain legally. This could have direct impacts on fundamental

freedoms if used to retaliate against those engaging in protected acts, as well as chilling effects if individuals fear that they are being monitored and choose to self-censor or not participate in activities they fear could arouse suspicion or lead to harm for them and their friends and family.

Freedom from Arbitrary Arrest and Detention

LAW ENFORCEMENT

The use of facial recognition systems can lead to arbitrary arrest and detention when states use FRT to support arbitrary or unlawful enforcement actions or when individuals are targeted by mistake due to erroneous facial recognition matches. The risk of arbitrary detention exists because FRT systems often struggle to achieve reliable performance in real-world settings. Though top facial recognition systems can achieve very high accuracy in ideal conditions, operational deployments continue to experience significant performance challenges due to the difficulty of matching to low-quality images where the subject may be obscured, turned away from the camera, or in bad lighting.[31]

Developers who sell to law enforcement users frequently emphasize that the technology is not reliable enough to be used as the sole basis for arrest.[32] However, there are significant risks that this advice will be disregarded and that the technology may end up substituting for, rather than supplementing, the more rigorous forms of evidence gathering and corroboration that are required to ensure due process. One Asian FRT developer interviewed for this report highlighted these risks when relating that one of their greatest challenges is dealing with users who expect the system to always return the correct individual as the first match. If law enforcement users operate under this assumption and do not have institutional safeguards in place to ensure that other evidence is used to justify detaining a suspect, it will lead to large numbers of false and arbitrary arrests.

The risk of arbitrary arrest and detention also exists when facial recognition is used for live surveillance, such as when it is deployed on a street corner or at a major event to scan the public against a watchlist of known criminals. While data on the performance of these systems is sparse, one independent assessment of six live facial recognition trials by the UK Metropolitan Police Service found that the system was only verifiably correct in 19 percent of instances.[33] Due to the risk of false positives from facial recognition systems, there is a risk that innocent individuals could be stopped and held after triggering false alerts by law enforcement systems. In theory, law enforcement officers should have procedures in place for secondary verification to avoid having to rely entirely on a facial recognition match when deciding whether to take action against an individual, but in practice this is not always the case. For example, interviews for this report revealed an instance in Latin America where an individual was held for six days before authorities realized the facial recognition match was erroneous.

Due to the risk of false positives from facial recognition systems, there is a risk that innocent individuals could be stopped and held after triggering false alerts by law enforcement systems.

BORDER CONTROL

If facial recognition is used to screen travelers against watchlists of criminal or terrorist suspects, facial recognition matches may be used as the basis for deciding to detain an individual at the border. While some of these interventions may be lawful, it is possible that others may be erroneous, due to misidentifications by FRT systems, or deliberately malicious, in the case of unlawful detentions. In ideal circumstances, border checks would not be reliant solely on FRT for traveler verification, and any errors in the process would be resolved through prompt intervention by human adjudicators. However, some countries may overestimate the reliability of FRT systems and create automated border systems that do not allow sufficient opportunity for meaningful human review of decisions. This could lead to the wrongful detention of travelers.

IDENTITY VERIFICATION

There is a risk that law enforcement, intelligence services, and the military may exploit data gathered through government or private sector face verification programs to arrest and detain individuals unlawfully. One example of a program that has raised these concerns is in Thailand, where interviews indicate that telecom companies have been pushed by the military to collect the face images of all SIM card owners. Though the use of FRT on these images could not be confirmed, the official justification for this requirement is that it would make it easier for security forces to track and identify individuals using mobile phones to set off bombs. This makes it highly likely that this SIM card registration system could eventually be repurposed to support FRT surveillance. In nations with few institutional safeguards and weak rule of law, the potential for abusing this kind of data collection is high.

PRIVATE SECURITY

There are substantial risks that law enforcement agencies may use private security systems as a cat's paw to obtain evidence for investigations that they could not obtain legally themselves. For example, if national law prevented a law enforcement agency from deploying an FRT monitoring system in a public area, officials may decide to get around that restriction by entering into arrangements with the owner of a store whose private CCTV camera system looks out over the same space. This could lead to law enforcement identifying and arresting suspects in an illegal manner without providing them due process.

Even if data sharing takes place under a legitimate legal regime, it is possible that errors in facial recognition analysis could lead to innocent people being arrested and detained. This risk also exists even when private operators are doing the identification themselves. If they report an individual to the police due to a false match by their FRT system, it may lead to that person's false arrest and imprisonment.

Right to Non-Discrimination

The Universal Declaration on Human Rights (UDHR), International Covenant on Civil and Political Rights, and International Covenant on Economic, Social, and Cultural Rights all guarantee individuals the right to non-discrimination, and this right cannot be restricted. Facial recognition presents risks to the principle of non-discrimination in two key ways.

The first relates to possible biases embedded in the systems themselves. In late 2019, the U.S. National Institute for Standards and Technology (NIST) tested nearly 200 algorithms and found that the majority had different accuracy rates for different demographic groups.[34] In particular, NIST found that Asians, African Americans, and American Indians were more likely to be misidentified by facial

recognition systems than white individuals, that women were more likely to be misidentified than men, and that children and the elderly were more likely to be misidentified than middle-aged adults.

Though some algorithms were shown to have no discernible bias—indicating that this issue may eventually be resolved with improvements in the development process—NIST's findings highlight the risk that current deployments of biased systems may lead to vulnerable and minority populations bearing a disproportionate burden of the effects of facial recognition errors. The impacts of these errors will vary according to the use case, but these biases are particularly concerning in the context of law enforcement use where false matches could lead to individuals being unjustly targeted for investigation or arrest. Interviews for this report confirmed that in many countries, governments have no procedure for formally assessing bias in the systems they are purchasing, despite human rights obligations to ensure that individuals enjoy equal protection under the law.

The second way facial recognition can lead to discrimination is if certain groups are disproportionately represented in the watchlists these systems are matching against. In the law enforcement or private security cases, for example, this may occur if the sources of matching images are criminal databases, which may be composed of a disproportionate number of minority individuals. Even if an algorithm shows no difference in its accuracy between demographics, members of these groups would be more likely to be identified and tracked by authorities because their information is more easily accessible. They are also more likely to be impacted because their communities are often already the focus of criminal justice or private security interventions that FRT may be a part of. This leads to risks that historical discrimination could be reinforced and amplified through the adoption of algorithmic systems. In the United States, for example, pharmacy chain Rite Aid was criticized for rolling out FRT security systems only in low-income, minority neighborhoods.[35]

If packaged together with face characterization software, facial recognition could also be used in some countries to intentionally discriminate against certain groups. The use of facial characterization to try and determine an individual's ethnicity, religion, or sexual orientation could be used as a way to profile individuals and mark them for further tracking, denial of services, or other restrictive measures. While characterization is technically separate from facial recognition, many platforms allow for both types of analysis to be performed, creating risks that some operators may use facial recognition selectively on certain groups as identified through facial characterization systems. Some Chinese developers, for example, have already built systems that send an alert to police whenever it detects someone it classified as a Uyghur.[36] Though these characterization technologies are often highly unreliable—and, in some cases, unlikely to ever be reliable—some governments and businesses may nonetheless deploy these tools without consideration for the impact of errors that result, or with the specific purpose of contravening the right to non-discrimination.

Right to Effective Remedy

LAW ENFORCEMENT

The UDHR guarantees all individuals the right to effective remedy in the case that their rights have been violated. This right is most directly threatened by forms of facial recognition surveillance that occur without the awareness of the subject. Because facial recognition allows for the movements and behaviors of large numbers of people to be recorded and analyzed remotely, individuals may not always be aware of when they are subjected to facial recognition. They may also be unaware of

instances where facial recognition was used to inform in-person stops by law enforcement officers or when it has been used as an investigative tool to gather evidence against them that is presented during trial. This lack of awareness makes it difficult for individuals to seek clarification on how and why the surveillance is taking place and to request remedy if they believe their rights have been violated. The right to remedy is also impacted if a state lacks legislation clearly authorizing and defining the limits of facial recognition use. If there is no clear law setting out how these systems can and cannot be used, it becomes far more difficult for individuals to successfully petition their national government for different policies.

Because facial recognition allows for the movements and behaviors of large numbers of people to be recorded and analyzed remotely, individuals may not always be aware of when they are subjected to facial recognition.

BORDER CONTROL

All travelers, but especially vulnerable populations such as migrants and asylum seekers, face challenges in determining how their biometric information is being used and shared by border authorities. Because these arrangements are usually categorized as a matter of national security, there is often extremely little transparency about the circumstances surrounding data processing and few opportunities to request clarification about who the information is being shared with. These obstacles are magnified for migrant populations, who face significant legal and practical hurdles in challenging the practices of immigration officials.

IDENTITY VERIFICATION

If authentication via FRT is made a requirement for accessing essential public services such as welfare, there is a risk to individuals who facial recognition fails to successfully verify. This risk is particularly serious in cases where authentication is occurring remotely or where the introduction of FRT causes authorities to remove other opportunities for non-biometric authentication due to overconfidence in the performance of facial recognition systems. In these instances, individuals may be left with few options to challenge errors made by FRT systems or seek compensation for any harms that result.

PRIVATE SECURITY

Depending on what mechanisms are in place to resolve errors, it is possible that some individuals may be denied access to stores, sports venues, residential complexes, and more due to false matches by security systems. If there are not processes in place to allow a human adjudicator to quickly address and rectify errors, it could lead to people being denied their rights, without the ability to seek redress. Private security systems could also share many of the risk factors associated with law enforcement deployments by virtue of the fact that they tend to be deployed in similarly opaque ways. This makes it challenging for individuals to determine whether their rights have been violated and to seek remedy. Private security deployments, however, have a greater opportunity to mitigate some of these risks through notice and consent practices.

Freedom of Religion

LAW ENFORCEMENT

The use of facial recognition systems can impact citizens' freedom of religion due to the chilling effects of deployments targeting particular groups. In countries with a hostile stance toward certain religious minorities, the use of cameras to track and make record of members entering and exiting religious services could make individuals hesitant to participate in religious activity. In China, authorities have gone so far as to install cameras in religious buildings to monitor visitors.[37] Even if the gathered data is never actively exploited to take actions against those individuals, the simple act of monitoring may affect those individuals' perceptions of their safety, and thus their actions.

In some other countries, facial recognition has been used as an excuse for denying individuals the right to practice their religion. For example, in 2019, officials in Tashkent, Uzbekistan forced 100 men to shave their beards so that they could be more easily identified against their passport pictures by smart surveillance systems.[38] Similar justifications could cause Muslim women to be forced to remove their face coverings, denying them their right to religious expression.

Freedom of Movement

LAW ENFORCEMENT

The use of facial recognition by law enforcement may create chilling effects on people's freedom of movement. If certain public areas are known or believed to be monitored by facial recognition, individuals wanting to exercise their right to privacy by avoiding those systems may become limited in the areas they feel comfortable occupying. People may feel cut off from areas such as transit stations, commercial hubs, or common gathering spaces or stop traveling within the country due to a fear of their movements being tracked.

BORDER CONTROL

Facial recognition can be used by states to help control who is allowed to enter and leave the country. Under the International Covenant on Civil and Political Rights (ICCPR), individuals are afforded the freedom to exit or enter their country at will. The only exceptions to this freedom are restrictions that are provided by law, necessary for reasons including national security or public order, and consistent with other rights under the ICCPR. While FRT can help states more effectively implement lawful restrictions on people's entry and exit, it can also make it easier for states to implement unlawful measures, including arbitrarily preventing dissidents or activists from traveling outside the country or barring entry to immigrants or asylum seekers with a right to enter the territory.

ACCESS MANAGEMENT

Errors made by FRT access management systems may prevent individuals from accessing areas they have a right to occupy. Depending on whether there are readily accessible means to resolve errors, this could lead to people being locked out of residential complexes or being unable to access transportation or enter their workplaces. FRT access management systems may also create chilling effects on these rights and freedoms if individuals wishing to avoid being monitored by FRT become limited in the spaces they feel comfortable occupying, the housing they feel they can occupy, or the jobs they feel they can take. If the use of FRT in these settings cannot be justified as necessary and proportionate, people may be forced to choose between these freedoms and preserving their right to privacy.

