Resisting the Menace of Face Recognition

Adam Schwartz ⋮ 15-18 minutes ⋮ 10/26/2021

Face recognition technology is a special menace to privacy, racial justice, free expression, and information security. Our faces are unique identifiers, and most of us expose them everywhere we go. And unlike our passwords and identification numbers, we can't get a new face. So, governments and businesses, often working in partnership, are increasingly using our faces to track our whereabouts, activities, and associations.

Fortunately, people around the world are fighting back. A growing number of communities have banned government use of face recognition. As to business use, many communities are looking to a watershed Illinois statute, which requires businesses to get opt-in consent before extracting a person's faceprint. EFF is proud to support laws like these.

Face Recognition Harms

Let's begin with the ways that face recognition harms us. Then we'll turn to solutions.

Privacy

Face recognition violates our human right to privacy. Surveillance camera networks have flooded our public spaces. Face recognition technologies are more powerful by the day. Taken together, these systems can quickly, cheaply, and easily ascertain where we've been, who we've been with, and what we've been doing. All based on a unique marker that we cannot change or hide: our own faces.

In the words of a federal appeals court ruling in 2019, in a case brought against Facebook for taking faceprints from its users without their consent:

> Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo. … [I]t seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building.

Government use of face recognition also raises Fourth Amendment concerns. In recent years, the U.S. Supreme Court has repeatedly placed limits on invasive government uses of cutting-edge surveillance technologies. This includes police use of GPS devices and cell site location information to track our movements. Face surveillance can likewise track our movements.

Racial Justice

Face recognition also has an unfair disparate impact against people of color.

Its use has led to the wrongful arrests of at least three Black men. Their names are Michael Oliver, Nijeer Parks, and Robert Williams. Every arrest of a Black person carries the risk of excessive or even deadly police force. So, face recognition is a threat to Black lives. This technology also caused a public skating rink to erroneously expel a Black patron. Her name is Lamya Robinson. So, face recognition is also a threat to equal opportunity in places of public accommodation.

These cases of "mistaken identity" are not anomalies. Many studies have shown that face recognition technology is more likely to misidentify people of color than white people. A leader in this research is Joy Buolamwini.

Even if face recognition technology was always accurate, or at least equally inaccurate across racial groups, it would still have an unfair racially disparate impact. Surveillance cameras are over-deployed in minority neighborhoods, so people of color will be more likely than others to be subjected to faceprinting. Also, history shows that police often aim surveillance technologies at racial justice advocates.

Face recognition is just the latest chapter of what Alvaro Bedoya calls "the color of surveillance." This technology harkens back to "lantern laws," which required people of color to carry candle lanterns while walking the streets after dark, so police could better see their faces and monitor their movements.

Free Expression

In addition, face recognition chills and deters our freedom of expression.

The First Amendment protects the right to confidentiality when we engage in many kinds of expressive activity. These include anonymous speech, private conversations, confidential receipt of unpopular ideas, gathering news from undisclosed sources, and confidential membership in expressive associations. All of these expressive activities depend on freedom from surveillance because many participants fear retaliation from police, employers, and neighbors. Research confirms that surveillance deters speech.

Yet, in the past two years, law enforcement agencies across the country have used face recognition to identify protesters for Black lives. These include the U.S. Park Police, the U.S. Postal Inspection Service, and local police in Boca Raton, Broward County, Fort Lauderdale, Miami, New York City, and Pittsburgh. This shows, again, the color of surveillance.

Police might also use face recognition to identify the whistleblower who walked into a newspaper office, or the reader who walked into a dissident bookstore, or the employee who walked into a union headquarters, or the distributor of an anonymous leaflet. The proliferation of face surveillance can deter all of these First Amendment-protected activities.

Information Security

Finally, face recognition threatens our information security.

Data thieves regularly steal vast troves of personal data. These include faceprints. For

example, the faceprints of 184,000 travellers were stolen from a vendor of U.S. Customs and Border Protection.

