Facial Recognition Technology Regulation
A Practical Guide for Congress
Congress Should Act Now on Facial Recognition Technology

The dearth of accountability safeguards as government agencies acquire facial recognition technologies prompted Open the Government and a growing list of civil society groups to urge Congress to swiftly regulate the technology. New policies and research suggest there is increasing need to establish protections for facial recognition technology. San Francisco, Somerville, Massachusetts and Oakland have banned government agencies from adopting the technology amid widespread concerns about threats to civil rights and liberties. Compounding these concerns is the quiet adoption of facial recognition technology as a surveillance tool to secretly monitor citizens and non-citizens alike. A yearlong investigation by the Center on Privacy and Technology at Georgetown Law uncovered a startling statistic: images of over half of all American adults are in a facial recognition database accessible by law enforcement.

In fact, several members of Congress have first-hand experience with the flaws of facial recognition technology. In 2018, the American Civil Liberties Union (ACLU) ran a test of Rekognition, Amazon’s facial recognition product, and found it incorrectly identified 28 members of Congress as individuals who had been arrested for a crime when matched against a database of 25,000 publicly available arrest photos. According to the ACLU’s experiment, 40 percent of the false matches generated by Rekognition were of people of color, despite people of color only composing 20 percent of Congress.

Open the Government’s Sunshine Week report, Government Inc.: Amazon, Government Security & Secrecy, details the substantial dangers of facial recognition systems when government agencies purchase the technology without full transparency and adequate safeguards in place to protect those who will be harmed when it fails. Our report also described the numerous mechanisms by which government agencies quietly acquire powerful technology under non-disclosure agreements (NDAs).

The time for Congress to check the growth of facial recognition technology on a national scale is now, before the technology becomes too ubiquitous for Congress to rein in. This is an opportunity for Congress to develop effective legislation that protects civil liberties and strengthens accountability.

Protecting the Right to Due Process

Lack of federal laws or regulations governing the use of facial recognition exacerbates civil rights concerns. Constitutional precedents on the warrantless use of facial recognition by law enforcement do not exist, and courts have yet to address whether use of these technologies constitute a search under the Fourth Amendment. Despite concerns about due process rights, there are no requirements that individuals charged with crimes be notified when facial recognition technology identifies them as suspects. Absent significant judicial review, Congress should use its legislative powers to regulate the proliferation of this technology.

The Technology is Cloaked in Secrecy

The acquisition of facial recognition technology is outpacing existing legal protections, and even where meager legal protections exist, the secretive nature of facial recognition often allows for circumvention of the law. For example, to date the Federal Bureau of Investigation (FBI) has failed to meet basic transparency requirements and conduct privacy assessments as mandated by federal law for its Next General Identification (NGI) database and its use of face recognition. The NGI database pulls from state and local databases, and provides law
enforcement agencies access to criminal and personal data. As more police departments acquire facial recognition technology, Americans are increasingly at risk of becoming victims of privacy abuses as their personal information falls into the dark hole of government data sharing without their knowledge.

On the state and local level, NDAs between companies and public officials restrict the public’s right to know about policing in their communities. Documents released by Orlando police revealed that Amazon required city officials to sign a NDA to keep details about Rekognition’s pilot from public scrutiny. Similarly, the Washington County Sheriff signed a NDA with Amazon. In Washington, D.C., police withheld records from members of Congress on their use of facial recognition technology because their agreements with the company, MorphoTrak, were stamped “Confidential and Proprietary.”

These NDAs pose a major threat to transparency and accountability as advocates rely on disclosures to fully expose the risks inherent in facial recognition technology and its associated harms.