PRIVATE SECURITY

Private FRT security systems may be used to deny individuals access to areas they have a right to occupy. The monitoring of neighborhoods by private security firms is one example. Interviews for this report showed that in many countries wealthy neighborhoods turn to private security providers rather than law enforcement to protect their homes. These security providers are increasingly adopting intelligent video analytics to support their work, which in some jurisdictions may include facial recognition. Information may be pooled across a neighborhood or multiple neighborhoods to enable private security services to monitor large areas using common watchlists created privately by communities from sources such as publicly available mugshot databases. These practices could result in the emergence of a patchwork of private surveillance operations with little transparency and no accountability to the public and lead to harassment and limitations on freedom of movement for those identified as persons of concern.

Rights of the Child

LAW ENFORCEMENT

Facial recognition has become a common tool used in child exploitation investigations. By matching the faces of children captured in photos and videos, investigators are able to produce leads that can help them identify and locate exploited children and their abusers. In general, FRT tends to have high error rates in these situations, as the quality of images and video may be very low. But many investigators around the world have nonetheless purchased or trialed FRT tools as part of their work. In particular, Clearview AI—the controversial firm whose facial recognition product allows customers to search against a database of 3 billion photos scraped from social media—has become a popular investigative tool for child exploitation cases in countries such as the United States, Canada, and Australia.[39] This is because its large, uniquely-sourced database helps investigators who may otherwise struggle to compile a broad, up-to-date database of photos to match against the images taken from child exploitation materials.[40] Notably, however, this breadth of coverage is also what raises such serious privacy risks when considering how Clearview could be used for other purposes.

Facial recognition has also been used as part of campaigns to identify and reunite missing children with their families. In New Delhi, for example, authorities reported that facial recognition allowed them to identify nearly 3,000 missing children in the city within four days.[41] Importantly, however, interviews for this report indicated that the accuracy rate of this system was only 1 percent when it was used. This makes it hard to determine what the actual value of the system was and how to balance the benefits of such a system with the consequences and costs of adjudicating errors. Further, these deployments are highly susceptible to mission creep. In India, for instance, facial recognition deployments initially justified as necessary for identifying missing children served as the basis for the system that eventually was used to identify 1,100 protesters in early 2020. Nevertheless, as the technology continues to improve, the use of FRT for identifying missing and exploited children may be one of the most justifiable, as long as it is subject to appropriate safeguards.

In addition to these potential benefits, FRT can also pose risks to children's rights when the images of minors become part of law enforcement surveillance systems. In Argentina, for example, a live facial recognition system deployed in the Buenos Aires subway was set up to scan people against a criminal database that includes dozens of children accused of minor crimes such as petty theft.[42] The risk of

misidentification in these cases is extremely high. Facial recognition systems are known to have high error rates for children because the photos being matched against are from ID cards that are rarely updated. This creates substantial risks to children and would almost certainly not be considered to meet any reasonable standard of proportionality or necessity.

IDENTITY VERIFICATION

If identity verification is used for purposes such as authenticating students taking remote tests or logging children into mobile apps or public services, the operator faces heightened requirements to ensure that the use is necessary and proportionate and that consent is properly obtained from guardians. If these requirements are not met, it could result in the collection and processing of data about children in violation of their rights.

ACCESS MANAGEMENT

Around the world, a variety of schools have begun to pilot the use of FRT to automate the process of taking attendance in classrooms. These programs seek to end the gaps and omissions of a teacher roll-call, as well as to verify if the student is really there in locations where fraudulent attendance is common.[43] Schools also hope to save teachers' time. One local Swedish authority justified its decision to begin trialing the technology by pointing to statistics showing that teachers in the country spent 17,000 hours a year reporting attendance.[44]

Interviews indicate that private schools, due to their greater administrative flexibility and pressure from parents, have been particularly aggressive in experimenting with different use cases. For example, a private school in Thailand has been using facial recognition to automatically send parents a text message notification when their children arrive safely each morning.

Depending on what information is collected, how it is used, and what opportunities children and their parents have to learn about and opt-out of these programs, these deployments could have serious impacts on the rights of these children, particularly the right to privacy. Given the heightened protections afforded to children and the presence of clear alternatives that do not involve the same invasion of privacy, it is highly questionable whether an FRT attendance system at a school could ever be deemed necessary and proportional. These deployments would also violate children's right to education if access is conditioned on submitting to unlawful privacy invasions. In fact, courts in France and Sweden have both found that automating attendance was not a strong enough reason to justify the privacy violation that resulted, and that consent cannot be considered meaningful in these cases because of the difference in authority between the student and their school.[45]

PRIVATE SECURITY

Some schools are trialing the use of FRT as a way to identify unauthorized intruders and gun-shaped objects and to supplement or substitute for other security measures, such as security officers and metal detectors.[46] As these systems would inevitably result in the collection of biometric information from students, these systems must meet high standards of necessity and proportionality to justify the privacy violation they would entail. This analysis must take into consideration the nature of the threat the school faces, the alternate security means available, and how data would be collected and used. If access to the school was premised on submitting to an FRT security system that was not able to meet an acceptable standard of necessity and proportionality, this would also violate children's right to education. The authors deem it unlikely that a school would be able to meet such a standard.

Right to Life, Liberty, and Security

LAW ENFORCEMENT

The use of facial recognition technologies by governments can potentially have positive impacts by helping to improve the ability of law enforcement to investigate criminal activity and protect individuals from threats to their safety and security. In recent years, police departments have credited facial recognition technology with helping solve crimes ranging from theft to armed robbery, sexual assault, and even murder.[47] Moreover, in at least one instance, the authors heard from investigators that evidence from facial recognition systems has been used to exonerate a suspect accused of violent crimes they did not commit.

Interviews for this report indicated that citizens in certain crime-affected developing nations are more supportive of facial recognition due to the perceived safety and security benefits of the technology. In countries where citizens lack trust in one another, surveillance systems can provide a sense of security that many find more important than the potential loss of their privacy.

However, little data exists to quantify and prove the value of FRT to law enforcement. Due to the high error rates of operational systems, it is possible that some police deployments may have only a small benefit and possibly end up wasting time and resources that would have been more effectively used elsewhere. Deployments of live facial recognition in the United Kingdom, for instance, were observed to only be verifiably correct in 19 percent of instances.[48] Depending on the threat posed by the individuals that will be included in watchlists and the costs of diverting personnel and resources to supporting FRT deployments, law enforcement agencies may be better off not investing in FRT capabilities, particularly live monitoring. Further, the deployment of FRT can undermine public trust in law enforcement, making it more difficult for officers to effectively police their communities.

In countries where citizens lack trust in one another, surveillance systems can provide a sense of security that many find more important than the potential loss of their privacy. However, little data exists to quantify and prove the value of FRT to law enforcement.

BORDER CONTROL

Facial recognition can be used as a way to help states improve criminal and terrorist screening processes at their borders. Facial recognition can automate the process of checking travelers against existing watchlists and improve the detection of individuals carrying falsified travel documents. In fact, UN Security Council Resolution 2396 obligates states to "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists."[49] The opportunity for states to decide against the use of these systems is thus somewhat constrained in the

border control context, highlighting the importance of ensuring that the systems put in place have strong safeguards to prevent harms to other human rights and fundamental freedoms.

PRIVATE SECURITY

Private sector FRT security systems may provide safety benefits when they are able to identify and prevent individuals who present a threat to others from entering certain areas. However, to have a chance of meeting the necessary standards of necessity and proportionality, the threats must be specific and pressing. It is not enough that someone has a criminal history. They must present an articulable threat to the specific situation or area they are barred from. Examples could include known gambling addicts being removed from casinos or individuals with a history of violence at a particular venue or who have made credible threats of violence against that venue being added to exclusion lists. Even if this condition is met, it is still necessary to demonstrate that alternate security measures would be ineffective in order to justify the more invasive practice of FRT.

Right to an Adequate Standard of Living

IDENTITY VERIFICATION

Facial recognition can help promote financial inclusion by enabling mobile banking services for rural and underserved populations. In areas where local residents lack access to traditional financial institutions, mobile banking can help individuals gain access to loans, build credit, and transact more securely. But this is only possible if there is a secure and trusted way for users to sign up for these services and verify their identities. Biometrics are the most secure foundation for this verification process. FRT allows individuals to sign up easily and remotely by sending in a selfie and letting the app provider verify that photo against either a second photo of the user's ID documents or a photo held by the country's national registry. This process has significant security benefits compared to non-biometric credentials and is easier and more accessible than alternative biometrics such as fingerprints or iris scans, which require dedicated capture devices that often are unavailable in remote areas and may be unreliable on certain groups, such as manual laborers with worn fingers or diabetic patients with eye damage.

ACCESS MANAGEMENT

Errors made by FRT access management systems may prevent individuals from accessing areas they have a right to occupy. Depending on whether there are readily accessible means to resolve errors, this could lead to people being locked out of residential complexes or unable to enter their workplaces. FRT access management systems may also create chilling effects on these rights and freedoms if individuals wishing to exercise their right to privacy by avoiding places that use FRT become limited in the spaces they feel safe occupying, the housing they feel they can occupy, or the jobs they can take. If the use of FRT in these settings cannot be justified as necessary and proportionate, people may be forced to choose between their work and housing or preserving their right to privacy.

PRIVATE SECURITY

The use of facial recognition for shoplifter detection could lead to people being denied access to essential needs without due process if offender watchlists are shared and combined across stores in a region. An example of this is FaceWatch, a UK firm that contracts with retailers to remotely monitor their security camera feeds using facial recognition and notify them when known shoplifters enter

the premises. FaceWatch's offender registry is made up of photos of shoplifters captured from all of the retailers in its network. This means that individuals may be denied access to an entire network of stores because of their actions in just one. If this model gains popularity in the future to the point where it is ubiquitous in the retail environment, it could create risks that a single instance of shoplifting could result in the disproportionate consequence of preventing an individual from participating in an enormous range of commercial activity. For example, if such systems deny access to locations such as grocery stores, it could affect the right to food.

Right to Own Land

IDENTITY VERIFICATION

Similar to the banking apps used to promote financial inclusion, FRT can also be used to enable mobile apps where users can register and transact their properties. In many developing nations, a large fraction of property owners do not have official, formalized ownership of their land and their homes. Registration drives often fail to make a dent in this issue for many nations, as they do not fix the underlying problem that the time and cost of going through official channels to register and sell properties leads many property owners to prefer informal, undocumented arrangements.

Improving this situation requires both reducing the friction associated with the registration and sale of property and making the process more attractive to owners by tying property ownership to expanded credit, loan opportunities, and other financial services. Both of these goals are aided by the emergence of new mobile platforms that allow property owners to register themselves and their land as part of new real estate and fintech ecosystems. One company interviewed for this report has already reported success with using FRT for such a program in Zimbabwe.

Right to Social Security

IDENTITY VERIFICATION

Facial recognition can be used as a way of verifying the identities of those collecting welfare benefits. The Indian state of Telangana, for instance, allows pensioners to claim their pensions by authenticating with a selfie, bypassing the process of having to visit the local treasury department.[50] The state is also considering using the same system to distribute rations in the future. This kind of system can be particularly helpful for individuals in remote areas or those who have jobs or medical conditions that make it difficult for them to regularly complete the manual process of physically claiming their benefits. However, if adequate safeguards are not in place, errors in authentication could lead to some being denied their rights to government benefits. There are also risks that low-quality algorithms without liveness detection may fail to detect the difference between a person and a photograph of the same person, allowing malicious actors to defraud welfare systems by tricking it with images of other people and claim their benefits.

Right to Just and Favorable Conditions of Work

ACCESS MANAGEMENT

Biometrics can help protect the rights of laborers by enabling systems of accountability in dangerous workplaces. In Thailand, for example, interviews for this report have confirmed that the government

uses iris scans as a way of keeping track of those who work on fishing boats. By making a log of each person who comes on and off a boat, authorities can ensure that laborers are not sold and rotated to other ships or lost overboard and not reported. Reporting indicates that the government is considering expanding this program to incorporate facial recognition as well.[51] Facial recognition can be particularly useful in those industries where alternative biometrics may be unreliable, such as when dealing with manual laborers with worn fingers or diabetic patients with eye damage.

