BUSINESS INSIDER

Facial recognition technology is getting out of control

Matthew Feeney

March 8, 2020

Until January few had heard of Clearview AI, a company that has scraped billions of publicly available images from millions of websites in order to build a facial image search engine app.

Clearview claims that more than six hundred law enforcement agencies have used its technology in the last year. News that police officers can search against a plethora of images uploaded to the most popular social media platforms has prompted outcry from officials, activists, and civil libertarians.

Clearview's technology should concern everyone who values privacy and security.

The dangers of Clearview's tech

Clearview CEO Hoan Ton-That has been on the defensive since a *New York Times* report raised the company's profile from relative obscurity to the topic of a nationwide privacy discussion. Ton-That claims that the First Amendment allows Clearview to scrape publicly available images, although some lawyers disagree.

Many of "Big Tech's" best-known firms, such as YouTube, Facebook, and Twitter have issued Clearview cease-and-desist letters. Clearview, clearly wary of the potential backlash to news of its technology, has hired former solicitor general Paul Clement to buttress its legal arguments.

Clearview did not provide a list of the agencies using its app to the *New York Times*. However, a leaked list of Clearview clients reveals that many of Clearview's customers are private companies such as Macy's as well as state and local police departments including the Miami Police Department, Philadelphia Police Department, Chicago Police Department, and New York State Police.

Clearview's credentialed users include FBI agents and Customs and Border Patrol officers. In the hands of a police officer prone to misconduct, Clearview's app would be a dangerous tool, allowing them to identify protesters, journalists critical of their departments, and people simply engaged in legal activity.

Too often, police across the country use surveillance technology without first informing the public. In one particularly egregious case, police in Baltimore partnered with a private company that builds airplane-mounted surveillance technology without even informing local officials, let alone the public.

Facial recognition is a more pressing concern than aerial surveillance. Thanks to technology like that developed by Clearview, anyone who has uploaded photos of themselves to social media is potentially identifiable to hundreds of law enforcement agencies.

Even those who have opted out of social media can be identified via Clearview. If someone took a photo of you — even if you have no social media whatsoever — and Tweeted it or posted it on their Facebook page, you could end up among the billions of images Clearview scraped.

Clearview defenders have highlighted that its technology has been used to identify children who have been sexually abused. Law enforcement agencies have noted that Clearview's technology has been used to investigate a wide range of crimes including murder, shoplifting, and identity theft.

But the fact that technology can be used to investigate crimes and help secure convictions is not a sufficient condition for its unbridled use. Wiretapping is often a valuable method for gathering evidence of serious crimes, but police cannot use wiretap technology without first having an order approved by a judge.

A liberal society requires citizens and residents to have private areas, and civil liberties protections help ensure the sanctity of such spaces even if many crimes are committed outside the watchful eye of surveillance technology.

Finding the right balance

A liberal approach to facial recognition that respects civil liberties without being technophobic would require that facial recognition databases queried by law enforcement should only include data related to people with outstanding warrants for violent and other serious crimes. It would also ban the use of real-time identification and require local officials to be transparent about the surveillance technology they plan to use.

It would be wrong to portray facial recognition as a technology that inevitably leads to civil liberty abuses. Like any other piece of technology, it can be used for good and ill. Yet the potential for tools like Clearview to be misused at a time when facial recognition is relatively unregulated should prompt lawmakers and officials to prevent law enforcement officers from using Clearview's app.

Lawmakers across the country have already taken steps to limit the use of surveillance technology and increase transparency.

The American Civil Liberties Union's Community Control Over Police Surveillance campaign resulted in surveillance transparency bills passing across the country. A handful of cities, including San Francisco and Cambridge, Massachusetts, have passed bans on government use of facial recognition.

Sens. Cory Booker (D-NJ) and Jeff Merkley (D-OR) recently introduced a bill that would place a moratorium on federal funds being used on state or local facial recognition systems and ban federal use of the technology until a commission outlined appropriate safeguards.

While I don't support a complete ban on facial recognition, it's not hard to understand why officials have implemented bans in an environment where technology is outpacing the law.

Technology may be moving faster than the law, but that's not a reason for officials to resign themselves to an inevitable world where the abolition of privacy is the price of a social life.

Facial recognition can be a valuable tool for law enforcement, but absent the right protections and regulations it's a surveillance nightmare. Lawmakers should take steps to ensure that police and other government officials can't use facial recognition technology to identify law abiding residents and citizens.

Matthew Feeney is the director of the Cato Institute's Project on Emerging Technologies.