Health, Ethics, and Law
Institute for Training, Research, and Advocacy

Indian Journal of Medical Ethics

Covid-19 Insights: Analysis from Ethics, Human Rights and Law Perspectives

Blog 26 | HEaL Institute & IJME – Covid-19 Insights | June 7, 2021

Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance | Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF), and Instituto Brasileiro de Defesa do Consumidor (IDEC).

June 7, 2021

We, the undersigned, call for an outright ban on uses of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance. These tools have the capacity to identify, follow, single out, and track people everywhere they go, undermining our human rights and civil liberties — including the rights to privacy and data protection, the right to freedom of expression, the right to free assembly and association (leading to the criminalization of protest and causing a chilling effect), and the rights to equality and non-discrimination.

We have seen facial recognition and remote biometric recognition technologies used to enable a litany of human rights abuses. In **China,** the **United States, Russia, England, Uganda, Kenya, Slovenia, Myanmar,** the **United Arab Emirates, Israel,** and **India,** surveillance of protesters and civilians has harmed people's right to privacy and right to free assembly and association. The wrongful arrests of innocent individuals in the **United States, Argentina,** and **Brazil** have undermined people's right to privacy and their rights to due process and freedom of movement. The surveillance of ethnic and religious minorities and other marginalized and oppressed communities in **China, Thailand,** and **Italy** has violated people's right to privacy and their rights to equality and non-discrimination.

These technologies, by design, threaten people's rights and have already caused significant harm. No technical or legal safeguards could ever fully eliminate the threat they pose, and we therefore believe they should never be used in public or publicly accessible spaces, either by governments or the private sector. The potential for abuse is too great, and the consequences too severe.

We call for a ban because, even though a moratorium could put a temporary stop to the development and use of these technologies, and buy time to gather evidence and organize democratic discussion, it is already clear that these investigations and discussions will only further demonstrate that **the use of these technologies in publicly accessible spaces is incompatible with our human rights and civil liberties and must be banned outright and for good.**

The scope of our call

The terms "facial recognition" and "remote biometric recognition" cover a wide range of technologies, from the facial authentication system that unlocks a person's phone, or otherwise authorizes one's access to certain places, to technology that identifies one's gait, to systems that purport to detect one's gender identity or emotional state.

Our call for a ban specifically focuses on, but is not limited to, the use of these technologies to identify or distinguish a person from a larger set of individuals, also known as facial or biometric "identification" (i.e. one-to-many matching). We are concerned about the use of these technologies to identify, single out, or track individuals using their face, gait, voice, personal appearance, or any other biometric identifier in a manner that enables mass surveillance or discriminatory targeted surveillance, i.e., surveillance that disproportionately impacts the human rights and civil liberties of religious, ethnic, and racial minorities, political dissidents, and other marginalized groups. We also acknowledge that, in certain cases, facial and other biometric "authentication" systems (i.e. one-to-one matching) can be built and used in a manner that equally enables problematic forms of surveillance, such as by creating large, centralized biometric databases which can be reused for other purposes.

Although some applications of facial recognition and remote biometric recognition claim to protect people's privacy by not linking to their legal identities, they can nevertheless be used to single out individuals in public spaces, or to make inferences about their characteristics and behavior. In all such situations, it does not matter whether data are anonymized to protect personally identifiable information or only processed locally (i.e. "on the edge"); the harm to our rights occurs regardless because these tools are fundamentally designed for, and enable, the surveillance of people in a manner that is incompatible with our rights.

Furthermore, many applications of facial and biometric classification, which make inferences and predictions about things such as people's gender, emotions, or other personal attributes, suffer from serious, fundamental flaws in their scientific underpinnings. This means that the inferences they make about us are often invalid, in some cases even operationalizing **eugenicist theories of phrenology and physiognomy,** thereby perpetuating discrimination and adding an additional layer of harm as we are both surveilled and mischaracterized.

Our call for a ban covers the use of these technologies when they are used for surveillance in publicly accessible spaces and in spaces which people cannot avoid. While law enforcement use of these technologies has attracted attention and criticism, their use by private actors can pose the same threat to our rights, especially when private actors effectively engage in surveillance on behalf of governments and public agencies in public-private partnerships or otherwise provide information derived from such surveillance to the authorities.