However, FRT systems can also jeopardize this right to the extent that they are expanded to support broader workplace surveillance practices. Some firms around the world have already been implementing extensive workplace monitoring programs that can penalize workers if they leave their office during assigned work hours, or even if they take three seconds too long to use the restroom.[52] FRT could make it easier for organizations to adopt these invasive practices, especially during an era of increasingly remote work where employers may be tempted to experiment with programs that track whether employees are at their desks or not.[53]

5

Facial Recognition and Human Rights Law

Some rights, such as the right to non-discrimination, cannot be restricted under international human rights law. Other human rights are not absolute and can be restricted if those restrictions meet certain tests. A number of the human rights that FRT is likely to impact, such as privacy, freedom of assembly, freedom of expression, and freedom of movement, can be subject to such restrictions. However, these restrictions are only allowed after a state actor has passed certain tests showing that the restriction is authorized by law, necessary for a legitimate purpose, and proportionate to the aim being sought.

Detailed below are the components of each one of these tests to help inform discussion of whether and how effective and rights-respecting governance regimes for facial recognition—and remote identification in particular—could be constructed. The authors of this report believe that private actors should also be subject to many or all of these guidelines, consistent with their responsibility to respect human rights under the UNGPs.

Lawfulness

To be legitimate, any proposed restrictions of individuals' rights must first be provided by law. The lawfulness test is explicitly outlined by the ICCPR and the UN Human Rights Committee as a condition for justifying restrictions on rights, including privacy, freedom of expression, freedom of movement, and freedom of assembly.[54] The lawfulness test exists to ensure that restrictions that are put in place are not arbitrary but rather conform to a legal regime which is public, capable of being challenged through democratic processes, and specific as to the conditions and safeguards associated with the proposed restrictions. Findings by the UN Human Rights Committee, UN Office of the High

Commissioner for Human Rights (OHCHR), and UN special rapporteurs have helped to clarify what it means for a restriction to be provided by law.

The first requirement is that the legal basis for restrictions must be publicly available. The UN Human Rights Committee has stated that a law "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public."[55] As stated by the UN high commissioner for human rights, "secret rules and secret interpretations of law do not have the necessary qualities of 'law.'"[56] If individuals do not have a way to learn the details of how their rights could be restricted by the government, they are unable to defend their rights or even know if they have been infringed.

The lawfulness test exists to ensure that restrictions that are put in place are not arbitrary but rather conform to a legal regime which is public, capable of being challenged through democratic processes, and specific as to the conditions and safeguards associated with the proposed restrictions.

Laws authorizing the use of facial recognition must also provide clarity and specificity on how the technology will be used. The UN Human Rights Committee has stated that any legislation authorizing surveillance actions that would interfere with individuals' privacy must be "sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, [and] procedures for the use and storage of data collected."[57] Legislation should also create safeguards relating to the construction of watchlists, and ensure that the use of facial recognition takes place under detailed record-keeping requirements.[58] Finally, legislation must give individuals the right to be notified if they have been subject to surveillance, and clarify the remedies available to those who suffer abuse.[59]

Legislation must also clarify the authorities of those entities permitted to deploy the technology in ways that could restrict individuals' rights. According to the UN Human Rights Committee, interference "must be made only by the authority designated under the law, and on a case-by-case basis."[60] Legislation cannot confer unfettered discretion upon these authorities, but must ensure their discretion is "circumscribed with reasonable clarity."[61] Law must also ensure that "robust, independent oversight systems are in place regarding surveillance . . . including by ensuring that the judiciary is involved in the authorization of such measures, in all cases."[62]

Laws could also identify uses of the technology that are strictly off-limits. In particular, limitations on rights cannot infringe on the essence of the right.[63] Determining this is challenging. FRT raises particularly thorny questions of cumulative impact. Multi-actor, long-term, or widescale use of FRT may have such a chilling effect on freedom of expression, assembly, religion, privacy, or movement that it damages the essence of the right, but this would be hard to evaluate on a case-by-case examination of individual deployments and requires legislative attention.

Necessity

Facial recognition deployments must also conform to the principle of necessity, which requires that any deployment that may abridge individuals' rights be justified as not just being desirable, but necessary. To demonstrate necessity, an actor must demonstrate that the proposed action must be the only way or the least intrusive way to achieve the aim being sought. This places a burden on prospective operators of facial recognition systems to demonstrate why this technology, specifically, is required to achieve the goal they have in mind. In verification contexts, this may require operators to demonstrate why other forms of identity verification—including the use of other, less intrusive biometrics, such as fingerprint and iris scans—would not be viable. In identification contexts, operators would have to demonstrate why their work required the ability to identify individuals against a watchlist by their face and what impact it would have on their operations if they were to forego that capability for an alternative method.

Independent, credible studies demonstrating the claimed efficacy and necessity of FRT might enable such a justification but are not typically available. To the extent that they are available, they often show that FRT's success rate is very low, as in the case of the Metropolitan Police of London, where only 19 percent of the matches generated by the system during observed trials were verifiably correct.[64] Necessity justifications should not only provide evidence that the system is accurate enough to reliably provide insights that would be impossible through alternative methods but also justify the system in the context of known error rates and impacts, resource and personnel costs, and the possible indirect costs to department operations, such as damage to community trust.

To demonstrate necessity, an actor must demonstrate that the proposed action must be the only way or the least intrusive way to achieve the aim being sought.

Moreover, when restricting such rights as freedom of expression or assembly, the UN Human Rights Committee has found that necessity must be demonstrated in a specific and individualized fashion.[65] UN Special Rapporteur David Kaye found that the same requirement ought to apply in the same way to restrictions on individuals' right to privacy, indicating a growing consensus that some forms of facial recognition deployments must be justified on an individual use basis in order to comply with human rights obligations.[66]

Legitimacy

The second component of the necessity test is that any use that would restrict an individual's rights must be undertaken in the service of a legitimate aim. Restrictions for some rights are only allowed in the case of a limited set of purposes. For example, the ICCPR specifies that freedom of expression may only be restricted when necessary "for respect of the rights or reputations of others, or for the protection of national security or of public order (ordre public), or of public health or morals."[67] UN Special Rapporteur Frank La Rue argued in 2013 that the right to privacy should be limited in the

same way.[68] Under such a framework, necessity must be demonstrated in the context of one of these specific purposes in order to be compliant with human rights. Many FRT deployments will likely take place under the justification of national security and public order, so it is important that this test not be treated as sufficient to justify a deployment in the absence of satisfying the other conditions.

Proportionality

Operators must also demonstrate that potential deployments are proportionate in scope and effect. Proportionality overlaps with necessity in demanding that the proposed intervention be the "the least intrusive instrument amongst those which might achieve their protective function."[69] Proportional measures are also those which are "reasonable in the particular circumstances" and "proportionate to the interest to be protected."[70] This requires an evaluation of not only the degree to which a particular deployment might abridge individuals' rights but also the significance of the interest being protected.

Proportionality is difficult to assess in the case of FRT, given the number of factors involved, but it is possible to begin constructing a set of questions that can guide analysis. The first is the geographic and temporal scope of the deployment, which affects the number of individuals impacted. This is particularly important in the case of live facial recognition monitoring, which can range from temporary, event-specific uses in limited and well-defined locations to the passive, indefinite monitoring of open public spaces. Deployments are more likely to be disproportionate if they are not tailored as narrowly as possible to affect only those who are reasonably likely to be involved in potentially dangerous or criminal activity.

The proportionality of both live and retroactive identification can also be assessed according to the enrollment policies used to create matching databases. Monitoring a sports arena or airport using a watchlist of known terror suspects is a more narrowly tailored—and thus proportionate—deployment than using the same system to monitor for criminal suspects of any kind. And both would be more proportionate than a system set up to identify and log the movements of any member of the public who passed beneath the camera by comparing them to a national ID registry.

Such an assessment should also consider alternative approaches to achieving the same goal and demonstrate in a fact-based manner that FRT is or is not necessary and the least restrictive option available to the operator. The reasonableness of a deployment also depends on whether the subjects are aware that their data is being collected and retained. If individuals are unaware of when and how their data is being processed, they are more likely to feel that their private lives are subject to constant surveillance, exacerbating chilling effects on freedom of expression and assembly.[71] If covert monitoring is not strictly required for the purpose of the deployment, failing to provide notice would likely lead to a disproportionate restriction of their rights and freedoms.

A deployment may also be disproportionate if it fails to provide adequate safeguards regulating under what circumstances and by whom the collected data may be accessed. An otherwise proportionate deployment that allows collected information to be shared with or accessed by entities with no clear purpose for using the data would create a disproportionate threat to subjects' rights.

Obligations of Private Actors

According to the UNGPs, companies have a responsibility to respect internationally recognized human rights. They do so by exercising human rights due diligence—having in place effective policies and procedures to identify and address potential and actual human rights impacts throughout their value chain and within their operations. Due diligence steps include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed.[72]

How companies are expected to respond to impacts will vary depending on their relationship to the impact. If they cause an impact, they are expected to cease or prevent it. If they contribute to an impact, they should cease or prevent their contribution and use their leverage to mitigate its effects to the greatest extent possible. Businesses should also seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products, or services by their business relationships, even if they have not contributed to those impacts. They should use their leverage with their business partners to accomplish this. If they lack the leverage to prevent or mitigate adverse impacts and cannot increase their leverage, they should consider ending the relationship.

The corporate responsibility to respect human rights is independent of whether governments are enforcing human rights-compliant laws and may in some cases require companies to adhere to higher standards than those set by national law. Given that national laws governing facial recognition directly or indirectly are often non-existent or nascent, this responsibility is particularly important.

The relationship between the corporate responsibility to respect human rights and the existing human rights obligations of governments is closely interwoven. The UNGPs reiterate long-standing international law, noting that governments have a duty to protect human rights from adverse impacts by third parties such as companies. This means they should have in place laws, regulations, enforcement, and remedy mechanisms dealing with those private sector actors which operate FRT systems.

6

Recommendations for Operators

To date, the authors of this report found that the guidelines for restricting certain rights through the use of FRT are rarely, if ever, met. Below, the study team suggests a set of expectations that, if fully implemented, could increase the probability that FRT could be deployed in a manner consistent with international human rights law. Notably, it is possible that there are uses of FRT that are fundamentally incompatible with human rights, regardless of the safeguards put in place.

It is this latter concern, combined with a lack of governance for FRT, that has helped prompt bans and discussions of moratoriums on multiple continents.[73] More robust discussions are urgently needed about whether there are use cases that are fundamentally incompatible with human rights, as well as how operators and policymakers can craft an appropriate and tailored governance framework that takes into account the full spectrum of potential impacts.

Identifying and Responding to Human Rights Impacts and Risks

1. **Conduct a human rights impact assessment (HRIA) prior to deploying a facial recognition system.**

   Prior to deploying new facial recognition systems, or before expanding the technology's use to new geographies or new purposes, operators should assess the potential human rights impacts, for example, by conducting an HRIA that evaluates the impacts of the deployment on the full range of human rights. Assessments should focus on identifying who will be impacted by the technology, what the actual and potential impacts could be in both the near and long term, and what mechanisms exist to allow the organization to create safeguards. Impact assessments should clarify the intended purpose and scope of the deployment and lay out policies and procedures

that will be put into place to guide operation and risk management. The assessment should also consider risks from data sharing with other entities.

Assessments should also include the lawfulness, necessity, and proportionality of the proposed use. This should include considering whether there are other approaches—including both alternate biometrics and non-biometric solutions—that would accomplish the same end without adverse impacts on human rights.

The assessment process should include technical, legal, and human rights experts from within the organization, as well as outside stakeholder groups and representatives from the communities who may be impacted by the product. Because some organizations deploying FRT may have little expertise in the technology, they may need to draw extensively on third-party expertise. Deployments in public areas should also require public consultations to be held so that operators can account for the concerns of the local population.