Mass Surveillance

Real-time tracking by police enables law enforcement to identify groups of people, persons of interest, and patterns of movement, and poses a significant risk to freedoms of speech and assembly. Nonetheless, surveillance technology is spreading quickly and secretly among law enforcement across the country. According to a study by Georgetown, at least a quarter of all law enforcement agencies have access to a facial recognition system. The rapid influx of the technology means that police are using personal data without regulation. In New York City, for example, IBM collaborated with the New York City Police Department (NYPD) to develop a face classification system from thousands of hours of NYPD surveillance footage that included “ethnicity search” as a custom feature. Only after a Congressional inquiry and Freedom of Information Act (FOIA) requests did we learn in 2017 that police in Washington, D.C. used a facial recognition system which allowed the department to query FBI databases without any Congressional policy guidelines in place.

On the federal level, agencies such as Immigration and Customs Enforcement (ICE) are using or considering using Rekognition. Advocates have expressed concern that facial recognition technology in the hands of ICE’s Enforcement and Removal Operations can lead to constant automated surveillance of public spaces patronized by undocumented immigrants, changing ICE’s role from an enforcement agency to a real-time surveillance apparatus. Surveillance of sensitive locations like medical facilities, places of worship, courtrooms and schools could discourage people from seeking out vital services for fear of being identified and detained.

Where facial recognition technology is used

- Law enforcement agencies around the country, including Orlando, New York City, Washington County, Oregon
- Federal Bureau of Investigation
- Immigration and Customs Enforcement
- Department of Homeland Security
- U.S. Customs and Border Protection, including dozens of airports
Implications for Civil Rights

Independent studies show problematic racial and gender inequities associated with facial recognition technology, illuminating the need for companies to address inherent bias and discrimination within the systems. Algorithms used by IBM and Microsoft correctly identified 99 percent of white men, but misidentified one in three dark-skinned women, according to a February 2018 report from MIT and Stanford researchers. Joy Buolamwini, one of the co-authors from MIT who testified at a Congressional hearing on facial recognition, showed how the technology misclassified famous African-American women, including Oprah Winfrey, as men.

On the law enforcement front, many police departments enter booking photos into their facial recognition databases. This can be problematic when the departments do not purge innocent people or misidentified suspects from the data. Additionally, criminal justice experts note that racially biased police practices in this country mean criminal databases already include a disproportionate number of people of color. Facial recognition then exacerbates racial disparities by misidentifying minority groups at higher rates. There are currently no requirements that law enforcement officers notify defense attorneys if their clients become the suspect of an investigation because of facial recognition technology.

Meaningful Federal Oversight is Lacking

Until there is federal action, advocates are looking to lawmakers at the state and local levels for protections against the spread of surveillance technologies. Proposals range from explicit bans to regulations that would curb potential abuse. San Francisco’s Stop Secret Surveillance Ordinance banning the purchase of facial recognition technology was the first to go into effect. Somerville’s Face Surveillance Full Ban Ordinance passed through city council and so did Oakland’s. Washington State has proposed legislation to regulate the technology.

While a few cities are considering legislation to ensure residents have influence over decisions on whether and how local police use surveillance technologies in their communities, in the vast majority of cases cities are acquiring surveillance technology without the knowledge or consent of residents or lawmakers. Importantly, none of the restrictions or oversight measures at the state and local levels provide oversight over the use of facial recognition technology by federal agencies. Congress is constitutionally required to exercise oversight by developing legislation that will fill the gap.

Criteria for Facial Recognition Technology Legislation

Federal, state and local government entities must establish strict safeguards before purchasing and deploying artificial intelligence-powered technologies, including facial recognition systems. To exercise oversight, they must mandate transparency from companies regarding the capabilities and limitations of the technology, including strengthening public records and mandatory reporting laws.

Governments have a duty to protect the public by establishing limits on collection, use, sharing, and retention of data by government technology contractors. They must investigate whether facial recognition and other technologies have a disparate impact on communities of color. They must provide the opportunity for public notice and comment prior to the procurement of facial recognition software.

Building on this general framework, the following are recommendations for Congress that can help inform legislative facial recognition proposals.
Critical Congressional Safeguards: Key Concerns about Facial Recognition Technology & Remedies

**Issue**

Bias and inaccuracy exist in facial recognition services used by law enforcement.

