

LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY MUST BE REGULATED NOW. HERE'S HOW.

THE ISSUE

Law enforcement agencies across the country are adopting and using face recognition technology (FRT) without explicit statutory or democratic authorization, and in ways that pose real risks to our civil rights and civil liberties. If policing agencies are going to continue to use this technology, such use must be subject to carefully-considered regulatory guardrails. This brief explains the concerns with FRT and describes what regulation is needed.

PERSISTENT ACCURACY AND BIAS CONCERNS

FRT presents significant accuracy and bias concerns. Because of inadequate or nonexistent testing, the accuracy of FRT as used by law enforcement is entirely unproven. Research has shown that many algorithms may exhibit higher error rates when attempting to identify women, minors, and especially people with darker skin.

RESEARCHERS CALL OUT ALGORITHMIC BIAS

The issue of demographic bias in face analysis algorithms gained significant attention with the publication of a [2018 MIT study](#) by Joy Buolamwini and Timnit Gebru, which found that several leading face classification algorithms were much less accurate at predicting the gender of people with darker skin tones.

Although this groundbreaking study examined the accuracy of face classification algorithms and not face recognition algorithms—related, yet different technologies—it raised awareness that demographics like skin color can significantly affect the accuracy of algorithms that analyze face photographs.

Although testing under laboratory conditions shows some improvement in the quality of many FRT algorithms, we have no information about how this technology operates under real-world conditions. The two are not comparable and one cannot assume the performance in the lab tells us much about performance under actual law enforcement conditions.

Racial bias concerns are not limited to the algorithms; rather, racial disparities in the criminal legal system can infect the entire FRT process. Communities of color have been and continue to be subject to disproportionate criminal enforcement—from stops, to searches, to arrests. This means that people of color are overrepresented in many of the databases police use to conduct FRT searches. Taken together, excessive enforcement actions against people of color combined with searching databases containing disproportionately more faces of color means these communities will bear the brunt of FRT’s harms. Already, unregulated police use of FRT has contributed to misidentifications that led to false arrests. To date, each person wrongly arrested because of FRT has been a Black man.

RISKS TO FREE EXPRESSION

Police also have used FRT to target individuals exercising their First Amendment rights, including at racial justice protests and during Juneteenth celebrations, raising serious concerns about creating a chilling effect on constitutionally protected activity.

PRIVACY INVASIONS AND SURVEILLANCE STATE FEARS

FRT use against Black community activists also evokes historical government surveillance practices targeting political dissidents and marginalized communities, from the FBI’s spying on civil rights leaders in the 1960s to the NYPD’s secret videoing of mosques after 9/11.

When it comes to surveillance, FRT could supercharge current police capabilities by facilitating searches of databases of millions of faces (including social media images scraped from the internet without individuals’ consent) in a matter of seconds.

Combined with ever-increasing networks of public and private surveillance cameras, FRT can enable governmental surveillance and tracking with unthinkable speed at an unprecedented scale, with no ability to opt out. After all, you can’t leave your face at home. History makes clear that without meaningful legislation reining in police use of FRT, there will be misuse.

MONITORING FREE EXPRESSION






In the summer of 2020, in the wake of the killing of George Floyd, community activists in Fort Lauderdale, Florida, organized a Juneteenth Block Party that included live music and a “healing space.” Some attendees marched with a banner calling to defund the police. Despite the fact that the gathering remained entirely peaceful, subsequent [investigative reporting](#) revealed that the Fort Lauderdale police ran face recognition scans to identify event organizers. In response to this revelation, one activist asked why the police resorted to FRT when “they could be working with me to better the both of us.”

THE SOLUTION

We need a new approach: one that is informed by the democratic process and that ensures police only may use FRT if it makes the public safer, if the public actually wants it, and if the technology does not perpetuate harms like racial injustice and invasions of privacy. Legislative bodies should enact comprehensive regulation to strike this balance.

Our legislative checklist presents a way forward, namely a set of minimum guidelines for comprehensive regulation of this powerful technology.

WHAT THE CHECKLIST DOES

-  **Establishes democratic authorization as the baseline.** The checklist insists that a regulatory framework, approved by a democratically accountable body, must be in place for police to use FRT.
-  **Requires absolute transparency about police use of FRT.** The checklist establishes reporting and auditing requirements to enable public oversight and evaluation of its benefits and harms.
-  **Limits the uses of FRT.** The checklist sets strict limits on permitted uses of FRT, restricting searches to certain serious offenses and clarifying which uses are never allowed, like using FRT for surveillance. For permitted uses, the checklist outlines specific guardrails for deploying FRT, such as requiring a warrant to conduct searches. These limitations ensure that legislation can allow FRT as a valuable investigatory tool and still safeguard the public's constitutional rights.
-  **Mandates testing protocols and accuracy benchmarks.** The checklist ensures that law enforcement are permitted to use only the most accurate technology available, as verified through independent, expert testing. Additionally, it includes a requirement that these systems be tested in real-world conditions—"operational testing"—to make sure the public knows whether and how well this technology actually works.
-  **Requires training for officers using and analyzing FRT.** A key component of the checklist requires that police officers who analyze and use FRT results receive adequate training. Training officers on the sources of error and bias that can impact the process will help ensure accurate use.

CLEARVIEW HAS YOUR FACE

Face recognition company Clearview AI has [made headlines](#) due to its uniquely invasive process for creating databases for face recognition searches: it scrapes billions of images from internet platforms like Facebook, Instagram, and Venmo without individuals' consent (or even knowledge) and in violation of these platforms' terms of service. Governments from around the world—including the U.K., Australia, France, and Canada—have declared Clearview's practices illegal violations of its citizens' privacy, issued multimillion dollar fines, and in some cases, banned Clearview entirely.

Still, more than 600 law enforcement agencies in the U.S. have used Clearview. Multiple police agencies have deployed Clearview to [identify protestors](#) at racial justice protests. This technology remains unregulated in the United States.