An Issue Brief on

Facial Recognition Technology

RESTORE the FOURTH

Only 30 years ago, facial recognition technology (FRT) seemed like science fiction, but today it has applications in nearly every aspect of our life. One such application is policing and mass surveillance. Over the past decade we've seen law enforcement use of FRT proliferate: the FBI has conducted over 390,000 FRT searches since 2011. That number has grown to almost 4,000 FRT searches a month. In Utah alone, law enforcement agencies logged more than 2,000 searches between 2015 and 2017. A recent GAO report revealed that of 42 federal government agencies, 20 are using FRT, and that federal government databases now hold well over one billion FRT-compatible images. The government has access to driver's license photos, even from other countries, and these are shared with law enforcement agencies across the country, including Immigration and Customs Enforcement (ICE) and the FBI.

Law enforcement can also contract with private companies that offer their own unique databases of images. One such contractor is the infamous Clearview AI, which holds a database of over 3 billion images of faces. Clearview AI's database is so large because they scraped user-submitted photos from social media to build it. While this may seem shocking, it's totally legal: outside of a few states that have strict biometric laws, law enforcement and their private contractors can use the photos you post to social media without your consent—using your face in line-ups without you ever even knowing.

What is FRT?

At its most basic level, facial recognition technology is a set of algorithms that have been designed to help computers identify individual human beings based on what our faces look like. FRT is a form of "biometrics"; in other words, an identifier based on unique measurements of individual human bodies. In the 1960s, when Woody Bledsoe invented a rudimentary form of FRT, the government quickly realized its implications for law enforcement, pouring CIA money into Bledsoe's research. With a large enough database, they realized, FRT could effectively automate police searches, saving the government money on policing.

The country saw its first large scale application of FRT under the justification of security at the 2001 Super Bowl—attendees were scanned and had their faces compared against a database of mugshots by police. The ACLU argued at the time that this raised Fourth Amendment concerns. The last twenty years' jurisprudence has developed considerably, strengthening the ACLU's case, as courts have grappled with the Fourth Amendment implications of mass, continuous digital searches in public.

The development and adoption of FRT was supercharged in the 2010s by the development and refinement of machine learning. Computers could now use a "training set" of images, often scraped from the Internet, to "learn" how one face differed from another. The result was a sharp increase in accuracy rates.

How accurate is FRT?

FRT requires a database to check inputted faces against. When an image is described as being a "95% match", it's important to realize that this doesn't mean that there's only a 5% chance that the image is not of a particular person of interest. Instead, it means that the image's "faceprint", or network of key points, matches with 95% confidence to the faceprint of another image held in the database. In a database of only 100 images, all taken from the same angle and lighting, that might be strong evidence. But in a database of 80 million images, like the FBI's Next Generation Identity System database, thousands of images could be matched at 95%, but would be false positives in the sense that the image was not of the actual culprit.

Images on the Internet are generally weighted towards middle-aged white men. The result is that all FRT systems available to law enforcement today are far more accurate for images depicting white men than for non-white or non-male people. Even when algorithms are trained on databases that better represent marginalized groups, the accuracy of match identification is limited by factors including aging, pose variation, partial occlusion, illumination and facial expression. For similar reasons, FRT systems are extremely inaccurate for trans people, wrongly identifying "trans men as

women up to 38% of the time and miscategorizing nonbinary people '100% of the time.'" This puts already highly-scrutinized community at risk of encounters with a policing system that regularly dehumanizes them.
Sometimes, lawmakers hear the criticism that FRT is inaccurate and suggest that the task is therefore to make FRT as accurate as possible. But as accuracy increases, privacy concerns are amplified. Inaccurate FRT systems have racial and gender biases baked in; a hypothetical fully accurate FRT system would be terrifying, and would represent the death of our privacy in public. Everyone's movements, whether to the store, to a protest, or to a healthcare provider, could be accurately tracked and routinely available to law enforcement.

Known FRT abuses:

Criminal charges based on false FRT matches
Most misidentifications using FRT are never disclosed. Right now, learning about misidentifications depends on police accidentally disclosing in particular cases that their identification depended on FRT. We know of three different cases, all involving black men, where the men were exonerated after being wrongly charged for crimes based on FRT matches.

Improper denials of benefits

Unemployment recipients across the United States have been denied benefits due to ID.me's flawed facial recognition models. One example out of Massachusetts highlights this: At a recent meeting of the MA legislature on facial recognition, officials from the Registry of Motor Vehicles (RMV) testified that 20% of applications to RMV were flagged as suspicious in their preliminary facial recognition screen using Rekognition's system. These 260,000 applications were reviewed by Massachusetts State Police, who determined that just 497 applications were actually fraudulent. In other words, with regards to fraud prevention, FRT uses a sledgehammer to crack a nut.