Private operators should use the HRIA to educate themselves about the circumstances and procedures by which government may demand access to information collected through facial recognition systems and consider the human rights implications of those requests. Operators should be prepared to challenge any illegal requests for information.

Law enforcement and other government operators should use the HRIA to clarify the legal authorities granted to them under the country's laws, as well as the obligations and limitations those laws place upon use. If there are no public laws that provide clear and specific guidance on how the technology can and cannot be used, it is unlikely the deployment could be justified under international human rights law.

Assessments should be made publicly available after completion to promote transparency and public trust.

2. **Institute structures and processes for identifying and escalating potential human rights concerns raised by the operation of facial recognition systems and ensuring that findings are acted on and integrated into decisionmaking.**

   Facial recognition operators should institute internal mechanisms for reviewing the operation and impact of facial recognition systems. These procedures should be informed by the findings of HRIAs and be established with the goal of ensuring that the assessment of rights impacts is an ongoing process that is tightly integrated into decisionmaking. Internal structures should encourage and reward staff for voicing concerns that come up during their work and allow those concerns to be escalated as necessary to a specialized body with the authority to set organizational policy for how to deal with potential rights issues. These processes should involve representatives from multiple teams from across the organization, including leadership. To the extent necessary, the organization should consult with external experts to inform their decisionmaking. An example of an organization that has established a successful model for regular external consultation is the West Midlands Police, described in greater detail.

Case Study: West Midlands Police Ethics Committee

Serving the cities of Birmingham, Coventry, Wolverhampton, and surrounding areas, the West Midlands Police is one of the largest police forces in the United Kingdom. In 2019, the department established an independent ethics committee to give advice on proposals for new data science tools and projects being considered by the force.[74] The committee members work with the police department throughout the lifetime of a project to provide ongoing feedback and help the police address any concerns that emerge.

he members of the committee are independently selected by elected officials with policing input and represent a broad range of disciplines, from human rights and sociology to data analytics and data governance. All reports and meeting minutes produced by the committee are made publicly available to help promote transparency. Though police chiefs have the power to disregard the members' recommendations, the committee's ability to publicly raise concerns about projects gives them substantial political power since police chiefs are accountable to their civilian commissioners.

So far, the projects that the group has reviewed have been focused primarily on improving case management, identifying crime hot spots, and estimating criminal risk ratings. However, according to interviews, the force also held off on rolling out a proposed system for retroactively identifying faces in captured footage so that the ethics committee could be consulted first. This may be one of the most important effects of the committee: to simply slow down the process of rolling out potentially risky technologies so that more time and thought can be given to when and how it should be deployed.

3. **Perform rigorous testing on facial recognition systems prior to deployment to determine their accuracy and ensure they are free from demographic biases.**

   Operators should have a process in place to evaluate potential models for their accuracy and bias prior to deployment. Organizations should prioritize sourcing facial recognition systems from developers that provide clear documentation as to the capabilities and limitations of the technology; can assure that the model has been trained on diverse data sets that include members of the groups likely to encounter the system during deployment; and has been independently assessed for accuracy and bias by third-party researchers or in standardized assessments, such as the NIST Facial Recognition Vendor Test (FRVT).

   After a facial recognition system has been procured, operators should design and implement a testing regime to measure its real-world performance and impacts before it is officially deployed. This can include scenario testing utilizing volunteers or closely monitored operational testing in a strictly controlled setting. These tests should aim to measure the true performance of the system in a real-world environment, including the true error rates of the system and its human operators as well as the operational value of the system in achieving the goals of deployment.

4. **Institute policies to ensure accountability for compliance with these recommendations.**

   Operators should institute internal policies and procedures that help give effect to these principles. This should include instituting audit trails for the collection, use, and sharing of facial recognition data, designating specific individuals or offices with responsibility for compliance, and assessing third-party processors who support the organization's operations.

Government operators should treat statutory requirements as a minimum baseline and seek to go beyond these obligations in the way they track their efforts to reduce impacts and report compliance. Private operators should submit to regular independent reviews of their policies and procedures to provide assurance of their commitment to complying with human rights obligations.

5. **Provide individuals with the opportunity to seek remedy for rights violations.**

   So that grievances can be addressed early and remediated directly, operators should put into place easily accessible mechanisms for individuals to report known or suspected violations of their rights due to the use of facial recognition.[75] This presupposes that individuals were notified that FRT was used in the first place. Where operators identify that they have caused or contributed to adverse impacts, they should provide for remediation through appropriate processes. These can include judicial or operational mechanisms as appropriate, as long as these are legitimate, accessible, predictable, equitable, transparent, and rights-compatible.

Transparency

1. **Release a policy statement outlining the operator's human rights commitments.**

   The statement of commitment should clearly set out the organization's expectations for its personnel, partners, suppliers, and other linked parties. These expectations and commitments should be informed through consultation with relevant internal or external expertise and should be approved at the most senior level of the organization. The policy statement should be made public and circulated both internally to personnel in the organization and externally to partners and other relevant parties. Organizational policies and procedures should be in coherence with the plan to provide accountability and incentives for aligning business activities with the stated commitments. The precise issues that such a policy should contain will depend on the nature of the deployment and of the operator. Such policies could include:

   - Deploying internal processes and management structures to assess human rights risk on an ongoing basis and escalate concerns as needed;
   - Supporting transparency and engagement, such as by including external advisers on FRT decisions and public reporting on customers, deployment, and efforts to avoid non-discrimination;
   - Requiring notification and consent and enabling remedy, as applicable; and
   - Limiting the sharing of information with other public or private sector actors and giving clarity about when and how data sharing arrangements may be undertaken. This is particularly important in the case of data sharing with law enforcement authorities, where private operators should seek to clarify the level of authorization agencies must provide before honoring any requests for data and outline their procedures for notifying affected subjects.

   Organizations should undertake regular, independent audits to assess their adherence to these policies and practices. The results of these audits should be made publicly available to improve public trust and ensure that any issues that emerge are addressed in a timely manner.

2. **Provide clear notice when FRT is in use.**

   Operators using passive FRT in public areas should post clear signage to inform individuals that facial recognition is in operation before they enter into the field of view for the system and provide a mechanism for individuals to opt-out of the system easily and on the spot if consent is being relied on as the legal basis for processing. The notice should provide basic details about the scope and purpose of operation, who data may be shared with, and where further details and the privacy policy of the operator can be found.

   Notice requirements should apply not only to private operators but also to government and law enforcement agencies. While some law enforcement agencies may argue that these requirements may undermine public security programs, the authors argue that it would be extremely difficult to justify covert passive FRT surveillance as necessary and proportional except in very limited, exceptional circumstances.

3. **Be open and transparent about organizational policies and practices relating to how data is collected, used, and shared.**

   Operators should post a privacy policy online that details the scope and purpose of their deployment; the legal basis they rely on to justify data collection; the company's practices regarding the collection, storage, and use of face templates; with whom data may be shared; retention and deletion policies; the rights of data subjects to access and request erasure of their information; and the safeguards the operator has put in place to prevent abuse or misuse. They should identify the training data sets and algorithms used in the product and demonstrate that testing occurred to identify and address any bias in how the system operates in practice.

   If the basis for collection is subject consent, organizations should make publicly available their policies around how and when they obtain consent from subjects, how they ensure that consent is informed and freely given, and what mechanisms they have in place to allow subjects to withdraw consent easily. Firms should conduct regular, independent audits to assess whether the company's practices align with these policies and make the results of these audits publicly available.

4. **Communicate how impacts are addressed.**

   Operators should identify how they are managing potential and actual human rights impacts through public reporting. The reporting should focus on the risks and impacts that are most relevant for that particular actor. This can help alleviate concern that the technology is being used in unknown ways and provide greater confidence that issues such as bias have been addressed. For private actors, increased transparency on outcomes and use cases would help firms in this sector come out of the shadows and differentiate themselves from less responsible competitors.[76]

5. **Provide individuals with the opportunity to request access to data about them that was collected using facial recognition and to request correction or erasure as appropriate.**

   Operators should put into place easily accessible mechanisms for individuals to discover what, if any, information has been collected about them during the operation of facial recognition systems. They should be able to obtain copies of the data in an accessible format, for a reasonable cost, and within a reasonable period of time. Individuals should be given

the opportunity to request the correction of erroneous or incomplete information held by operators, as well as the erasure of their data.

6. **Institute record-keeping procedures and release regular transparency reports detailing how FRT has been used.**

   Organizations should keep records of the operation of their FRT systems and release transparency reports to publicly share these details.

   Law enforcement operators should keep track of the number of times FRT systems are used during investigations. Agencies should also track the number of successful and false arrests resulting from FRT-generated leads, the number of times investigators successfully and unsuccessfully sought judicial authorization for FRT use, the number of complaints the department receives, the agents who accessed the FRT system, and how many times FRT was used to investigate different categories of crime. This information, as well as broader details about the size and scope of FRT infrastructure, should be released publicly as part of regular transparency reports to help improve accountability and public trust.

   Private operators should similarly track the way their organization uses FRT and record the number of instances where technical or operator failure led to harms or negative rights impacts. To the extent they are legally able, private operators should commit to notifying individuals if any biometric data or other information collected through FRT programs is sought by law enforcement. They should also publish the number of government requests they receive annually.

Operational Rules

1. **Limit the collection and use of biometric data to what is necessary to achieve narrowly defined and rights-respecting purposes, and do not share or reuse data in ways incompatible with that original purpose.**

   The purpose of biometric data processing must be clearly defined prior to deployment. Information collected by facial recognition systems should not be used or shared for reasons incompatible with this original purpose. Compatibility should be judged by considering what the subject would reasonably expect given the original context of collection, the linkage between the original purpose and the new proposed purpose, and the possible risks of further processing.

   Some types of data processing will always be incompatible with human rights obligations, no matter the subject's expectations or consent. These situations occur when the essence of a subject's human rights may be violated. Examples include the characterization of individuals' ethnicity for the purpose of discrimination, unconstrained and indiscriminate mass surveillance, and the use of facial recognition to target and restrict the rights of certain individuals without due process.

2. **Practice principles of privacy and data protection by design and default.**

   Operators should ensure their facial recognition systems are designed, configured, and used in ways that preserve privacy and data protection by default. Operators should ensure during

the procurement process that their chosen facial recognition system is architected in such a way as to enforce privacy and data protection throughout the full life cycle of the data being collected. The systems should be designed to support rather than complicate organizational goals of transparency, data integrity, collection minimization, accountability, and remedy.

Examples of relevant practices could include ensuring that data is encrypted and stored securely, that the system is set to delete any information collected from individuals who are not matched by the system, and that only face templates rather than raw images are stored. Firms should implement organizational practices to ensure privacy by design is followed and enforced, such as conducting regular internal reviews, assigning dedicated personnel to oversee privacy issues, and training employees on privacy.

3. **Ensure staff are trained as to the capabilities, limitations, and proper use of the facial recognition system.**

   Prior to deployment, facial recognition operators should require their employees to undergo training on the capabilities and limitations of facial recognition systems and proper procedures to help ensure responsible use. At a minimum, this training should include information on how to adjudicate matches returned by the system, how to adjust confidence intervals for different use cases, what the sources and rates of error are during real-world deployments, and how to ensure that data collection is secure and reduced to the minimum necessary for operation. Staff should also be trained on appropriate processes for data sharing with other companies and government agencies.

4. **Institute policies and practices that ensure for meaningful human oversight or review over any decisions made by facial recognition systems.**

   Operators should ensure that the decisions made by facial recognition systems are subject to review or oversight by individuals with the authority to alter those decisions. Organizations should ensure that facial recognition systems are only used to assist human decisionmaking rather than replace it. If an operator does decide to implement automated facial recognition decision systems without a human in the loop, it should ensure that any individuals subject to those decisions know it was the result of FRT and have the opportunity to promptly request review by a human.