Criminals and foreign governments can use stolen faceprints to break into secured accounts that the owner's face can unlock. Indeed, a team of security researchers did this with 3D models based on Facebook photos.

Face Recognition Types

To sum up: face recognition is a threat to privacy, racial justice, free expression, and information security. However, before moving on to solutions, let's pause to describe the various types of face recognition.

Two are most familiar. "Face identification" compares the faceprint of an unknown person to a set of faceprints of known people. For example, police may attempt to identify an unknown suspect by comparing their faceprint to those in a mugshot database.

"Face verification" compares the faceprint of a person seeking access, to the faceprints of people authorized for such access. This can be a minimally concerning use of the technology. For example, many people use face verification to unlock their phones.

There's much more to face recognition. For example, face clustering, tracking, and analysis do not necessarily involve face identification or verification.

"Face clustering" compares all faceprints in a collection of images to one another, to group the images containing a particular person. For example, police might create a multi-photo array of an unidentified protester, then manually identify them with a mugshot book.

"Face tracking" follows the movements of a particular person through a physical space covered by surveillance cameras. For example, police might follow an unidentified protester from a rally to their home or car, then identify them with an address or license plate database.

"Face analysis" purports to learn something about a person, like their race or emotional state, by scrutinizing their face. Such analysis will often be wrong, as the meaning of a facial characteristic is often a social construct. For example, it will misgender people who are transgender or nonbinary. If it "works," it may be used for racial profiling. For example, a Chinese company claims it works as a "Uighur alarm." Finally, automated screening to determine whether a person is supposedly angry or deceptive can cause police to escalate their use of force, or expand the duration and scope of a detention.

Legislators must address all forms of face recognition: not just identification and verification, but also clustering, tracking, and analysis.

Government Use of Face Recognition

EFF supports a ban on government use of face recognition. The technology is so destructive that government must not use it at all.

EFF has supported successful advocacy campaigns across the country. Many local communities have banned government use of face recognition, from Boston to San

Francisco. The State of California placed a three-year moratorium on police use of face recognition with body cameras. Some businesses have stopped selling face recognition to police.

We also support a bill to end federal use of face recognition. If you want to help stop government use of face recognition in your community, check out EFF's "About Face" toolkit.

Corporate Use of Face Recognition

The Problem

Corporate use of face recognition also harms privacy, racial justice, free expression, and information security.

Part of the problem is at brick-and-mortar stores. Some use face identification to detect potential shoplifters. This often relies on error-prone, racially biased criminal justice data. Other stores use it to identify banned patrons. But this can misidentify innocent patrons, especially if they are people of color, as happened to Lamya Robinson at a roller rink. Still, other stores use face identification, tracking, and analysis to serve customers targeted ads or track their behavior over time. This is part of the larger problem of surveillance-based advertising, which harms all of our privacy.

There are many other kinds of threatening corporate uses of face recognition. For example, some companies use it to scrutinize their employees. This is just one of many high-tech ways that bosses spy on workers. Other companies, like Clearview AI, use face recognition to help police identify people of interest, including BLM protesters. Such corporate-government surveillance partnerships are a growing threat.

The Solution

Of all the laws now on the books, one has done the most to protect us from corporate use of face recognition: the Illinois Biometric Information Privacy Act, or BIPA.

At its core, BIPA does three things:

1. It bans businesses from collecting or disclosing a person's faceprint without their opt-in consent.
2. It requires businesses to delete the faceprints after a fixed time.
3. If a business violates a person's BIPA rights by unlawfully collecting, disclosing, or retaining their faceprint, that person has a "private right of action" to sue that business.

EFF has long worked to enact more BIPA-type laws, including in Congress and the states. We regularly advocate in Illinois to protect BIPA from legislative backsliding. We have also filed amicus briefs in a federal appellate court and the Illinois Supreme Court to ensure that everyone who has suffered a violation of their BIPA rights can have their day in court.