Police targeting of sex workers

As sex work has moved to more digital spaces, it's become easier for law enforcement to surveil workers with technology such as FRT. Law enforcement has used FRT to track down sex workers and perform "welfare checks" on them, putting workers who are often victims of police violence in contact with law enforcement. Sex workers are also often targeted by public/private partnerships that employ FRT. Law enforcement often collaborates with private "anti-trafficking" organizations like Thorn (who also partners with Palantir—the ICE-collaborator and security firm that helps fund Clearview AI). Thorn's Spotlight program, which relies on FRT to function, scrapes and collects sex workers' online ads. It turns them over to law enforcement, presumably with the intent to have officers search those ads (all without a warrant or the workers' consent) to identify workers.

Police targeting of protestors

As always, surveillance tech has a chilling effect on people's right to peacefully assemble and FRT is no different. When people know that they may be surveilled for simply going to a protest, they are discouraged from attending those protests, robbing them of their constitutional rights.

In some cases, police have been known to arrest activists using facial recognition matches, long after the protest has ended and everyone has gone home. Facial recognition contributed to the identification of protesters at two protests in Washington, DC. The GAO report referred to above on the use of facial recognition by the federal government, documented that the Capitol Police, CBP and the State Department all used this technology to identify January 6th rioters at the Capitol.

Cameras may originally be installed with public safety justifications on narrow grounds, and then be used to identify and police protesters. Non- violent protesters fear that their identification could result in retribution by political or ideological opponents. This concern precipitated a moratorium by Apple, IBM, and Microsoft on sales of FRT to law enforcement and a new law in Virginia to tighten restrictions on the use of facial recognition technology by local law enforcement agencies.

ICE targeting of immigrants

Immigrants are often targets of Facial Recognition Technology. Clearview AI—one of the most infamous facial recognition companies in the nation—regularly collaborates with ICE. ICE has also been caught using state license databases for FRT, searching for undocumented immigrants who had been able to legally obtain licenses in certain states in order to deport them. ICE also often gets FRT databases from state DMVs secretly, without drivers ever realizing their license photo is being used in this way. In the government's broad attempt to target and criminalize undocumented immigrants with surveillance technology, they've thrown citizens under the bus as well—ignoring their Fourth Amendment rights in order to conduct FRT searches.

Airport adoption of facial recognition constrains freedom to travel

On the pretexts of increased airport security and customer convenience, Customs and Border Patrol is attempting to make use of FRT routine at US airports, for both international and domestic travel. The law requires consent to being subjected to FRT, because there has been no rulemaking process under the Privacy Act to allow this form of data collection. However, CBP structures the airport experience to obscure passengers' right to refuse FRT, and to encourage airlines to require FRT so as to avoid the need for rulemaking.

Facilitating oppression of ethnic and religious minority groups

The Chinese government has been using FRT to suppress protests in Hong Kong, and to facilitate the roundups and persecution of Uyghurs. We invite lawmakers to consider ways in which the racial disparities involved in US law enforcement's FRT deployments duplicate these kinds of oppression.

What does Restore the Fourth recommend?

The Fourth Amendment essentially protects your right to thrive undisturbed by government if you're not engaged in the planning or commission of actual crimes. FRT threatens this vital liberty by forcing everyone into a perpetual line-up of potential suspects whose movements through public space can be continually tracked and parsed for "suspicious" patterns. Misidentifications are already leading to costly legal battles with life-ruining consequences for some. Accurate identifications, by governments intent on surveilling and criminalizing whole races or ethnicities, increase marginalized groups' chances of violent or deadly interactions with police.

We therefore support the federal ban on facial recognition and other biometric technologies proposed by Sen. Markey; local, municipal and state bans and restrictions on law enforcement use of FRT; and measures that ban or restrict private use of FRT, such as that passed in Portland, OR. Local or government-only bans inherently carry the possibility that local law enforcement will circumvent them by collaborating with private companies that may use FRT on their behalf. This is necessary to consider when introducing bans, and shows why it may be more beneficial to take ordinances further than just banning "government use" of FRT.

Jurisdictions with FRT Bans

Alameda, CA
Berkley, CA
Oakland, CA
San Francisco, CA*
New Orleans, LA
Boston, MA*
Brookline, MA
Cambridge, MA*
Easthampton, MA
Northampton, MA
Somerville, MA*
Springfield, MA
Worchester, MA
Portland, ME
Minneapolis, MN*
Jackson, MS
Pittsburgh, PA
Portland, OR
Bellingham, WA
King County, WA*
Port of Seattle, WA
Madison, WI
Vermont
Virginia

* Denotes FRT ban efforts RT4 has been involved with.