CENTER FOR DEMOCRACY & TECHNOLOGY

Recognizing the Threats: Congress Must Impose a Moratorium on Law Enforcement Use of Facial Recognition Tech

October 14, 2021

The House has largely been locked in partisan conflict since the January 6 insurrection, but when it comes to concerns about law enforcement use of facial recognition, it can be difficult to tell the difference between Republican and Democratic representatives. In July, the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on this subject, and members of both parties all appeared to agree that law enforcement use of facial recognition technology poses serious threats to privacy, civil liberties, and civil rights.

The Center for Democracy & Technology (CDT) has joined with allies in calling for Congress to enact a moratorium on the use of facial recognition for law enforcement and immigration enforcement purposes. CDT has long urged that this technology poses severe risks to civil liberties and civil rights, and that congressional oversight and legislation are needed to address these risks. But what, if anything, will Congress actually do?

A bill already introduced in Congress — the Facial Recognition and Biometric Technology Moratorium Act — would impose a moratorium on federal government use of facial recognition technology until Congress can enact a comprehensive set of rules to mitigate the threats to human rights. This proposed legislation — which would cover all government use of biometric surveillance tools — provides a very helpful framework for addressing the risks from law enforcement and immigration enforcement use of facial recognition.

Risks of Law & Immigration Enforcement Uses of Facial Recognition

CDT has focused on calling for a moratorium on the use of facial recognition in the law enforcement and immigration context, where the threats from biometric technologies are most severe and the need for guardrails is most urgent. Earlier this year, CDT joined with over 40 other civil society organizations in outlining Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology. The coalition statement presents six critical concerns raised by law enforcement use of this technology:

- **Disproportionate harm to Black and Brown communities regardless of technical accuracy**: Even if we could eliminate the gender and racial bias demonstrated by facial recognition technology, its use can exacerbate the disproportionate harms faced by Black and Brown communities that are already subject to overpolicing.
- **Privacy threats**: Law enforcement use of facial recognition permits invasive and persistent tracking and targeting that threatens individual privacy.
- **Chills First Amendment activities**: Use of facial recognition for law enforcement purposes can chill free speech and other protected First Amendment activities, including political protests and religious activities.
- **Lack of due process**: Law enforcement use of facial recognition can violate due process rights and procedural justice, in particular where police and prosecutors refuse to disclose when and how the technology has been used.
- **Lack of consent**: Facial recognition systems used by law enforcement have often relied upon faceprints obtained without consent (e.g., Clearview AI).
- **Biased and inaccurate algorithms**: Facial recognition algorithms, and the ways in which they have been used by law enforcement, are biased against women and people of color.

The concerns about discrimination are particularly acute. Studies have documented how facial recognition software is biased against women and people of color. Groundbreaking research by Joy Buolamwini and Timnit Gebru showed error rates as high as 34.7% for detecting the faces of darker skinned women, as compared to only 0.8% for detecting light skinned males, and a report by the National Institute of Standards and Technology found that facial recognition algorithms were 100 times more likely to produce false positives for people from African or Asian countries as compared to lighter-skinned people from European countries.

Such disparate error rates can have dire consequences in the law enforcement context. Reporting has already documented three cases in which Black men have been wrongfully arrested based on flawed facial recognition systems, including Robert Williams, who provided compelling testimony in the July House hearing.

Current Law Enforcement Uses of Facial Recognition

Law enforcement and immigration enforcement use of facial recognition is widespread and growing, despite a lack of safeguards to regulate these uses. Two studies by the Georgetown Law Center on Privacy & Technology demonstrate the pervasive intrusiveness of law enforcement facial recognition systems in states across the country, as well as the lack of rules to govern such programs. At the federal

level, an August 2021 GAO report outlined the use of the technology at 24 federal agencies, including six that use it in domestic criminal investigations and two that use it for border security and immigration enforcement. The study also reported that ten agencies plan to expand their use of facial recognition.

Earlier this past summer, a June 2021 GAO report focused on law enforcement use revealed that over a dozen federal agencies are not even aware of what facial recognition systems they are using for law enforcement purposes. The June report is particularly concerning, since agencies that are unaware of their own use of facial recognition technologies are unlikely to have taken steps to mitigate the civil liberties and civil rights threats posed by their systems.

Facial recognition can be a valuable tool for law enforcement and immigration enforcement, but when the government seeks to take advantage of "innovations in surveillance tools," it must still comply with constitutional and civil rights safeguards. Where technology gets out ahead of legal protections, it is necessary to press pause on the use of surveillance tools that threaten human rights.