**Remedy**

- Condition funds to acquire facial recognition services on accuracy and bias testing by independent third parties.
- Require law enforcement agencies to establish strict safeguards and privacy standards before purchasing and deploying facial recognition software.
- Require federal law enforcement agencies that pilot facial recognition to undertake meaningful human review of results prior to making final decisions on whether to adopt the technology. Review should include:
  - Examination of potential violations of human or fundamental rights; personal freedom; or privacy.
  - Examination of risks that the technology could be used to track people based on race, ethnicity, religious or political views.
- Condition federal assistance for facial recognition technology on the public release of internal audits.
- Require the National Institute of Standards (NIST) test all facial recognition software for accuracy before acquisition.
- Support comprehensive research into the algorithmic sources of racial bias in facial recognition tools by NIST and academic institutions, and require release of that research to the public.
- Require facial recognition tools to meet specific standards before market release.

**Issue**

Facial recognition technologies are complex and inaccessible to lawmakers and the public.

**Remedy**

- Mandate transparency from companies regarding the capabilities and limitations of facial recognition technology in terms that customers, consumers and the public can understand.
- Create rules and allocate resources to incentivize lawmakers to employ staffers with the relevant technical expertise needed for effective oversight in order to close the technological expertise gap that typically exists between the public and private sectors.

**Issue**

Unlawful surveillance threaten civil rights and liberties.

**Remedy**

- Require judicial authorization based on probable cause to condition use of facial recognition technology in order to protect against unlawful surveillance.
- Require the public release of technology policies that address privacy and data retention concerns prior to allocating funding for agencies’ acquisition of facial recognition.
Issue

FOIA applies to government agencies not private contractors.

Remedy

- Reform FOIA to ensure government contractors provide the information necessary for the government to respond to requests related to facial recognition and surveillance technology systems. The much-needed reform will ensure the public is empowered with adequate information to understand the use and impact of surveillance technology.

Once Congress embarks on a comprehensive oversight plan that will hold technology contractors accountable when deploying innovative facial recognition technology, the public’s confidence in the systems will increase and the society can fully realize the technology’s vast potential.

Companies and Technology Contractors Checklist

Has the company taken specific measures to mitigate harm of facial recognition services, by:

- Stopping the sale of facial recognition technology to government agencies until mechanisms and safe guards are in place to prevent abuse?

- Improving transparency reporting to meet public demand for information on invasive surveillance technology and AI use?

Commit to strengthening accountability to the public

- Has the company developed and publicly released AI principles and a policy framework, confirming the following?
  - The company will not pursue technologies whose purpose contravenes widely accepted principles of international law and human rights.
  - The company will not pursue technologies that gather or use information for surveillance violating internationally accepted norms.
  - Neither the company nor its contractors will work with clients that violate international human rights law.
  - The company will consider fully how use of its AI or machine learning technology could be weaponized or used to support lethal force, even if the technology is not expressly created for that purpose.

- The company commits to transparency and review regarding contracts with government agencies, in the United States and beyond. It will also require a commitment from national security agencies specifying how their technologies will be used before a government contract is issued.

- Listen and respond to the demands of the employees and shareholders, provide protections for conscientious objectors, employee organizing, and ethical whistleblowers.

- Expand whistleblower protection to non-full time employees of tech companies such as contractors.

- Refrain from implementing nondisclosure agreements or other legal barriers that stand in the way of accountability in the public sector.

- Commit to improving the explainability of AI and machine learning systems to enable oversight and accountability.
Contact Us

For more information on any aspect of this guide, or if you would like more information on how Open the Government can assist your office, please contact us at (202) 332-6736 or info@openthegovernment.org.

Visit our website at www.openthegovernment.org

Engage with us on social media
Endnotes


3 ACLU public records requests to Orlando Police Department related to Amazon Rekognition facial recognition service, ACLU, January 18, 2018, available at: https://www.aclunc.org/docs/20180522_ARD.pdf#page=7

4 Letter from the DC Office of the Attorney General, to the U.S. House Committee on Oversight and Government Reform, June 7, 2017.


