Stanford | Global Digital Policy Incubator
Cyber Policy Center

GLOBAL DIGITAL POLICY SNAPSHOT

PROTECTING HUMAN RIGHTS IN THE REGULATION OF FACIAL RECOGNITION TECHNOLOGY

AUGUST 2020

INSIDE THIS BRIEF:

KEY TAKEAWAYS

Challenge: Facial recognition technology is being deployed rapidly across the world––for many purposes––by governments and the private sector, but often without adequate assessment of potential human rights impacts. Regulators lack a coherent and consistent human rights framework for assessing the impact of various applications of facial recognition.

State of Play: The regulatory environment around facial recognition has become increasingly fragmented. Regulations are starting to proliferate at all levels of government through restrictions on particular uses of the technology by government agencies, limits on private sector applications, and rules about utilization of biometric data. This fragmentation reflects and contributes to a lack of consensus on the right way to regulate facial recognition or how to assess the normative implications of its use.

Recommendations: This snapshot makes six recommendations to government policymakers about how to protect human rights when facial recognition is deployed:

- Require notice of situations where citizens are exposed to facial recognition;
- Create comprehensive rules on data protection and processing for private sector uses of facial recognition;
- Require both public sector and private sector actors to assess the efficacy and facial recognition technologies before deploying them;
- Require human rights impact assessments for all uses of facial recognition which could implicate human rights;
- Place a moratorium on facial recognition use in law enforcement, immigration and criminal justice contexts until human rights impacts can be addressed;
- Restrict import and procurement of facial recognition technology from and export of these technologies to authoritarian regimes.

INTRODUCTION

Over the past several years, both government and private sector actors have deployed facial recognition technologies at an accelerated pace. These applications have been used for both malign and benign purposes, ranging from China's alarming surveillance of their minority communities, to smartphone companies featuring facial recognition to unlock phones, to U.S. law enforcement agency deployment of facial recognition to track criminals (and, more recently, protestors), to airlines' use of facial recognition to facilitate faster boarding at airports. Yet, there is a lack of consensus on the right way to regulate the varied and advancing uses of facial recognition technology, and an insufficient framework for addressing human rights risks posed by this technology.

LANDSCAPE OF REGULATION ABOUT FACIAL RECOGNITION

Facial recognition technology is currently regulated in three ways: (1) regulation of specific applications of facial recognition technology by government agencies; (2) rules limiting utilization of facial recognition by private sector actors; and (3) regulations that govern both the public and private sector.

Across all three of these categories, much of the regulation that impacts facial recognition globally actually regulates **processing of all forms of biometric data, not just facial recognition systems**. Biometrics includes a range of physical characteristics that can be used to identify people, such as data on facial structure, DNA samples or fingerprint measures. Illinois's Biometric Information Privacy Act (BIPA), and certain provisions of the European Union's General Data Protection Regulation (GDPR) provide examples of this broad model of biometric data regulation, that also encompasses facial recognition.

The first category of laws that focus specifically on use of facial recognition technology by **government actors, frequently focus on application of the technology for law enforcement purposes.** For example, California has placed a three-year statewide moratorium on use of facial recognition technology by law enforcement. Following racial justice protests across the US which focused on police misconduct, the city of Boston banned the use of facial recognition technology by any city employee.

In other cases, the focus of facial recognition regulation is on **private sector use**. Laws focused on commercial uses of biometric information address concerns about how companies profit from people's data and the risks posed to privacy. Again, Illinois's Biometric Information Privacy Act (BIPA) is an example of this type of regulation. It requires any private entity to provide notice and obtain written consent before collecting, storing or processing biometric data. Civil lawsuits filed under this act have resulted in large settlements from companies like Facebook, and have in some cases been successfully filed outside of Illinois. Canada also has special regulation focused on commercial uses of biometric information, and this features different rules than those applied under the country's Privacy Act which applies to government entities.

LANDSCAPE OF REGULATION ABOUT FACIAL RECOGNITION, CONT.

More rarely, laws may **apply to both public and private sector uses**. For example, Morocco's moratorium on facial recognition applies across the board. The European Union's approach to data processing under GDPR also has implications for both public and private uses.

Laws also vary in their approach to regulation. Some impose a **complete ban on the use of facial recognition by parties covered under the law**. These complete bans––as in the case of Boston's and Oakland's prohibitions on use of facial recognition by public officials––can be permanent or indefinite, but have also been put in place as a temporary moratorium to allow the government more time to develop stronger regulation. The Morocco moratorium, referenced above, is an example of this type of moratorium.

Other laws instead **govern the particular circumstances under which facial recognition can be used,** and what process must be undertaken to ensure the technology is used appropriately. Washington State, for example, recently enacted requirements that any government agency that wants to use facial recognition for any public purpose must provide public notice, hold a minimum of three community meetings, and release an impact assessment. It also requires law enforcement to get a warrant or court order before using the technology. Additionally, there are limits on the types of government decisions that can be based on facial recognition technology without human review. The law also requires that government employees be trained to understand the technology's limitations and requirements for third-party testing of any technology that will be used by the government. A new South African law on data protection places limitations on the circumstances under which biometric data processing may occur, including requiring consent from the data subject in most cases. These regulations typically require consent, but also often include carve outs for "public interest" or "national security. These measures attempt to **create guardrails without banning the use of the technology entirely**.