Three major tech companies are already doing so, announcing last year that civil liberties and civil rights risks motivated them to halt their sales of facial recognition technology to law enforcement. IBM sent a letter to Congress stating that it no longer offers its general purpose facial recognition software and calling for "a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies." Microsoft announced that the company would cease selling facial recognition technology to law enforcement until there is a national law governing the technology to protect human rights. And Amazon first imposed a one-year moratorium on police use of its "Rekognition" software, and then extended the moratorium until further notice.

The Facial Recognition and Biometric Technology Moratorium Act Provides a Roadmap for Important Protections

Congressional action to rein in the threats posed by law and immigration enforcement uses of facial recognition technology is overdue, and the Facial Recognition and Biometric Technology Moratorium Act offers a great place to start. The bill would prohibit federal government acquisition and use of biometric technologies including facial recognition, with an exception for situations in which Congress has enacted a specific and robust set of safeguards. So, while Congress grapples with designing guardrails to address the harms that use of facial recognition can cause, federal law enforcement and immigration enforcement agencies would need to cease all use of the technology.

Section 3(b) of the bill lays out the types of safeguards that Congress would need to enact in order to grant an exception to the moratorium; it essentially provides a roadmap for the types of protections that Congress should implement to address the civil liberties and civil rights threats that CDT and our allies have outlined. Specifically, the bill sets out five categories of safeguards that Congress would need to enact in further legislation.

Purpose specification: Legislation must describe the entities permitted to use the biometric surveillance system, the specific type of biometric system authorized, the permitted purposes, and any prohibited uses. Some purposes should simply not be allowed. In particular, as CDT has previously urged, law enforcement should not be permitted to use real-time facial recognition on police body cameras, which would unduly infringe on privacy and free expression. Further, as Privacy International has explained, even if the cameras were unbiased and accurate, integrating facial recognition capabilities "would subvert the purpose of body-worn cameras as a tool of police accountability and transparency by turning them into a tool for mass surveillance." A risk-based approach can help identify other circumstances in which facial recognition should not be allowed.

Some purposes pose significantly less risk, such as where U.S. citizens voluntarily participate in U.S. Customs and Border Protection's (CBP) Global Entry Program and consent to the use of facial recognition to verify their identities and expedite processing when they reenter the country. Such one-to-one matching to *verify* identity is generally more accurate and poses fewer threats to civil liberties and civil rights than one-to-many matching, which is common in law enforcement investigations and attempts to identify an individual from a larger pool.

Use standards: Congress must set standards for use and management of information derived from facial recognition systems, including rules on data retention, sharing, access, and audit trails to mitigate the privacy threats from collection of biometric data. Data retention periods should be no longer than is necessary; although it may be appropriate to retain images in the databases against which "probe" photos are tested for longer than the probe photos themselves, all images should be subject to time limits tied to the purpose for which they are collected and used.

Further, access and sharing should be limited to authorized personnel who require access to perform their duties and have undergone training in the purposes and rules governing the system. The rules should also outline requirements for data security. In light of a data breach involving facial images held by CBP, a Congressional Research Service report recommends that Congress may wish to "pay particular attention to the security of facial recognition and other biometric data."

Audit requirements: Legislation must outline auditing requirements to ensure accuracy, as well as standards for minimum accuracy rates, by characteristics such as gender, skin color, and age. Regular and independent audits can be an important tool in protecting human rights in the context of artificial intelligence such as facial recognition.

The bill specifically states that audits must assess that biometric systems are meeting baseline "accuracy rates by gender, skin color, and age." Under this mandate, no law enforcement or immigration enforcement entity should be permitted to deploy facial recognition, unless and until developers are able to design algorithms that are accurate and no longer biased against women and people of color. Law enforcement and immigration enforcement agencies should also be required to test their algorithms for bias against other marginalized communities, such as people with disabilities, and take steps to cure any such impacts prior to using facial recognition tools.

Accuracy rates will also depend on how agencies actually deploy facial recognition tools. The entities using these tools can set "match thresholds," which determine which images will be returned as a potential match; low thresholds lead to the return of more images as potential matches and more false positive matches, whereas high thresholds will yield fewer potential matches and may increase the rate of false negatives (or undetected matches). Importantly, the bill's audit provision also specifies that Congress must enact requirements for ongoing audits, which would test systems to determine whether accuracy rates remained consistent.