We have also seen a worrying development with private facial recognition providers compiling and amalgamating **databases of "suspicious" individuals,** and sharing these databases with multiple clients. This in effect creates "nationwide databases" shared between private companies which are compiled at the discretion of untrained staff, are not subject to any oversight, and which can lead to discrimination against individuals who appear on watchlists in all premises using such databases.

The use of these technologies to surveil people in city parks, schools, libraries, workplaces, transport hubs, sports stadiums, housing developments, and even in online spaces such as social media platforms, constitutes an existential threat to our human rights and civil liberties and must be stopped.

Why a ban?

Facial recognition and remote biometric recognition technologies have significant technical flaws in their current forms, including, for example, facial recognition systems that reflect racial bias and are less accurate for people with darker skin tones. However, technical improvements to these systems will not eliminate the threat they pose to our human rights and civil liberties.

While adding more diverse training data or taking other measures to improve accuracy may address some current issues with these systems, this will ultimately only perfect them as instruments of surveillance and make them more effective at undermining our rights.

These technologies pose a threat to our rights in two major ways:

First, the training data — the databases of faces against which input data are compared, and the biometric data processed by these systems — are usually **obtained without one's knowledge, consent, or genuinely free choice to be included,** meaning that these technologies encourage both mass and discriminatory targeted surveillance by design.

Second, as long as people in publicly-accessible spaces can be instantaneously identified, singled out, or tracked, their human rights and civil liberties will be undermined. Even the idea that such technologies could be in operation in publicly accessible spaces creates a chilling effect which undermines people's abilities to exercise their rights.

Despite questionable claims that these technologies improve public security, any benefits will always be vastly outweighed by the systematic violation of our rights. We see growing evidence of how these technologies are **abused** and deployed with little to no transparency.

Any survey and analysis of how policing has historically been conducted shows that experimental use of surveillance technologies often criminalizes low-income and marginalized communities, including communities of color, the same communities that have traditionally faced structural racism and discrimination. The use of **facial recognition and remote biometric recognition technologies is not an exception** to this, and for that reason it must be stopped before an even more dangerous surveillance infrastructure is created or made permanent.

The mere existence of these tools, whether in the hands of law enforcement or private companies (or in public-private partnerships), will always create incentives for function creep and increased surveillance of public spaces, placing a chilling effect on free expression. Because their very existence undermines our rights, and effective oversight of these technologies is not possible in a manner that would preclude abuse, there is no option but to ban their use in publicly accessible spaces entirely.

What will a ban look like?

There are some surveillance technologies that are simply so dangerous that they inevitably cause far more problems than they solve. When it comes to facial recognition and remote biometric technologies that enable mass surveillance and discriminatory targeted surveillance, the potential for abuse is too great, and the consequences too severe.

There is no room for doubt: the protection of human rights and civil liberties demands a ban on the use in publicly accessible spaces of these technologies by national, state, provincial, municipal, local, and other governments, including all their subdivisions and authorities — and especially their law enforcement and border control agencies, who already have sufficient human and technological resources to maintain safety without these technologies.

As a global network of civil society organizations, we acknowledge that every country has different ways to develop solutions that prioritize human rights under their unique constitutional, conventional, or legal systems.

However, whatever the means may be, the result must be an outright ban on the use of these technologies to surveil, identify, track, classify, and follow people in publicly accessible spaces.