BIPA prevents one of the worst corporate uses of face recognition: dragnet faceprinting of the public at large. Some companies do this to all people entering a store, or all people appearing in photos on social media. This practice violates BIPA because some of these people have not previously consented to faceprinting.

People have filed many BIPA lawsuits against companies that took their faceprints without their consent. Facebook settled one case, arising from their "tag suggestions" feature, for $650 million.

First Amendment Challenges

Other BIPA lawsuits have been filed against Clearview AI. This is the company that extracted faceprints from ten billion photographs, and uses these faceprints to help police identify suspects. The company does not seek consent for its faceprinting. So Clearview now faces a BIPA lawsuit in Illinois state court, brought by the ACLU, and several similar suits in federal court.

In both venues, Clearview asserts a First Amendment defense. EFF disagrees and filed amicus briefs saying so. Our reasoning proceeds in three steps.

First, Clearview's faceprinting enjoys at least some First Amendment protection. It collects information about a face's measurements, and creates information in the form of a unique mathematical representation. The First Amendment protects the collection and creation of information because these often are necessary predicates to free expression. For example, the U.S. Supreme Court has ruled that the First Amendment protects reading books, gathering news, creating video games, and even purchasing ink by the barrel. Likewise, appellate courts protect the right to record on-duty police.

First Amendment protection of faceprinting is not diminished by its use of computer code, because code is speech. To paraphrase one court: just as musicians can communicate among themselves with a musical score, computer programmers can communicate among themselves with computer code.

Second, Clearview's faceprinting does not enjoy the strongest forms of First Amendment protection, such as "strict scrutiny." Rather, it enjoys just "intermediate scrutiny." This is because it does not address a matter of public concern. The Supreme Court has emphasized this factor in many contexts, including wiretapping, defamation, and emotional distress. Likewise, lower courts have held that common law claims of information privacy—namely, intrusion on seclusion and publication of private facts—do not violate the First Amendment if the information at issue was not a matter of public concern.

Intermediate review also applies to Clearview's faceprinting because its interests are solely economic. The Supreme Court has long held that "commercial speech," meaning "expression related solely to the economic interests of the speaker and its audience," receives "lesser protection." Thus, when laws that protect consumer data privacy face First Amendment challenge, lower courts apply intermediate judicial review under the commercial speech doctrine.

To pass this test, a law must advance a "substantial interest," and there must be a "close fit" between this interest and what the law requires.

Third, the application of BIPA to Clearview's faceprinting passes this intermediate test. As discussed earlier, the State of Illinois has strong interests in preventing the harms caused by faceprinting to privacy, racial justice, free expression, and information security. Also, there is a close fit from these interests to the safeguard that Illinois requires: opt-in consent to collect a faceprint. In the words of the Supreme Court, data privacy requires "the individual's control

of information concerning [their] person."

Some business groups have contested the close fit between BIPA's means and ends by suggesting Illinois could achieve its goals, with less burden on business, by requiring just an opportunity for people to opt-out. But defaults matter. Opt-out is not an adequate substitute for opt-in. Many people won't know a business collected their faceprint, let alone know how to opt-out. Other people will be deterred by the confusing and time-consuming opt-out process. This problem is worse than it needs to be because many companies deploy "dark patterns," meaning user experience designs that manipulate users into giving their so-called "agreement" to data processing.

Thus, numerous federal appellate and trial courts have upheld consumer data privacy laws that are similar to BIPA against First Amendment challenge. Just this past August, an Illinois judge rejected Clearview's First Amendment defense.

Next Steps

In the hands of government and business alike, face recognition technology is a growing menace to our digital rights. But the future is unwritten. EFF is proud of its contributions to the movement to resist abuse of these technologies. Please join us in demanding a ban on government use of face recognition, and laws like Illinois' BIPA to limit private use. Together, we can end this threat.