Rigorous safeguards for civil liberties and civil rights: The core and most critical requirement of the moratorium bill's roadmap for protections against the harms of facial recognition technology use is the fourth provision, which mandates rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity. It will be a tall order for Congress to craft comprehensive rules to provide robust safeguards for all of these fundamental rights. Congress would need to devote significant time and effort to this task, including full consultation with affected communities, civil rights and civil liberties groups, and other stakeholders.

We can identify some minimum requirements toward these goals. To safeguard due process, law enforcement must at a minimum be required to provide notice to criminal defendants whenever facial recognition has been used in an investigation. The law should also ensure that there is a meaningful opportunity to challenge any such evidence.

As a preliminary step to protect privacy, Congress should mandate that law enforcement must obtain a warrant based on probable cause before they can seek to identify a criminal suspect or to track any individual's movements using facial recognition. To protect free speech and association, rules would

need to prohibit monitoring people engaged in First Amendment-protected activities, such as the use of facial recognition to identify protestors who are not engaged in unlawful violent activities.

Designing safeguards for racial, gender and religious equity will be one of the most difficult challenges, since even beyond the harms from discriminatory accuracy rates, facial recognition technology in the hands of law enforcement and immigration enforcement can lead to the "automation of racism." Measures like those contained in the George Floyd Justice in Policing Act would help address inequities in policing, providing a baseline for additional protections that should address the further risks from a powerfully invasive technology like facial recognition.

Compliance mechanisms: To fulfill the bill's requirement for compliance mechanisms, Congress would need to ensure that the mandatory audits described above would have consequences. Law enforcement and immigration enforcement agencies should be required to promptly address any deficiencies uncovered in audits, or cease using any systems that failed to comply with the rules developed under the other categories of safeguards.

The compliance mechanisms should also require transparency to the public to promote accountability. This should include regular public reporting by law enforcement and immigration enforcement agencies, describing when and how they use facial recognition. It should also include statistics documenting the performance of those systems, and the number of arrests or enforcement actions that have been based in whole or in part on use of such technologies. In addition, the applicable rules should mandate that if law enforcement or immigration enforcement agents misuse these powerful biometric technologies, they will be subject to disciplinary action.

Beyond the five parts of the moratorium bill's roadmap, another critical requirement for any federal legislation regulating law enforcement and immigration enforcement use of facial recognition is that it must not preclude more stringent state and local restrictions. Since 2019, over a dozen local jurisdictions have imposed bans on law enforcement use of facial recognition technology, and these local governments should be permitted to make such choices for their own communities. The Facial Recognition and Biometric Technology Moratorium Act would go one step further, and would incentivize local governments to develop their own similar legislation. Specifically, the bill provides that, in order for state or local governments to receive federal criminal justice funding under the Byrne grant program, the jurisdiction must impose a moratorium on the use of biometric technologies, subject to the same "exception" provision that applies to the federal government.

Given the severity of the threats from law enforcement and immigration enforcement use of facial recognition, crafting rules to meet all of these goals will not be easily accomplished. Some of CDT's

allies would say it is an impossible task, and all law enforcement use must be permanently banned; conversely, some organizations have called for relatively limited regulations that fail to address the full scope of threats posed by facial recognition technologies. We know that the FBI regularly deploys facial recognition in its investigations, Customs and Border Protection (CBP) uses the technology for border enforcement, and the June 2021 GAO report covers these two agencies and 18 additional federal law enforcement entities that are already using facial recognition technology. So, it is worth using the roadmap in Section 3(b) of the moratorium bill to think through the types of rules that could mitigate the serious threats posed by law enforcement use of the technology.

A Path Forward

As drafted, the Facial Recognition and Biometric Technology Moratorium Act would apply to all government uses of biometric technologies, and not only to law enforcement and immigration enforcement uses. However, some purposes —- such as a system for federal employees to verify their identities through one-to-one matching of images, enabling them to enter their workplaces — pose fewer risks to individual rights than law enforcement investigations. Congress may wish to consider modifying the moratorium bill to focus on law enforcement, immigration enforcement, and other high-risk government uses of biometric technologies.

Further, the White House Office of Science and Technology Policy is working to develop a bill of rights to guard against harms from the use of powerful automated tools, including issuing a call for information from the public on the use of biometric technologies; this effort could also lead to the identification and adoption of critical safeguards.

Nonetheless, Congress should take advantage of the apparent bipartisan consensus on the threats posed by law enforcement use of facial recognition and move forward promptly with a moratorium. There are currently no federal laws that specifically regulate law enforcement use of facial recognition technology. It is time for that to change.