5. **Implement security measures to protect the data contained in enrollment databases, and retain face templates for no longer than necessary.**

   Operators should institute policies to protect enrollment data from unauthorized access, including encryption, access controls, employee training, antivirus software, and other standard security practices. Firms should also institute retention limits for the data they collect. Template data should be kept for no longer than is necessary to achieve the purpose for which it was collected. At the end of the allotted period, biometric data should be deleted or de-identified as appropriate, noting that de-identified data can still be de-anonymized under certain circumstances.[77] Organizations should institute a regular review process to ensure that these retention limits are enforced.

6. **Whenever possible, obtain free and informed consent before enrolling individuals in a program that uses facial recognition.**

When possible, operators should strive to obtain explicit consent from each individual before capturing their biometrics and enrolling them in an FRT system. Consent should also be required before an operator shares any biometric information outside of the organization or uses it for additional purposes. Subjects should have the ability to withdraw their consent at any time, and operators should establish clear and simple processes for this. For consent to be freely given, there must not be a clear imbalance of power between the subject and the operator, and there must be a reasonable way to access the service without using FRT. For consent to be informed, subjects must be informed in plain language of the identity of the operator, the potential uses of their data, any possible sharing of it, how it is stored and for how long, and other facts that can help them evaluate the risks of enrolling in the system.

In circumstances where biographic information is not linked to face enrollment data, such as in the case of unique persistent identifiers used for in-store tracking, many operators prefer to rely on op-out consent. The validity of this process should depend on whether subjects are presented with clear notice that facial recognition is taking place and easy opportunities to withdraw their consent for processing. Ideally, the opt-out process should be as simple as scanning a QR code that would allow the subject to quickly add a de-identified face template to the store's do-not-track list, though additional options for those without mobile devices should also be made available. Signs listing merely a mailing address, phone number, or invitation to fill out multi-step forms buried on a company website should not be considered to meet this standard.

7. **When not based on explicit consent, FRT deployments must include heightened protections, including strict limits on enrollment and data reuse.**

   In some situations, such as law enforcement or private security deployments, it may be impossible to obtain consent from every subject. Such deployments raise serious rights concerns and should not proceed unless operators are able to demonstrate their lawfulness, necessity, and proportionality to a high standard. Meeting these standards would, at a minimum, require procedural safeguards to ensure accountability and enforce strict limits on who may be enrolled to ensure that the number of individuals impacted is limited to the minimum necessary.

   The composition of these watchlists should always be limited to the minimum necessary sample to achieve the purpose of the system. This includes limiting enrollment to subjects who have a proven and specific relationship to the operator and where the purpose of enrollment is not hypothetical but has been clearly demonstrated. For example, enrolling all individuals with a criminal background into an event security deployment would be clearly disproportionate and unacceptable. In the case of retroactive identification used by law enforcement to analyze crime footage, match lists could be limited to only those who had previously been arrested or only those who had been convicted of a criminal offense. Enrollment data should be retained for no longer than strictly necessary and should never be used or shared for reasons outside the original narrow purposes for which the gallery was created.

7

Recommendations for Policymakers

The vast majority of facial recognition deployments around the world are occurring under ambiguous legal regimes. Few countries have passed legislation explicitly authorizing the use of facial recognition or outlining the conditions under which it should be used and supervised. If a legal basis for deployment is cited at all, it usually involves government agencies referencing broad legislation authorizing general investigative powers that do not provide specific safeguards for facial recognition use. This creates large risks of mission creep, where deployments intended for one purpose are continuously expanded to serve other goals without any formal oversight. This type of legal environment is contrary to the requirement under human rights law that interference in individuals' rights—if they are subject to restriction at all—only take place in cases envisaged by the law and where the precise circumstances in which that interference takes place are explicitly stated and assessed by independent authorities.

In most countries, the current focus of privacy-related policymaking is on passing comprehensive data protection laws. Few countries are looking toward legislation specific to facial recognition. Broad data protection legislation, while important, is inadequate to address the unique risks posed by facial recognition. Nations must work toward passing legislation that specifically governs the permissible deployments of FRT. Such laws should identify when deployment is permissible for government agencies as well as the private sector, and when particular uses may be fundamentally incompatible with human rights. They should also set out the types of procedural requirements, oversight, and public transparency measures outlined below. If the following guidelines were adopted, they would increase the probability that FRT could be deployed by in a manner consistent with international human rights law.

Creating a Legal and Regulatory Regime that Protects Fundamental Rights and Freedoms

1. **Clarify impermissible uses of FRT for both public and private sector actors.**

   Policymakers should consider whether there are uses of FRT that simply cannot be made compatible with international human rights law (or relevant constitutional law), potentially because they infringe on the essence of the right. These restrictions should be clearly articulated in any piece of legislation. For example, the EU Agency for Fundamental Rights indicated that it was hard to imagine when the use of FRT during protests could be made consistent with EU human rights law.[78] European Digital Rights (EDRi)—an association of 44 civil society organizations—has called for a ban on "biometric processing that could amount to mass surveillance in public spaces."[79] The state of Washington in the United States recently passed a law that prevented public agencies from using FRT to "create a record describing any individual's exercise of rights guaranteed by the First Amendment of the United States Constitution," including freedom of speech, freedom of assembly, and freedom of religion.[80] The use of FRT on children could be another area that is made subject to automatic limitations.

2. **Set out the legal basis under which different forms and uses of FRT can proceed.**

   Policymakers should clearly set out the conditions under which FRT deployments may be considered legitimate.

   One possible legal basis is consent. Governments should specify the standards of consent that private sector and non-law enforcement government operators should seek to obtain before enrolling individuals in FRT systems. Governments should clarify when, if ever, opt-out consent is acceptable, as opposed to explicit opt-in consent, and specify that any consent must be informed and freely given. For consent to be freely given, there must not be a clear imbalance of power between the subject and the operator, and there must be a reasonable way to access the service without using FRT. For consent to be informed, subjects must be informed in plain language of the identity of the operator, the potential uses of their data, any possible sharing of it, how it is stored and for how long, and other facts that can help them evaluate the risks of enrolling in the system. Lawmakers should also specify that individuals have the right to withdraw their consent at any point and that operators should establish clear and simple processes for this.

   Other legal bases may exist that are not based on the consent of the subject, but policymakers should be aware that under human rights law, many fundamental rights and freedoms may only be restricted in the service of certain narrow purposes, including national security, public order, public health or morals, or in order to safeguard others' rights and freedoms. Law should set out when these purposes may allow operators to use FRT without subjects' consent and ensure that these rules are specific as to the conditions and safeguards associated with these uses.

3. **Encourage the adoption of common standards of accuracy and non-discrimination.**

   Ideally, governments would be able to require that facial recognition software meet certain standards of accuracy and non-discrimination and be certified to them before deployment. In reality, it is difficult to settle on common standards of performance given the wide diversity of

contexts FRT can be used for, the multiple different metrics FRT performance can be measured along, and the challenge of predicting real-world performance based on data gathered in a controlled laboratory setting. However, recent work by academic, corporate, and government researchers can help to move the FRT industry toward common standards of testing and reporting and hopefully lead to common benchmarks for performance.

Relevant government bodies should remain engaged with this work with an eye toward eventually devising—in collaboration with technologists—appropriate performance thresholds for FRT systems, beginning with high-risk uses such as law enforcement deployments. Governments will then need to identify bodies that are trusted to evaluate systems according to these standards. Eventually, governments may be able to require government agencies to use certified systems, helping assure industry that there will be a reliable market for certified software. These standards can then serve as a quality signal for private sector operators, further incentivizing FRT developers to ensure their products and services meet these benchmarks.

Even in the absence of formal certification schemes, governments should, at a minimum, require that any agency using FRT collects and publicly reports details about the algorithm's performance (including any demographic effects) and the provenance of training data involved in the systems they use. They can also require developers to make their algorithms available for third-party testing. This will limit government agencies to sourcing from developers that practice transparency in their development process, helping to push the industry toward common standards of testing and reporting.

4. **Ensure remedy is available to individuals impacted by FRT deployments.**

   For remedy to be feasible in the FRT context, law must ensure that individuals have the ability to learn whether they are included in any matching database used in a facial recognition system and to request removal if appropriate. Individuals must also have the right to know whether or not FRT was used to identify them and the right to be made aware of and request correction or erasure of any records that result. During trial, criminal defendants should have the right to be made aware of whether facial recognition was used against them over the course of law enforcement's investigation.

   Individuals who believe that the use of FRT has infringed on their rights should have access to judicial remedies. However, agencies should also consider establishing ombudsmen who can respond to concerns about the use of FRT and potentially provide additional and more timely remedy compared to the judicial system. Private operators should endeavor to establish operational mechanisms to provide remedy outside of established judicial proceedings and ensure that these processes are legitimate, accessible, predictable, equitable, transparent, and rights-compatible.

5. **Establish strong privacy and data protection regulations to set limits on the collection and use of data.**

   While general privacy and data protection laws cannot replace the need for FRT-specific legislation, they have an important role to play in complementing FRT laws by setting baseline norms around how data can be collected, used, and shared. In particular, these laws should:

- Institute requirements for physical, technical, and organizational security measures to protect data;
- Set limits on data retention to ensure data is not kept for longer than necessary;
- Require operators to limit data collection to the minimum necessary to achieve their purpose;
- Restrict the reuse and sharing of data for purposes incompatible with the original context of collection;
- Obligate operators to ensure the data they hold is accurate, complete, and up-to-date;
- Require operators to adhere to principles of privacy and data protection by design and default; and
- Provide individuals with the rights to access, correct, and, when appropriate, erase data about them.

6. **Create a framework for private sector actors to follow in conducting human rights due diligence.**

   Governments can lay out broad frameworks that companies should follow regarding human rights due diligence processes. This process should include conducting human rights impact assessments prior to the deployment of new and potentially risky technologies, assessing suppliers to ensure that the quality of the technology being used will not lead to additional risks, and ensuring ongoing review of company practices and policies. Government guidance could help engage new sectors deploying the technology and also prompt more responsible behavior by smaller actors that may not be part of ongoing discussions on FRT and human rights/ethics.

7. **Build an enforcement capacity to ensure that operators are complying with their obligations under national or human rights law and create penalties for organizations that violate individuals' rights.**

   Government should establish penalties for human rights abuses arising from FRT. Enforcement will likely be multifaceted. Individuals and groups should be able to bring cases when their rights are impacted by FRT. Given the potentially large groups affected by issues such as bias, class actions must be permitted. However, as individuals may not always know when their rights have been violated, regulators and oversight bodies should also be proactive in identifying instances where companies or government agencies are operating in illegal ways.

   Regulators with adequate technical backgrounds should be tasked with proactively and independently carrying out risk-based audits of companies in the FRT value chain, focusing particularly on issues of non-discrimination and adherence to requirements regarding privacy, data-sharing, and notice and consent.

Regulating Government Facial Recognition Operators

1. **Require public sector agencies to carry out human rights impact assessments (HRIAs) prior to the use of FRT.**

   Law should set out the steps that public agencies should have to go through prior to deploying an FRT system. Lawmakers should clarify that FRT systems can only be legally deployed once this process has been completed.

Part of the authorization process should involve conducting an assessment to identify the potential risks of the deployment on the full range of human rights. This assessment should clarify the intended purpose and scope of the deployment, identify who will be impacted by the technology, and lay out policies and procedures that will be put into place to guide operation and risk management. Lawmakers can require operators to collect detailed technical information from algorithm suppliers as part of this process, helping promote transparency and ensuring that operators take these details into account when making procurement decisions.

Assessments should also evaluate the lawfulness, necessity, and proportionality of the use. This should include considering whether there are other approaches that would accomplish the same end without adverse impacts on human rights. The assessment process should include technical, legal, and human rights experts from within the organization, as well as outside stakeholder groups and representatives from the communities who may be impacted by the product.

2. **Create mechanisms for independent oversight over the deployment and use of FRT by government operators.**

   Lawmakers should establish structures to ensure that independent oversight is exercised at each stage of an FRT system's life cycle, including in determining whether a proposed deployment should be considered lawful and in auditing departmental practice to ensure compliance with operational rules. This oversight should include a range of expertise, including not only technical experts but also human rights and constitutional law experts.