Beyond all of these approaches to regulation, there are non-regulatory factors that impact the use of facial recognition in different contexts. For example, courts in various jurisdictions have determined that the use of facial recognition is subject to limits under existing human rights laws. In addition, private sector policies and practices are increasingly influencing the parameters of appropriate use. Many of the largest companies producing facial recognition technology have recently announced changes to their own internal policies that limit the circumstances under which the technology can be deployed, in some cases halting the use of the technology altogether until policymakers develop appropriate rules. Taken together, these non-regulatory considerations factor heavily into the policymaking landscape.

HUMAN RIGHTS IMPLICATIONS & RISKS

Regulation of facial recognition is important because of substantial human rights implications and inherent risks associated with the technology.

The Right to Privacy: The most fundamental human rights risk posed by facial recognition technology relates to the right to privacy. Risks to privacy arise in two ways in the context of facial recognition. The first is through the data collection process itself. Facial recognition systems must be trained on large quantities of data (in this case images of faces). This data is used to develop the software and to test its accuracy. In order to get sufficient data to develop these systems, some companies have collected images of people by scraping social media sites, or through other means which do not involve the consent of those whose image is being captured. This means that people's faces can be included in databases without them even being aware of it. Secondly, there are privacy risks posed if data collected is not stored securely and is then put to use for malign purposes by unauthorized users.

The Right to Equal Protection and Non-Discrimination: A second major human rights concern relates to the risk of reinforcing bias and discrimination. Research has found that facial recognition systems are often systematically better at identifying certain faces (typically white and male faces) than others. This means that misidentification is more likely for certain groups of people, especially minority communities. When applied in the context of law enforcement, facial recognition can lead to discriminatory decisions that impact due process rights. In addition, the groups that tend to be less-well-identified are often those that already face discrimination or bias, so these systems have the potential to amplify existing structural problems faced by vulnerable groups.

These concerns are also exacerbated by assumptions that technology is inherently reliable, less biased and more accurate than humans. That understanding can lead to wrongful decisions made by technology going unquestioned by humans. After two high profile cases where an innocent person was arrested based on an error made by facial recognition software, the Detroit police chief acknowledged: "if we would use the software only, we would not solve the case 95 to 97% of the time."

Liberty and Autonomy - The Rights to Freedom of Expression, Assembly, Association, Movement: Finally, facial recognition technology, especially if used for mass surveillance or unwarranted monitoring, can have implications for a wide range of human freedoms. Ubiquitous facial recognition is a growing trend in authoritarian contexts, where the technology is being used to repress dissidents, monitor minority groups, and to control citizens. The most prominent examples are China and Russia. In China, facial recognition has been deployed as part of an ongoing campaign of persecution against the Uyghers and other minority groups. In Russia, facial recognition has been used at protests, something which is being challenged in the European Court of Human Rights. In a very concerning trend, widespread deployment of facial recognition is gaining support in some democratic contexts without adequate consideration for its impact on basic liberty. Several concerning cases within democracies have arisen recently, including police use of facial recognition in South Wales and police in both Miami and New York using facial recognition to arrest protestors. As they craft policies around use of facial recognition technology, it's critical for democracies to develop regulations that protect human rights.

RECOMMENDATIONS FOR POLICY MAKERS

To ensure that facial recognition is not deployed in ways that violate human rights, lawmakers should incorporate the following recommendations when considering regulation of this technology:

1. **Require notice to citizens that makes it clear under what circumstances citizens may be exposed to facial recognition, what it will be used for and how their data will be handled.**
2. **Create comprehensive rules on informed consent, data storage and data processing for commercial use of facial recognition, to ensure that any use is done in line with the protection of human rights.**
3. **Require both public sector and private sector actors to assess the efficacy and reliability of facial recognition technologies deployed for any purpose before it is deployed.** Facial recognition technology may be an appropriate solution to some problems, but it also comes with inherent risks to human rights. An evaluation of the risks and benefits of particular applications should be conducted before putting human rights at risk.
4. **Require human rights impact assessments before deployment of facial recognition technology by any government or private sector entity when human rights could be implicated.** These assessments should be made publicly available, along with a mitigation strategy detailing how any risks will be overcome.
5. **Place a moratorium on use of facial recognition for law enforcement, immigration services or criminal justice purposes, until human rights impacts can be rectified with confidence.**
6. **Restrict import and/or procurement of surveillance tools from authoritarian regimes, and export of tools developed in countries with strong, rights-respecting regulations to countries lacking such regulations.**

DIVING DEEPER ON REGULATION OF FACIAL RECOGNITION

Rules for a New Surveillance Reality, Amos Toh, *Human Rights Watch*

Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance, *Amnesty International*

Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement, *CITRIS Policy Lab*

Human Rights in the Age of AI: A Case Study Examining Law Enforcement Use of AI-Powered Facial Recognition, *Access Now*

AUTHORS

Eileen Donahoe is Executive Director of the Global Digital Policy Incubator. She previously served as the U.S. Ambassador to the UN Human Rights Commission, and serves in leadership and advisory roles across the global democracy and human rights community.

Megan Metzger is a Research Scholar and Associate Director of Research for the Global Digital Policy Incubator. She completed a PhD in Politics at NYU as a member of the Social Media and Political Participation Lab and her research focuses on how technology impacts rights and political behavior.

Kip Wainscott is a Senior Advisor for the Global Digital Policy Incubator. A lawyer and policy professional with experience in government, civil society, and the private sector, he has worked extensively on issues concerning technology's impact on democracy and human rights.

With research assistance from Sreya E Guha, Madeline Libbey, Jeffrey Propp, and Avalon Wolfe.

This snapshot was created in partnership with the International Center for Not-for-Profit Law.

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW