February 2021

Facial Recognition in the Public Sector: The Policy Landscape

Rashida Richardson

This brief is one of two presenting strategies for addressing challenges associated with facial recognition. These briefs provide policymakers concrete options for setting guardrails and aim to stimulate debate on possible paths forward.

This brief relays the use of facial recognition technology in the public sector around the world and surveys proposed and pending laws and regulations to mitigate human and civil rights concerns associated with government use of facial recognition.

The other brief, *Transparency and Accountability Mechanisms for Facial Recognition* by Els J. Kindt explores in greater depth three existing regulatory mechanisms of general application that may have specific relevance to facial-recognition technology: data protection impact assessments, technical standards, and certification mechanisms.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

Executive Summary

Facial-recognition technology is increasingly common throughout society. We can unlock our phones with our faces, smart doorbells let us know who is outside our home, and sentiment analysis allows potential employers to screen interviewees for desirable traits. In the public sector, facial recognition is now in widespread use—in schools, public housing, public transportation, and other areas. Some of the most worrying applications of the technology are in law enforcement, with police departments and other bodies in the United States, Europe, and elsewhere around the world using public and private databases of photos to identify criminal suspects and conduct real-time surveillance of public spaces.

Despite the widespread use of facial recognition and the concerns it presents for privacy and civil liberties, this technology is only subject to a patchwork of laws and regulations. Certain jurisdictions have imposed bans on its use while others have implemented more targeted interventions. In some cases, laws and regulations written to address other technologies may apply to facial recognition as well.

This brief first surveys how facial-recognition technology has been deployed in the public sector around the world. It then reviews the spectrum of proposed and pending laws and regulations that seek to mitigate or address human and civil rights concerns associated with government use of facial recognition, including:.

- moratoriums and bans
- standards, limitations, and requirements regarding databases or data sources
- data regulations
- oversight and use requirements
- government commissions, consultations, and studies

Facial Recognition in the Public Sector

Facial-recognition technology is used in the private and public sectors for a wide range of purposes including identification, verification, object or person detection, access control, group demographic analysis, and sentiment or affect analysis.

Law Enforcement

Law-enforcement agencies use facial-recognition technology to support investigations and for mass or targeted surveillance. These uses are rarely regulated and there is growing concern regarding ones that fail to comply with existing constitutional or other legal protections. The most common law-enforcement use of the technology is face identification, in which images obtained from law-enforcement or private sources are compared with a preexisting database of face images. This is controversial for several reasons. For instance, many law-enforcement databases that are used to run facial-recognition searches are significantly biased, error-ridden, or misleading (such as mugshot databases are not well maintained and often include individuals that are not charge with a crime).[1]

Some law-enforcement agencies use facial-recognition technology in live video surveillance. In the United Kingdom, the London Metropolitan, Leicestershire, and South Wales police use facial recognition on live public closed-circuit television (CCTV). However, use of real-time facial recognition in law enforcement is not limited to public camera feeds. The London Metropolitan police admitted to supplying images for facial-recognition scans performed on a privately owned estate. In the United States, police departments in Detroit and New York City have used the technology on video or images obtained from CCTV systems of private businesses.

Education

In the education sector, facial recognition is used for access control, where the technology is installed at building entrances and exits to control and monitor access by students and visitors as well as to identify potential security risks. It is also used for educational administrative tasks such as taking attendance, assessing the attentiveness or emotional state of students, and monitoring examinations. In Europe, the Swedish Data Protection Authority (DPA) fined a

1 Kenneth C. Laudon, "Data quality and due process in large interorganizational record systems," Communications of the ACM, January 1986.

school for implementing a pilot of facial-recognition technology to track students' attendance. Though the school obtained permission from students and their parents, the DPA found the pilot violated several articles of the EU's General Data Protection Regulation. In the United States, a high school in Lockport, New York, faced a statewide backlash for installing facial-recognition technology for security purposes.

Transportation

Facial-recognition technology is used at ports of entry and in public transportation systems. In China, it is integrated into bus and rail transit entries to scan passengers' faces instead of physical tickets or digital ticket codes, and similar uses are being piloted in Kazakhstan. In Argentina, the Buenos Aires subway system's cameras use the technology to monitor footage for individuals on a government watch list. In New York City, facial recognition is used to detect faces on display monitors to deter fare evasion. The city has also piloted the technology at its bridges and tunnels to identify drivers with outstanding warrants and traffic violations as well as to match driver's license images with vehicle occupants.

Some U.S. jurisdictions and countries are also using or considering integrating facial-recognition technology into the administrative practices of transportation agencies. For example, Minnesota had proposed legislation that would require its use as part of the application process to obtain a driver's license and state identification card, and Australia had proposed legislation to allow government agencies to use facial recognition to detect whether a person has multiple driver's licenses.

Housing

Commercial security systems that include facial recognition, such as Amazon's Ring and Stonelock's Smart Terminal System, have become a common feature in private residences; but facial-recognition entry systems for tenants of public housing buildings is also an emergent use. In the United States, facial recognition is installed to monitor and regulate entry to government-managed public and affordable housing complexes in Detroit and New York City. In Russia, the Moscow local government has announced a city-wide deployment of live facial recognition on public CCTV cameras and surveillance systems at the entrances of most apartment buildings.

Migration and Immigration

In the United States, federal immigration authorities have used facial recognition and other biometric technologies, though there is debate over whether their uses are limited to what has been publicly disclosed. The Customs and Border Protection agency oversees the Biometric Exit Program, in which facial recognition is used to verify individuals with corresponding passport information for expedited screenings, and the Immigration and Customs Enforcement agency claims that the technology's use is limited to special agents investigating child exploitation and cybercrime. However, some allege that the agency is using facial recognition for surveillance to aid arrests and deportation.[2] The European Union also uses facial-recognition technology similar to the Biometric Exit Program at ports of entry to verify individuals' identity for visa applications and asylum requests, the use of which is closely regulated by several laws. Several other countries, including Turkey and Israel, use the technology for border security and checkpoints.

Policy and Regulation

Over the last decade, national, state, and local governments have introduced or enacted legislation that seeks to mitigate or address risks and harms associated with the use of facial-recognition technology in the public sector. Civil society and the research community have also proposed legislative and regulatory interventions seeking to address privacy, bias, and other human and civil rights concerns associated with government use of the technology. The scope and reach of these

2 Mijente, the National Immigration Project, and the Immigrant Defense Project, Who's Behind ICE? The Tech Companies Fueling Deportations, October 2018.

measures vary significantly. Some seek to evaluate the risks, benefits, and trade-offs of facial recognition in order to determine an appropriate regulatory framework, while others seek to create specific limitations or use requirements in the hope of preventing or at least limiting the most harmful outcomes.

Moratoriums and Bans

With growing public concern and mounting evidence of adverse effects, legislative proposals for bans or moratoriums on the use of facial-recognition technology are becoming more prevalent, but they vary in scope. Bans are official legal prohibitions on use, whereas moratoriums are temporary legal prohibitions that typically end at a predetermined date and/or when certain conditions are met. These measures can be unconditional (that is, applying to all government uses), sectoral, or limited to specific uses.

Unconditional Bans

In the United States, nine jurisdictions have enacted unconditional bans on government use of facial-recognition technology, most of which include private rights of action or statutory damages for individuals harmed by violation of these laws.

In 2019, San Francisco became the first jurisdiction to ban municipal use of facial recognition. However, it is not an unconditional ban since it includes an exemption for inadvertent access to or receipt of information from the technology and a provision that allows the sheriff and district attorney to ask the Board of Supervisors for exemptions to perform investigative or prosecutorial functions with an explanation of how compliance with the law will obstruct either function.

These exemptions are notable because they allow uses or information sharing that can undermine the intentions of the law. For example, if businesses or residents of San Francisco use camera-enabled doorbells and security systems that include facial-recognition analysis, then private companies that manage these technologies can share information with law enforcement without violating the ban. Additionally, the law does not prevent law-enforcement bodies in San Francisco from outsourcing facial-recognition analysis to other jurisdictions, such as federal or neighboring municipalities.

In June 2020, Boston passed a ban that prohibits the use of the technology by any city official or entity as well as obtaining facial-recognition analysis or use via agreement or request of a third party. This aims to address loopholes identified in the San Francisco law. There are also several proposals in Massachusetts seeking statewide bans on government use.

Sectoral Bans

Globally, several jurisdictions have taken a sectoral approach to bans and moratoriums on facial recognition. There are laws and pending legislation proposing bans or moratoriums on its use in education, housing, and law enforcement. Although there are few proposals regarding the use of facial recognition in the educational sector, the state of New York has passed a statewide moratorium on the use of biometric technologies, including facial recognition, in schools until 2022. This law also directs the state's Education Department to study issues regarding the use of biometric technologies in schools and draft potential regulations.

In the United States, there is pending legislation at the federal, state, and local levels proposing bans or moratoriums on the use of facial recognition in housing, particularly in public or government-subsidized housing. For example, the federal No Biometric Barriers to Housing Act prohibits it in housing units that receive funding from the Department of Housing and Urban Development and it directs the department to release a report on the use of facial recognition in rental housing units. Yet, some housing and civil rights advocates have noted that this proposal and others include loopholes that permit this through third-party cooperation. Other housing-related proposals seek to prevent landlords from mandating the use of facial recognition for tenants to access their homes, citing how disproportionate error rates can create unnecessary barriers for residents and accelerate gentrification.

The most prominent sectoral approach regards the use of facial-recognition technology in law enforcement. In the United States, there are several laws and legislative proposals banning this, including the federal Facial Recognition and Biometric Technology Moratorium Act of 2020, which also prevents the use of federal grants for state and local acquisition or use of the technology. After initially ruling out previous proposals, the European Union is once again considering a ban on facial recognition after the European Parliament's civil liberties committee recommended a ban on law-enforcement use. Proposals targeting the use of facial-recognition technology in law enforcement are common because of the difficulty in monitoring and enforcing the various legal standards police should follow in addition to the civil liberties risks posed by noncompliance, such as unjust and discriminatory surveillance. Yet, it has been shown that if these proposals are not carefully drafted, law-enforcement bodies may be able to circumvent such efforts.

Specific Uses

There are also laws and proposals that seek to ban or limit the integration of facial recognition in other public technologies like police body cameras and public Wi-Fi kiosks. In the United States, California, New Hampshire, and Oregon have passed laws banning the use of facial recognition on police body cameras, and some local police departments have formal or informal policies with similar prohibitions. In New York City, the privacy policy for the public Wi-Fi kiosk, LinkNYC, includes a provision stating that facial recognition will not be used, though this can be revised by city officials or the vendor. In Los Angeles, the police department has banned the use of drones equipped with any kind of facial-recognition software.

Standards, Limitations, and Requirements Regarding Databases or Data Sources

Instead of outright banning the use of the technology, some proposals seek to create standards, requirements, and/or limitations regarding the data sources and databases used to develop or perform facial-recognition analysis. Following a report detailing the use of poor-quality and flawed photos of suspects for facial recognition analysis in law enforcement, the Center on Privacy and Technology at Georgetown Law recommended best practices that can be adopted as departmental or jurisdictional policy regarding data sources. The recommendations include prohibiting the use of artist or composite sketches and celebrity look-alike probe images, as well as establishing minimum photo-quality standards (such as pixel density and percentage of the face that must be visible in the photo).[3] These proposals seek to reduce the risk of suspect misidentification and to increase internal oversight mechanisms.

There are also several proposals that seek to impose use requirements or limitations regarding certain government databases that can be used to perform facial-recognition analysis. Most of these proposals seek to mitigate or address privacy concerns about government misuse of sensitive data within certain databases, or bias concerns that are exacerbated when such analysis is performed using certain databases.

In the United States, there are proposals that create use requirements and limitations on the state driver's license databases after it was revealed federal immigration agencies used facial-recognition technology such databases without the knowledge or consent of states or drivers. For example, Utah originally considered creating a warrant requirement for federal immigration agencies to use its driver's license database; but that proposal was later amended to explicitly ban the use of facial recognition for civil immigration enforcement. Other states have similar laws or proposals that expressly limit federal immigration and law-enforcement bodies access to driver's license databases for facial-recognition use. Some advocates and researchers have called for policies that prohibit the use of facial-recognition technology on mugshot

3 Clare Garvie, Garbage In, Garbage Out: Face Recognition on Flawed Data, Georgetown Law, Center on Privacy and Technology, May 16, 2019.

databases since these are unreliable (for example, photos are not purged if the person is not convicted of a crime) and disproportionately comprised of Black and Latinx individuals.

Data Regulations

Since government use of facial-recognition technology inherently involves the processing of personal data, several laws that attempt to regulate data collection and processing also apply to its use by governments.

Europe

The European Union's General Data Protection Regulation (GDPR) addresses data protection and privacy issues in Europe by providing various legal procedures and requirements concerning the collection and use of sensitive and personal information, and it can be applied to the processing of data captured by facial-recognition technology. Member states have also enacted national laws to implement certain elements of the GDPR and to inform national enforcement. In 2019, Sweden's Data Protection Authority issued its first fine for violation of the GDPR on after a high school launched a facial-recognition pilot program to track students' attendance. That same year, the United Kingdom's Information Commissioner's Office issued an opinion clarifying how use of facial recognition in law enforcement should be understood and regulated.[4] This opinion made several pronouncements, but two are pertinent to understanding the application of the Data Protection Act 2018, the United Kingdom's implementation of the GDPR. First, it found that sensitive processing, which triggers Data Protection Act 2018 enforcement, relates to all facial images captured and analyzed by software, and that it occurs irrespective of whether the image captured matches a person on a government watch-list or if the image is deleted within a short time. Second, the opinion found that the GDPR applies to the whole process of live facial recognition, including considerations about deployment, compilation of watch-lists, and processing and deletion of the data.

Canada

Canada's Personal Information Protection and Electronic Documents Act regulates how the private sector collects, uses, and discloses personal data, while the Privacy Act regulates government use of personal data. Most provinces and territories have enacted privacy laws that mirror the Personal Information Protection and Electronic Documents Act and have empowered commissioners or ombudspersons to interpret and apply all relevant laws. In compliance with the Privacy Act, institutions can complete privacy impact assessments for programs or services.

Since 2004 the federal Office of the Privacy Commissioner has reviewed privacy impact assessments for Passport Canada's project that uses facial recognition to detect fraud in passport applications. Since 2012, the Office of the Privacy Commissioner has made several recommendations on how the project can mitigate the privacy and bias risks associated with its use of facial recognition.[5] These included providing statistical evidence to demonstrate the need for the program, implementing regular monitoring and updates to the system to reduce biased performance, and encrypting all data in the facial-recognition database. In 2012, the British Columbia Information and Privacy Commissioner decided that facial recognition cannot be used to identify rioters without a court order, after a private insurance company offered to give police access to its system when riots occurred in Vancouver following a hockey game. In 2020, the federal Office of the Privacy Commissioner announced an investigation under the Privacy Act into the Royal Canadian Mounted Police's use of Clearview AI's facial-recognition technology, and it also announced a joint investigation of Clearview AI with its counterparts in Alberta, British Columbia, and Quebec. These investigations resulted

4 Information Commissioner's Office of the United Kingdom, ICO statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition, January 24, 2020.

5 Office of the Privacy Commissioner of Canada, Automated Facial Recognition in the Public and Private Sectors, March 2013.

in Clearview AI ending all offerings of its facial-recognition services in Canada.

United States

In the last two decades, several jurisdictions in the United States have enacted laws that regulate the collection, use, and disclosure of biometric data, which can implicate the use of facial-recognition technology. Most of these laws apply to the private sector; but as private litigation under these statutes increases, they can include government use of facial recognition as it relates to preexisting private-public partnerships. In Illinois, a group of plaintiffs recently brought a legal action against Motorola and Vigilant, alleging violations of the state's Biometric Information Privacy Act. The lawsuit alleges that the companies used millions of images from the state's mugshot database to provide a "facial search engine" and other facial-recognition products to various law-enforcement agencies. Although the case is still pending, the plaintiffs are seeking various forms of relief that can affect third-party agreements and private-public partnerships regarding facial recognition.

Oversight and Use Requirements

There are proposals that seek to create use requirements for facial-recognition technology and oversight mechanisms that can mitigate abuse, misuse, or harmful outcomes. Those offering use requirements can be broken into two categories: policies that seek to provide greater transparency regarding current and prospective government uses of facial recognition, and policies that seek to impose requirements on government agencies using the technology.

Transparency Requirements

In the United States, there are numerous bills and laws that seek to provide the public with more information regarding government use of surveillance technologies, which includes facial recognition. Some of these are part of a national effort to enact municipal or state-level transparency laws that provide public or legislative oversight, and in some cases require approval before an agency can acquire or use a surveillance technology. Yet, some have noted that the efficacy of these transparency laws can depend on whether the parts of government with oversight authority are cooperative and supportive of the law, and whether there is a robust advocacy community to provide external pressure or accountability. Other proposals specifically regarding the use of facial-recognition technology mandate annual public reporting on its use by government. For example, Utah's facial recognition legislation provides that only the Department of Public Safety is authorized to use facial recognition and requires it to annually report on the type of crimes the technology was used to investigate and the number of likely matches provided for each type of crime.

Use Requirements

Policies that impose requirements on government agencies using the technology are more varied. While some of the abovementioned proposals specifically target the data and images used to perform facial-recognition analysis, the following proposals target government practices and procedures. They include notice and consent, training, and documentation requirements.

In the United Kingdom, the London Metropolitan police is required to post online where facial recognition will be used before deployment, to place signs in and around areas where the technology is used, and to make officers available to talk to the public about facial recognition.

In the United States, there are several proposals regarding training in the use of facial recognition. Utah's legislation requires law-enforcement personnel to be trained in how to make facial recognition comparisons and identification, in addition to completing implicit bias training. Some have also recommended that law-enforcement officials should receive frequent and targeted training in their legal obligations (for example, *Brady* requirements to disclose exculpatory evidence and probable-cause standards) and best practices regarding the use of facial recognition. The Utah legislation also provides documentation require-

ments for the use of facial recognition. It requires law-enforcement personnel to provide a statement of the specific crime and a factual narrative to demonstrate that the suspect is connected to a crime before facial recognition can be used.

Oversight Mechanisms

Finally, there are proposals that impose oversight or review procedures for government use of facial recognition. In the United States, some proposals require government agencies to seek a second opinion when facial-recognition analysis suggests an identification match and others require human review of such analysis or decision made relying on it. In the United Kingdom, there are governance and oversight requirements before, during, and after the deployment of facial recognition. For example, the purpose of a deployment must be authorized before use and a potential match made by facial-recognition technology must be submitted for human review. Researchers have also advocated for and noted that some departments have formally and informally practiced double-blind confirmation requirements in which facial-recognition analysis as an investigative lead can only be used when two analysts independently conclude the same photo as a possible match.

Government Commissions, Consultations, and Studies

Though often paired with bans, moratoriums, and other restrictive regulations, government-mandated commissions, consultations, and studies are a common and often preliminary proposal regarding facial recognition. Australia's Human Rights Commission has published a discussion paper on artificial intelligence that includes a proposal to introduce a moratorium on the use of facial-recognition technology until an appropriate legal framework is put in place. The proposal also declared that the commission and the Office of the Australian Information Commissioner should consult experts to develop this legal framework. Similarly, in the United States, the Ethical Use of Facial Recognition Act prevents federal agencies, employees, and contractors from using the technology without a warrant until a congressional commission recommends a legal framework for its government and commercial use.

Conclusion

In the United States, Europe, and elsewhere around the world, policymakers have awoken to the risks that facial-recognition technology presents to human rights and civil liberties. While existing policy frameworks may address some of those risks in certain jurisdictions, the technology remains largely ungoverned. As policymakers seek to address these risks in a more comprehensive manner, they should seek out an active dialogue with their counterparts in other jurisdictions, to broaden their understanding of possible policy remedies and refine their own proposals. This policy brief aims to provide a foundation to support such dialogue.

February 2021

About the Author(s)

Rashida Richardson is a visiting scholar at Rutgers Law School and Rutgers Institute for Information Policy and Law, where she specializes in race, emerging technologies, and the law.

About GMF Digital

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) works to support democracy in the digital age. GMF Digital leverages a transatlantic network of senior fellows to develop and advance strategic reforms that foster innovation, create opportunity, and advance an equitable society.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org