   Lawmakers should establish independent bodies and require certain types of FRT deployments—such as those proposed by law enforcement agencies—to go through a review process prior to being authorized. Potential operators can be required to submit technical information to these bodies and provide details about the policies and procedures they have developed to govern its operation. These bodies can also be granted a role in providing ongoing review of deployments to ensure that operators are accounting for new and emerging risks and are not failing to apply proper procedures or allowing mission creep to take place.

   Policymakers should work to ensure that these arrangements are sustainable. This will require dedicated sources of funding to ensure that staff can be retained and experts compensated for their participation. If bodies are established at a local rather than national level, there should be mechanisms for taking the insights and lessons learned from individual bodies and institutionalizing them as part of broader rules and procedures.

3. **Ensure that the use of FRT by law enforcement is subject to oversight by an independent judiciary.**

   Governments should set out when particular applications of FRT must be approved by an independent judicial authority prior to deployment. This should include, at a minimum, any attempt to use FRT for real-time monitoring of particular suspects. However, some governments may also wish to make independent judicial authorization a requirement in the case of retroactive identification as well.

Case Study: Oakland Privacy Advisory Commission

In 2016, the city of Oakland, California established a Privacy Advisory Commission (PAC) to provide advice and technical assistance to the city on how to protect privacy rights in connection to the use of surveillance technologies such as facial recognition.[81] The PAC is made up of nine members, including at least one attorney or activist with expertise in privacy and civil rights, one past or present member of law enforcement, one auditor or CPA, one hardware or software professional, and one expert in government openness and transparency. The commissioners are appointed on a volunteer basis and have no staff, which limits their capacity, but they have been granted a statutory role in overseeing the way the city deploys any surveillance technology.

In 2018, Oakland's city council passed an ordinance—developed by the PAC—that sets out the steps the city must take before it can acquire or deploy any surveillance technologies.[82] This includes notifying the PAC prior to soliciting funds or proposals, submitting a use policy and impact report to the commission before seeking approval for new or existing technologies, and providing an annual report on how surveillance technology is being used by the city. As part of this process, the PAC holds public hearings to receive information about the proposals and solicit public feedback.

Currently, the PAC's role is only advisory, with the ultimate power about whether and how to support the acquisition and use of surveillance technology falling to the city council itself. Nevertheless, interviews indicate that this process has served as an invaluable opportunity to gain public clarification from city employees as to what technology they are purchasing, how it is being deployed, and what policies are being put into place to govern its use. When the PAC finds that city impact reports or use policies do not adequately take into account the potential risks, the consultation process allows these issues to be addressed through engagement with outside experts. For example, one of the most frequent issues the PAC has encountered has been the question of data sharing and reuse, where the commission has been able to push city officials to take a more future-oriented approach to their policies and protections. The requirement for annual reports also helps ensure that there is ongoing oversight into how these technologies are being used, which helps protect against the risks of mission creep.

While not every city may have the resources or capacity to implement this kind of oversight model, its use by larger trend-setting jurisdictions may help catalyze the development of smarter policies and procedures that can help inform the approach of others.

4. **Clarify how evidence derived from FRT may be used in court.**

   Lawmakers should clearly establish that matches made by FRT systems should not be considered evidence of guilt. When FRT is used as a way to generate investigative leads, law should clearly set out when those matches can and cannot be used to justify additional investigative measures, including other forms of surveillance. During trial, criminal defendants should have the right to be made aware of whether facial recognition was used against them over the course of law enforcement's investigation.

5. **Require agencies to conduct scenario or operational tests prior to deployment to gather data about the real-world performance of FRT systems and identify possible risks.**

   Prior to deploying FRT, public agencies should be required to design and execute a rigorous series of evaluations to gather data about how the proposed system would perform in the real

world. This may include scenario testing utilizing volunteers or closely monitored operational testing in a strictly controlled setting. These tests should aim to measure the true performance of the system in a real-world environment, including evidence of the true error rates of the system and its human operators and the operational value of the system in achieving the intended goals of deployment. Agencies should be required to set out performance targets prior to testing and refrain from deploying systems that are not able to meet them.

6. **Require government operators to adhere to the operational rules and principles listed in the previous section.**

   These mandates should include requirements to:

   - Limit the collection and use of biometric data to the minimum necessary for narrow and legitimate purposes;
   - Practice principles of privacy and data protection by design and default during operation;
   - Ensure staff are properly trained in the proper use of FRT systems;
   - Ensure for meaningful human review over decisions made by facial recognition decision systems;
   - Implement security measures to protect sensitive data; and
   - Practice minimization in enrollment policies.

7. **Require public agencies to publicly release information about their policies and procedures regarding FRT and to publish regular transparency reports detailing how their systems have been used.**

   Policymakers should require that law enforcement operators keep track of the number of times FRT systems are used during investigations. Agencies should also track the number of successful and false arrests resulting from FRT-generated leads, the number of times investigators successfully and unsuccessfully sought judicial authorization for FRT use, the number of complaints the department receives, and how many times FRT was used to investigate different categories of crime. This information, as well as broader details about the size and scope of FRT infrastructure, should be released publicly as part of regular transparency reports to help improve accountability and public trust. Law enforcement agencies should also be required to report the number of instances where they requested FRT data from private operators, the circumstances surrounding those requests, and the investigative outcomes.

   Border control agencies and other government actors should also be required to regularly disclose information about how they are using FRT, including the number of times the technology is used annually for different purposes, the number of complaints received, the number and outcome of any instances of rights violations, and details about how data was shared with other agencies or other countries.

8. **Place clear restrictions on the sharing of data between government agencies and between government and the private sector.**

   This should include forbidding government agencies to obtain FRT-related data from the private sector that the government would not be permitted to gather itself without due process. All government agencies should be required to have clear rules regarding data sharing that are

consistent with the law. In general, data sharing should be limited to what is strictly necessary to fulfill the purpose of the deployment and authorized by a third party such as a court.

9. **Provide resources to support technical capacity building for government agencies.**

   Small government agencies often lack the technical capacity to be able to assess potential suppliers of FRT technology to determine their accuracy or the risks that a system may have discriminatory effects. National governments should work to ensure that all agencies considering FRT have access to the expertise and resources necessary to be able to undertake a rigorous evaluation of the technology's capabilities, limitations, and risks.

About the Authors

Amy K. Lehr is a senior associate with the Human Rights Initiative at the Center for Strategic and International Studies (CSIS). She is the former director of the CSIS Human Rights Initiative and was a senior fellow with the program. In that role, her work focused on human rights as a core element of U.S. leadership, labor rights, emerging technologies, and the nexus of human rights and conflict. Amy previously served as legal adviser to the UN special representative on business and human rights and helped develop the UN Guiding Principles on Business and Human Rights. She was a fellow at the Harvard Kennedy School's Corporate Responsibility Initiative. Amy formed part of a business and human rights legal practice, engaging with businesses, investors, multilateral organizations, civil society, and governments to address global human rights challenges. She previously worked for development nongovernmental organizations in Myanmar and Thailand. She was a Council on Foreign Relations term member. Amy received her AB from Princeton and her JD from Harvard Law School.

William Crumpler is a researcher with the Strategic Technologies Program at CSIS, where his work focuses on cybersecurity policy and the governance of artificial intelligence and other emerging technologies. He holds a BS in materials science and engineering from North Carolina State University.

Appendix A

Project Methodology

Below, we have provided a brief outline of our research methodology for this project. It is our hope that other organizations may be able to use this approach to aid in the investigation of how other technologies impact human rights.

Understanding the Technology

1. **Conduct desk research into how the technology works and its strengths and limitations.**
    a. To better understand how the technology in question works, we conducted a literature review of explanatory documents and presentations released by developers, industry associations, academic researchers, and relevant NGOs with significant in-house technical expertise. This review focused on the technical principles underlying the technology, the role of machine learning in training facial recognition systems, and how data is generated and shared during and after operation.
    b. To better understand the strengths and limitations of the technology, we conducted a literature review of media reports covering the findings of tests performed by academic researchers, reports on the topic by relevant NGOs with significant in-house technical expertise, and the findings of third-party testing and evaluation bodies. This review focused on the accuracy of systems measured in both laboratory and real-world settings, the way accuracy varies across demographic groups, the advantages and disadvantages of facial recognition relative to other biometrics, and the current trends in performance.

2. **Reach out to individuals involved in the research, development, testing, and deployment of the technology, and request interviews to gather additional information.**
    a. We spoke with facial recognition developers, independent researchers, and operators to confirm and deepen our understanding of how the technology works, the current state of and predicted future improvements to accuracy and bias, and the strengths and limitations of the technology when applied in real-world settings.

Understanding Global Deployment Trends and Impacts

1. **Draft a list of countries likely to be engaged in the development and deployment of the technology, with particular emphasis on those deemed likely to be deploying the technology in ways that could create significant risks to human rights.**
    a. This preliminary assessment was based on existing knowledge about nations' human rights record, technological sophistication, history of deploying technologies with significant human rights impacts, and linkages with other countries that are known to export tools and knowledge about how to use technology in ways that restrict human rights.
    b. This preliminary assessment was scoped to ensure that countries of interest were identified from a variety of geographic regions.
2. **Conduct desk research on how the technology is being deployed in the top countries of interest.**
    a. We leveraged media reporting, reports from local or international NGOs, government announcements, and other authoritative sources to compile a list of instances of planned or actual use of the technology in each country of interest. We recorded the details that have been made public about these deployments, the impact they have had, the governance structures they intersect with, and any gaps where details have not been made public.
    b. From these reports, we compiled a list of journalists, researchers, advocates, policymakers, and operators involved in the deployment, operation, governance, and investigation of the technology in each of the countries of interest.
3. **Reach out to the individuals identified in each country involved in the technology's deployment and governance, and request interviews to gather additional information.**
    a. In the case of journalists, researchers, NGOs, and advocates, we used the interviews as an opportunity to verify details and obtain updates on the deployments identified as part of step 2 (a), gain insight into the governance and operational context that exists in the country, and learn what information, reforms, or additional capacity the individual or group believes would be necessary to fully understand how the technology was being deployed, what its impact was, and how it can be governed in a way that would ensure the protection of human rights.
    b. In the case of operators, we used the interviews as an opportunity to learn more about the technical strengths and limitations of their products and services, the rules and regulations that apply to their deployments, and the internal processes they have developed to incorporate human rights concerns into their operations.

c. In the case of policymakers and government agencies, we used the interviews as an opportunity to verify details about government deployments and gain insight into the status of efforts to develop regulations and governance structures for the technology.

Developing a Human Rights Framework

1. **Conduct a review of existing human rights literature to identify existing principles, tests, and frameworks for thinking about the impacts and governance of the technology when used by the public sector.**
    a. We reviewed human rights literature, including the UDHR, ICCPR, ICESCR, Human Rights Council General Comments, UN Special Rapporteur reports, and ECHR/ECJ case law, to identify the primary human rights impacted by the use of facial recognition and other surveillance technologies by government operators.
    b. Based on our findings, we identified and elaborated on the tests that have been applied to facial recognition and similar surveillance technologies in the past to determine whether their use by governments violated human rights.
2. **Conduct a review of existing human rights literature to identify existing principles, tests, and frameworks for thinking about the impacts and governance of the technology when used by the private sector.**
    a. We reviewed human rights literature, including the UNGPs, Human Rights Council General Comments, UN Special Rapporteur reports, and ECHR/ECJ case law, to identify the primary human rights impacted by facial recognition use by private actors.
    b. Based on our findings, we identified and elaborated on the tests that have been applied to facial recognition and similar surveillance technologies in the past to determine whether their use by private actors violated human rights

Developing Recommendations

1. **Conduct a review of existing literature on proposals and recommendations for facial recognition use and governance.**
    a. We reviewed reports and publications by think tanks, advocacy organizations, academics, government agencies, developers, and industry groups to understand the current sets of issues being debated as part of a conversation around facial recognition use and governance.
    b. From these reports, we compiled a list of researchers, advocates, academics, and policymakers around the world involved in the crafting of these use and governance recommendations for facial recognition.
2. **Reach out to individuals involved in proposing recommendations for facial recognition governance and request interviews to gather additional information.**
    a. We spoke to policymakers at the local, regional, and federal level from countries around the world; academics; advocacy organizations; independent researchers; think tanks; and other CSOs to learn more about the context of proposed recommendations and identify priorities for governance.