For all these reasons, we urge:

---

1. Policymakers and lawmakers at all levels of government around the world to:

a. Stop all public investment in uses of facial recognition and remote biometric technologies that enable mass surveillance and discriminatory targeted surveillance;

b. Adopt comprehensive laws, statutes, and/or regulations that:

i. prohibit the use of these technologies for surveillance of public and publicly accessible spaces, including public transportation, by or on behalf of national, federal, state, provincial, municipal, local, and/or other political subdivisions governments, including their agencies, departments, secretariats, ministries, executive offices, boards, commissions, bureaus, or their contractors, and/or other subdivisions and authorities; with special emphasis on any type of law enforcement, criminal investigation, border control, and intelligence agencies;

ii. prohibit the use of these technologies by private entities in public spaces, publicly-accessible spaces, and places of public accommodation, where such use could enable mass surveillance or discriminatory targeted surveillance, including but not limited to their use in parks, schools, libraries, workplaces, transport hubs, sports stadiums, and housing developments;

iii. prohibit government agencies, especially law enforcement agencies, from using and accessing data and information derived from the use of these technologies by private companies and other private actors, except for the purposes of audits or compliance checks;

iv. protect persons against the use of these technologies to make decisions in issues related to economic, social, and cultural rights, including housing, employment, social benefits, and healthcare;

v. exclude the use of these technologies, and the information derived from them, as evidence to criminally prosecute or accuse people to imprison or otherwise detain them; and

vi. restrict government access to biometric information stored by private companies;

c. Establish rules and regulations that prohibit the procurement of these technologies by government and state agencies for uses that enable mass surveillance and discriminatory targeted surveillance;

d. Stop using facial recognition and remote biometric technologies for mass surveillance or discriminatory targeted surveillance of religious, ethnic, and racial minorities and political dissidents and other marginalized groups;

e. Mandate the disclosure of the use of these technologies to those individuals that were unknowingly subjected to them and who were not given a chance to exercise their due process rights to contest the use of the technology; and

f. Provide appropriate reparation to individuals who were damaged by the use of these technologies;

---

2. Courts and judicial officers to acknowledge the existential threats to human rights that arise from the use of these technologies and to act to prevent and, if necessary, redress the harms caused by their use; and

---

3. Administrative agencies, including data protection and consumer protection agencies, to use their full authority to protect privacy and consumer rights, including urging companies to stop the use of these technologies.

Finally, we acknowledge that the existential threat posed by facial recognition and remote biometric recognition technologies should be tackled not only by countries and governments of all kinds, but also by other important actors at the international and national levels.

For that reason, we call on:

---

1. International organizations, such as the U.N. Office of the High Commissioner for Human Rights Office (OHCHR), to step up and condemn the current development and use of facial recognition and remote biometric recognition technologies to surveil communities across the globe;

2. **Private entities** that develop or use facial recognition and remote biometric recognition technologies to:

a. Make public commitments to cease the creation, development, sale, and use of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance;

b. Immediately cease the production of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance, and delete any illegitimately acquired biometric data used to build databases and any models or products built upon such data;

c. Issue transparency reports that detail all their public contracts (including ones that are suspended, ongoing, or in the making) for the provision of these technologies; and

d. Meaningfully engage with and refrain from retaliating against workers that organize in their workplaces to challenge or refuse the development of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance;

---

3. Workers of technology companies, with the support of their unions, to organize in their workplaces against the development or sale of facial recognition and remote biometric recognition technologies, to the extent possible;

---

4. Investors and financial institutions to:

a. conduct human rights due diligence on their ongoing and future investments in companies developing and selling facial recognition and remote biometric recognition technologies in order to find where these technologies are incompatible with human rights and enable mass surveillance and discriminatory targeted surveillance; and,

b. call on the companies they invest in to cease creating, developing, selling, or otherwise making available these technologies in ways that enable mass surveillance and discriminatory targeted surveillance;

---

5. Donor organizations to ensure funding for litigation and advocacy by non-governmental and civil society organizations that seek redress for harms before courts and actively engage in policymaking at local, state, provincial, national, federal, supranational, regional, and international systems.

Conclusion

We ask civil society, activists, academics, and other stakeholders from across the globe to sign on to this letter and join the fight to ensure that the use of these technologies in publicly accessible spaces is banned now and forever so that our human rights and civil liberties are protected.

Contact **mailto:banBS@accessnow.org** for more information about how you can support this initiative and visit **accessnow.org/ban-biometric-surveillance** to see the full list of signatories and add your name to the list.

Regional languages: Open letters: Hindi, Bengali, Gujarati, Tamil, Assamese

International languages: Open letters: French, Mandarin, Portuguese, Spanish, Turkish