3. **Based on the results of the literature review and interviews, draft a set of recommendations for various stakeholder groups.**
    a. Using the human rights framework developed previously as a scaffold, we developed a set of recommendations for stakeholder groups drawing both on the ideas surfaced through our literature review of recommendations as well as through our research and interviews into global deployment trends and impacts.
4. **Refine recommendations through workshops and consultations with experts.**
    a. We held two workshops as well as a number of individual interviews with experts to review our draft recommendations and receive feedback on their framing and applicability.
    b. Based on the feedback received, we drafted our final recommendations framework.

Endnotes

1 "Beijing park dispenses loo roll using facial recognition," BBC News, March 20, 2017, https://www.bbc.com/news/world-asia-china-39324431.

2 On ethnicity, see: Parmy Olson, "The Quiet Growth of Race-Detection Software Sparks Concerns Over Bias," *Wall Street Journal*, August 14, 2020, https://www.wsj.com/articles/the-quiet-growth-of-race-detection-software-sparks-concerns-over-bias-11597378154. On sexuality, see: "Row over AI that 'identifies gay faces'," BBC News, September 11, 2017, https://www.bbc.com/news/technology-41188560. On political orientation, see Beth Ellwood, "Facial recognition technology can predict a person's political orientation with 72% accuracy," PsyPost, March 4, 2021, https://www.psypost.org/2021/03/facial-recognition-technology-can-predict-a-persons-political-orientation-with-72-accuracy-59888. And on criminality, see: "Facial recognition to 'predict criminals' sparks row over AI bias," BBC News, June 24, 2020, https://www.bbc.com/news/technology-53165286.

3 Law Enforcement Imaging Technology Task Force, *Facial Recognition Use Case Catalog* (Ashburn, VA: IJIS Institute, March 2019), https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf.

4 Danny O'Brien, "Massive Database Leak Gives Us a Window into China's Digital Surveillance State," Electronic Frontier Foundation, March 1, 2019, https://www.eff.org/deeplinks/2019/03/massive-database-leak-gives-us-window-chinas-digital-surveillance-state.

5 "Nodeflux, Indonesia's First and Largest Vision AI Company to Immerse Global Recognition at the South by Southwest (SXSW) Conference and Festival 2019," Markets Insider, March 12, 2019, https://markets.businessinsider.com/news/stocks/nodeflux-indonesia-s-first-and-largest-vision-ai-company-to-immerse-global-recognition-at-the-south-by-southwest-sxsw-conference-and-festival-2019-1028021207.

6 Angelica Mari, "Brazilian police introduces live facial recognition for Carnival," ZDNet, February 25, 2020, https://www.zdnet.com/article/brazilian-police-introduces-live-facial-recognition-for-carnival/; and Robin

Yapp, "Brazilian police use 'Robocop-style' glasses at World Cup," *The Telegraph*, April 21, 2011, https://www.telegraph.co.uk/news/worldnews/southamerica/brazil/8446088/Brazilian-police-to-use-Robocop-style-glasses-at-World-Cup.html.

7 "New report raises concerns over Met Police trials of live facial recognition technology," University of Essex, July 3, 2019, https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns.

8 David Meyer, "Privacy, bias and safety: On facial recognition, Berlin and London choose different paths," Fortune, February 2, 2020, https://fortune.com/2020/02/02/facial-recognition-police-privacy-bias-germany-uk/.

9 Karen Hao, "Live facial recognition is tracking kids suspected of being criminals," *MIT Technology Review*, October 9, 2020, https://www.technologyreview.com/2020/10/09/1009992/live-facial-recognition-is-tracking-kids-suspected-of-crime/.

10 "Mexico's Coahuila to buy 1,100 facial recognition cameras," Bnamericas, January 24, 2019, https://www.bnamericas.com/en/news/ict/mexicos-coahuila-to-buy-1100-facial-recognition-cameras/.

11 For India, see: "Protesters in India object to facial recognition expansion," DW, February 18, 2020, https://www.dw.com/en/protesters-in-india-object-to-facial-recognition-expansion/a-52412455. For Russia, see: Ilya Arkhipov and Jake Rudnitsky, "In Moscow, Big Brother Is Watching and Recognizing Protesters," Bloomberg, May 1, 2021, https://www.bloomberg.com/news/articles/2021-05-02/in-moscow-big-brother-is-watching-and-recognizing-protesters. And for Uganda, see: "Three bodies of last week protests not claimed," *Daily Monitor*, November 23, 2020, https://www.monitor.co.ug/uganda/news/national/three-bodies-of-last-week-protests-not-claimed-3207394.

12 Nyan Hlaing Lin and Min Min, "Hundreds of Huawei CCTV cameras with facial recognition go live in Naypyitaw," Myanmar Now, December 15, 2020, https://www.myanmar-now.org/en/news/hundreds-of-huawei-cctv-cameras-with-facial-recognition-go-live-in-naypyitaw.

13 For the United States, see: Government Accountability Office, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues* (Washington, DC: September 2020), https://www.gao.gov/products/gao-20-568. For the European Union, see: "European Entry-Exit System," eu-LISA, October 27, 2020, https://pages.nist.gov/ifpc/2020/presentations/12_European%20Entry%20Exit%20system%20-%20IFPC%202020%20v1.0.pdf; and Anna Strattman, Wied Pakusa, and Markus Münzel, "Biometric Processes of the Entry Exit System," Federal Office for Information Security (Germany), October 27, 2020, https://pages.nist.gov/ifpc/2020/presentations/13_20201027_NIST_IFPC_BSI.pdf. For Japan, see: Yukihiro Sakaguchi, "Narita, Haneda and Kansai install facial recognition boarding," *Nikkei Asia*, December 17, 2017, https://asia.nikkei.com/Spotlight/Tokyo-2020-Olympics/Narita-Haneda-and-Kansai-install-facial-recognition-boarding. For Kenya, see: Facial Recognition System Installed at Moi International Airport," UN International Organization for Migration, October 7, 2019, https://www.iom.int/news/facial-recognition-system-installed-moi-international-airport. For Brazil, see: "Boarding Insurance uses facial recognition and offers new experiences to travelers," Serpro, October 12, 2020, https://www.serpro.gov.br/menu/noticias/noticias-2020/serpro-embarque-seguro-reconhecimento-facial. And for the UAE, see: Jay Hilotin, "Use these biometrics to pass through UAE airports," *Gulf News*, October 7, 2019, https://gulfnews.com/uae/use-these-biometrics-to-pass-through-uae-airports-1.1570459646018.

14 "Resolution 2396," UN Security Council, December 21, 2017, https://undocs.org/en/S/RES/2396(2017); "Facial Recognition System Installed at Moi International Airport," UN International Organization for Migration; Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business* (Minneapolis, Minnesota: University of Minnesota, 2020), https://www.law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf.

15 For mobile devices, see: "About Face ID advanced technology," Apple, February 26, 2020, https://support.apple.com/en-us/HT208108. For banking, see: Niccolo Mejia, "Facial Recognition in Banking – Current Applications," emerj, December 5, 2019, https://emerj.com/ai-sector-overviews/facial-recognition-in-

banking-current-applications/. And for paying, see: Agence France-Presse, "Smile-to-pay: Chinese shoppers turn to facial payment technology," *The Guardian*, September 4, 2019, https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology.

16 For public transit, see: "Chinese Facial Recognition Tech Rolls Out On Kazakh Buses," RFE/RL, October 20, 2019, https://www.rferl.org/a/china-kazakhstan-technology/30223745.html. For welfare, see: Aditya Chunduru, "Interview: Telangana Could Soon Use Facial Recognition Authentication For Ration Distribution, Says State's IT Secy Jayesh Ranjan," MediaNama, September 29, 2020, https://www.medianama.com/2020/09/223-telangana-jayesh-ranjan-interview-facial-recognition/. And for voting, see: Rina Chandran, "Votes for women? Not without facial recognition technology in Afghanistan," Reuters, November 8, 2019, https://www.reuters.com/article/us-afghanistan-women-privacy-trfn/votes-for-women-not-without-facial-recognition-technology-in-afghanistan-idUSKBN1XI1HN.

17 Aloysius Low, "In Singapore, facial recognition is getting woven into everyday life," NBC News, October 12, 2020, https://www.nbcnews.com/tech/tech-news/singapore-facial-recognition-getting-woven-everyday-life-n1242945.

18 Patrick Reevell, "How Russia is using facial recognition to police its coronavirus lockdown," ABC News, April 30, 2020, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736.

19 Cate Cadell and Gabriel Crossley, "Facial recognition and bathtime bookings: How China's universities are reopening," Reuters, August 31, 2020, https://www.reuters.com/article/us-health-coronavirus-china-students/facial-recognition-and-bathtime-bookings-how-chinas-universities-are-reopening-idUSKBN25R0UW.

20 "Japan considers facial recognition for contact tracing at big events," *Japan Times*, September 25, 2020, https://www.japantimes.co.jp/news/2020/09/25/national/japan-facial-recognition-coronavirus-contact-tracing/.

21 In workplaces, see: Mike Rogoway, "Intel's Facial Recognition Will Track Employees and Visitors," Governing, March 11, 2020, https://www.governing.com/security/intels-facial-recognition-will-track-employees-and-visitors.html. In residential complexes, see: Tanvi Misra, "The Tenants Fighting Back Against Facial Recognition Technology," Bloomberg, May 7, 2019, https://www.bloomberg.com/news/articles/2019-05-07/when-facial-recognition-tech-comes-to-housing.

22 In schools, see: Tom Simonite and Gregory Barber, "The Delicate Ethics of Using Facial Recognition in Schools," *WIRED*, October 17, 2019, https://www.wired.com/story/delicate-ethics-facial-recognition-schools. In factories, see: T.E. Narasimhan, "How facial recognition technology is transforming attendance marking system," Business Standard, September 18, 2019, https://www.business-standard.com/article/technology/how-facial-recognition-technology-is-transforming-attendance-marking-system-119091801604_1.html. And in offices, see: Karunjit Singh, "Tech Mahindra adopts facial recognition to mark attendance," *Economic Times*, August 7, 2018, https://economictimes.indiatimes.com/news/company/corporate-trends/tech-mahindra-adopts-facial-recognition-to-mark-attendance/articleshow/65300255.cms.

23 Brenda Salinas, "High-End Stores Use Facial Recognition Tools To Spot VIPs," NPR, July 21, 2013, https://www.npr.org/sections/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips.

24 For shoplifting, see: Matt Burgess, "Some UK Stores Are Using Facial Recognition to Track Shoppers," WIRED, December 20, 2020, https://www.wired.com/story/uk-stores-facial-recognition-track-shoppers/; Everton Bailey, Jr., "Portland considering strictest ban on facial recognition technology in the U.S.," *The Oregonian*, February 21, 2020, https://www.oregonlive.com/portland/2020/02/portland-considering-strictest-ban-on-facial-recognition-technology-in-the-us.html. For trespassing, see: "Haier Industrial Park In Russia Deploys Dahua Technology's Intelligent Security System," Security Informed, n.d., https://www.securityinformed.com/news/haier-industrial-park-russia-dahua-technology-intelligent-security-system-co-4261-ga.1590063358.

html. For stadiums, see: Stephen Mayhew, "Danish football stadium deploys Panasonic facial recognition to improve fan safety," Biometric Update, July 1, 2019, https://www.biometricupdate.com/201907/danish-football-stadium-deploys-panasonic-facial-recognition-to-improve-fan-safety. For casinos, see: Jacob Solis, "How AI and facial recognition tech could reshape Las Vegas casinos," *Nevada Independent*, January 21, 2020, https://thenevadaindependent.com/article/how-new-ai-and-facial-recognition-tech-could-reshape-las-vegas-casinos. And for concerts, see: Steve Knopper, "Why Taylor Swift Is Using Facial Recognition at Concerts," *Rolling Stone*, December 13, 2018, https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.

25 "General comment No. 37 on the right of peaceful assembly (article 21)," UN Human Rights Committee, September 17, 2020, http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2bWPAXj3%2bho0P51AAHSqSubYW2%2fRxcFiagfuwxycuvi40wJfdPLI9%2feceDWBX%2fij2tgqDXgdjqx8wTKKbIoySyDPtsMO.

26 "Resolution 2396," UN Security Council.

27 Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business*.

28 Madhumita Murgia, "New details emerge of King's Cross facial recognition plans," *Financial Times*, September 3, 2019, https://www.ft.com/content/3293b4e6-ce3a-11e9-b018-ca4456540ea6; and Dan Sabbagh, "Facial recognition row: police gave King's Cross owner images of seven people," *The Guardian*, October 4, 2019, https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people.

29 "Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Office of the High Commissioner for Human Rights, May 28, 2019, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35.

30 Diala Shamas and Nermeen Arastu, "Mapping Muslims: NYPD Spying and its Impact on American Muslims," CLEAR Project, n.d., https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf; Lee Rainie and Mary Madden, "Americans' Privacy Strategies Post-Snowden," Pew Research Center, March 16, 2015, https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/; and Amory Starr et al., "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis," *Qualitative Sociology* 31 (2008): 251–270, doi:10.1007/s11133-008-9107-z.

31 Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT)* (Gaithersburg, MD: NIST, April 2021), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

32 "Amazon Rekognition: Use cases that involve public safety," Amazon Web Services, n.d., https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html.

33 Pete Fussey and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Essex, United Kingdom: Human Rights, Big Data and Technology Project, July 2019), https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

34 "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology (NIST), May 18, 2020, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

35 Jeffrey Dastin, "Rite Aid deployed facial recognition systems in hundreds of U.S. stores," Reuters, July 28, 2020, https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

36 Drew Harwell and Eva Dou, "Huawei tested AI software that could recognize Uighur minorities and alert police, report says," *Washington Post*, December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

37 Dominic J. Nardi, "Religious Freedom in China's High-Tech Surveillance State," United States Commission on International Religious Freedom, September 2019, https://www.uscirf.gov/sites/default/files/2019%20China%20Surveillance%20State%20Update.pdf.

38 U.S. State Department Office of International Religious Freedom, *Report on International Religious Freedom: Uzbekistan* (Washington, DC: Department of State, 2019), https://www.state.gov/reports/2019-report-on-international-religious-freedom/uzbekistan/.

39 Kashmir Hill and Gabriel J.X. Dance, "Clearview's Facial Recognition App Is Identifying Child Victims of Abuse," *New York Times*, February 7, 2020, https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html; Ryan Daws, "Aussie police use Clearview AI's facial recognition to fight child exploitation," AI News, January 11, 2021, https://artificialintelligence-news.com/2021/01/11/police-use-clearview-ai-facial-recognition-increased-26-capitol-raid/; and Andrew Russell, "RCMP used Clearview AI facial recognition tool in 15 child exploitation cases, helped rescue 2 kids," Global News, February 27, 2020, https://globalnews.ca/news/6605675/rcmp-used-clearview-ai-child-exploitation/.

40 Kashmir Hill, "Your Face Is Not Your Own," *New York Times*, March 18, 2021, https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html.

41 Anthony Cuthbertson, "Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology," *The Independent*, April 24, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html.

42 "Argentina: Child Suspects' Private Data Published Online," Human Rights Watch, October 9, 2020, https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online#.

43 Tom Simonite and Gregory Barber, "The Delicate Ethics of Using Facial Recognition in Schools."

44 "Facial recognition: School ID checks lead to GDPR fine," BBC News, August 27, 2019, https://www.bbc.com/news/technology-49489154.

45 "Penalty fee for face recognition in school," Integritetsskyddsmyndigheten, August 21, 2019, https://www.imy.se/nyheter/2019/sanktionsavgift-for-ansiktsigenkanning-i-skola; and République Française, "Tribunal Administratif de Marseille," La Quadrature du Net, February 27, 2020, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf.

46 Claire Galligan et al., *Cameras in the Classroom: Facial Recognition Technology in Schools* (Ann Arbor, Michigan: Gerald R. Ford School of Public Policy, 2020), http://stpp.fordschool.umich.edu/sites/stpp.fordschool.umich.edu/files/file-assets/cameras_in_the_classroom_full_report.pdf.

47 Julie Bosman and Serge F. Kovaleski, "Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?," *New York Times*, May 18, 2019, https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html; Craig McCarthy, "Facial recognition leads cops to alleged rapist in under 24 hours," *New York Post*, August 5, 2019, https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/; and Betsy Powell, "How Toronto police used controversial facial recognition technology to solve the senseless murder of an innocent man," *Toronto Star*, April 13, 2020, https://www.thestar.com/news/gta/2020/04/13/how-toronto-police-used-controversial-facial-recognition-technology-to-solve-the-senseless-murder-of-an-innocent-man.html?rf.

48 Fussey and Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*.

49 "Resolution 2396," UN Security Council.

50 Chunduru, "Interview: Telangana Could Soon Use Facial Recognition Authentication For Ration Distribution, Says State's IT Secy Jayesh Ranjan."

51 "Thailand scans fishermen's eyes to cut slavery," *The National*, February 20, 2018, https://www.thenationalnews.com/business/thailand-scans-fishermen-s-eyes-to-cut-slavery-1.706281.

52 Jeffrey Ding, "ChinAI #127: Three Seconds Too Long in the Bathroom," ChinaAI, January 17, 2021, https://chinai.substack.com/p/chinai-127-three-seconds-too-long.

53 Ashleigh Webber, "PwC facial recognition tool criticised for home working privacy invasion," Personnel Today, June 16, 2020, https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion/.

54 "International Covenant on Civil and Political Rights (Articles 12,17,19,21,22)," United Nations, 1967, https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf; UN Human Rights Committee, "General comment No. 16," Office of the High Commissioner for Human Rights, April 8, 1988, http://ccprcentre.org/page/view/general_comments/27798; UN Human Rights Committee, "General comment No. 27," Office of the High Commissioner for Human Rights, June 30, 2014, https://undocs.org/A/HRC/27/37; UN Human Rights Committee, "General comment No. 34," Office of the High Commissioner for Human Rights, September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf; and UN Human Rights Committee, "General comment No. 37," Office of the High Commissioner for Human Rights, September 17, 2020, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f37&Lang=en.

55 UN Human Rights Committee, "General comment No. 34 (paragraph 25)," Office of the High Commissioner for Human Rights, September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

56 UN Human Rights Committee, "The right to privacy in the digital age," Office of the High Commissioner for Human Rights, August 3, 2018, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf.

57 UN Human Rights Committee, "Concluding observations on the fourth periodic report of the United States of America (paragraph 22)," *International Covenant on Civil and Political Rights*, April 23, 2014, https://undocs.org/CCPR/C/USA/CO/4.

58 Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (paragraph 69)," United Nations Human Rights Council, December 28, 2009, https://undocs.org/A/HRC/13/37, and "Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (paragraph 50)," Office of the High Commissioner for Human Rights, May 28, 2019, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35.

59 UN Human Rights Committee, "The right to privacy in the digital age (paragraph 41)," Office of the High Commissioner for Human Rights, August 3, 2018, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf; and UN Human Rights Committee, "Concluding observations on the sixth periodic report of Italy (paragraph 38)," *International Covenant on Civil and Political Rights*, May 1, 2017, https://undocs.org/en/CCPR/C/ITA/CO/6; and UN Human Rights Committee, "The right to privacy in the digital age (paragraphs 40, 41)," Office of the High Commissioner for Human Rights, June 30, 2014, https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc.

60 UN Human Rights Committee, "General comment No. 16 (paragraph 8)," Office of the High Commissioner for Human Rights, April 8, 1988, http://ccprcentre.org/page/view/general_comments/27798.

61 UN Human Rights Committee, "The right to privacy in the digital age (paragraph 35)," Office of the High Commissioner for Human Rights, August 3, 2018, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf.

62 UN Human Rights Committee, "Concluding observations on the sixth periodic report of Italy (paragraph 38)," *International Covenant on Civil and Political Rights*, May 1, 2017, https://undocs.org/en/CCPR/C/ITA/CO/6.

63 Pierre Thielbörger, "The 'Essence' of International Human Rights," German Law Journal 20, no. 6 (2019): 924–939, doi:10.1017/glj.2019.69.

64 Fussey and Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*.

65 UN Human Rights Committee, "General comment No. 34 (paragraph 35)," Office of the High Commissioner for Human Rights, September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf; and Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (paragraph 66)," United Nations Human Rights Council, December 28, 2009, https://undocs.org/A/HRC/13/37.

66 "Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (paragraph 24)," Office of the High Commissioner for Human Rights, May 28, 2019, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35.

67 "International Covenant on Civil and Political Rights (paragraph 3)," United Nations, 1967, https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf.

68 Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (paragraph 29)," United Nations Human Rights Council, April 17, 2013, https://undocs.org/A/HRC/23/40.

69 UN Human Rights Committee, "General Comment No. 34 (paragraph 34)," Office of the High Commissioner for Human Rights, September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

70 UN Human Rights Committee, "General Comment No. 16 (paragraph 4)," Office of the High Commissioner for Human Rights, April 8, 1988, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf; and UN Human Rights Committee, "General Comment No. 34 (paragraph 34)."

71 "Digital Rights Ireland Ltd., Judgement of the Court, Joined Cases C293/12 and C594/12 (paragraph 37)," Court of Justice of the European Union, April 8, 2014, https://curia.europa.eu/juris/document/document_print.jsf?docid=150642&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=10148643.

72 "B-Tech Project," United Nations Human Rights Office of the High Commissioner, https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

73 Chris Burt, "Morocco places moratorium on facial recognition, California limits police use," Biometric Update, September 12, 2019, https://www.biometricupdate.com/201909/morocco-places-moratorium-on-facial-recognition-california-limits-police-use; Jess Bauldry, "No facial recognition for Lux CCTV," Delano, April 10, 2019, https://delano.lu/article/delano_no-facial-recognition-lux-cctv; Charles Rollet, "Belgium Bans Private Facial Surveillance," IPVM, July 6, 2018, https://ipvm.com/reports/belgium-biometrics.

74 "Information: Ethics Committee," West Midlands Police and Crime Commissioner, n.d., https://www.westmidlands-pcc.gov.uk/ethics-committee/.

75 United Nations Human Rights Office of the High Commissioner, "Designing and implementing effective company-based grievance mechanisms," *A B-Tech Foundational Paper*, January 2021, https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-company-based-grievance-mechanisms.pdf.

76 Examples of transparency reporting include "Company Assessments," Global Network Initiative, April 2020, https://globalnetworkinitiative.org/company-assessments/; "Transparency Reporting Index," Access Now, Last updated October 2019, https://www.accessnow.org/transparency-reporting-index/; and "2020 Ranking Digital Rights corporate Accountability Index," Ranking Digital Rights, https://rankingdigitalrights.org/index2020/.

77 Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications* 10, No. 3069 (2019), https://doi.org/10.1038/s41467-019-10933-3.

78 European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Vienna: European Union Agency for Fundamental Rights, 2020), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

79 Ella Jakubowska and Diego Naranjo, *Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States* (Brussels: European Digital Rights (EDRi), May 2020), https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf.

80 "Engrossed Substitute Senate Bill 6280," The Legislature of the State of Washington, March 31, 2020, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20200726113658.

81 "Creation Of A Privacy Advisory Commission," Oakland City Council, January 19, 2016, https://oakland.legistar.com/LegislationDetail.aspx?ID=2503814&GUID=DD0D90E4-1084-44D0-8E74-D7FA2530724D&Options=ID|Text|&Search=13349.

82 "Ordinance Adding Chapter 9.64 to the Oakland Municipal Code Establishing Rules for the City's Acquisition and Use of Surveillance Equipment," Oakland City Council, April 26, 2016, https://www.documentcloud.org/documents/4450176-View-Supplemental-Report-4-26-18.html.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**