The rise of the anti-facial recognition movement

Submitted by russell on Tue, 09/16/2014 - 08:11

The rise of the anti-facial recognition movement
By Joseph Cox on September 14th, 2014 for kernelmag.com

With Facebook automatically tagging your photos, Google Glass apps being able to pinpoint faces, and police using high-end technology to match digital and physical identities, big brother's watchful eye is all around us.

While the technology behind facial recognition continues to develop as its presence increases, some artists are trying to give citizens their privacy back the best way they know how—by designing contraptions that help ordinary citizens avoid detection.

You might not know Leo Selvaggio, but there's a chance you've seen him—or someone strikingly identical to him. He's white, male, and young. To be frank, there is nothing remarkable about his appearance, but that's precisely the point.

Selvaggio's the artist behind the URME Personal Surveillance Identity Prosthetic, a photo-realistic recreation of Selvaggio's face that allows others to be able to assume his identity to protect their own. The mask is made from a pigmented hard resin using 3D-printing technology that allows for the replication of Selvaggio's skin tone and hair. It's detailed enough to fool the technology and inconspicuous enough to avoid drawing attention from people in a crowd.

"What is actually happening is that you're creating disinformation." —Leo Selvaggio

"I wanted something practical, that people could actually use," Selvaggio recalls. He also offers cardboard versions for a cheaper price and a printable, free-to-download file. After raising well beyond his Indiegogo target of $1,000 back in June, Selvaggio has sold seven copies of the prosthetic mask, and over 50 of its low-tech alternative.

Instead of just remaining out of sight, the intention of the project is to flood the system with copies of his face. Not only does that protect whoever is behind the mask, it allows Selvaggio to explore his other interest: the conception of identity.

"What is actually happening is that you're creating disinformation," Selvaggio says. "What happens when there's a hundred Leos walking in public spaces, all from different parts of the country? What is an automated system going to say about me then?"

The state of facial recognition
The inspiration for the URME Personal Surveillance Identity Prosthetic came in part from personal circumstance. Selvaggio lives in Chicago, the most-spied-on city in the United States. It's home to Operational Virtual Field, a networked system of 24,000 cameras that can automatically search for a specific individual, pick them out, and bring up any other records that the system has access to. According to an ACLU report, the city's mayor predicted

that by 2016, there will be a camera on "almost every block," and in June, police officers made their first arrest based off of the technology.

Although this may be an exciting idea for law enforcement, there are myriad problems with the technology that need to be considered.

Researchers in China claimed to have developed a kit that can match faces with up to 99.15 percent accuracy

"While facial recognition systems are billed as cutting-edge and sophisticated, they have been proven to be a problematic technology prone to errors," says Mike Rispoli from Privacy International. "The angle in which the picture was taken, the lighting in the surrounding areas, the person's skin tone or clothing, and other variables all have a significant impact on how the faceprint is registered and has been shown to create false matches."

A 2011 PowerPoint slide by the National Security Agency, leaked by Edward Snowden, showed how easily the technology can create false matches. A facial recognition query for Osama bin Laden, for example, turned up four bearded men bearing only the slightest resemblance to him, according to the New York Times.

Such errors could have serious consequences

"When these systems are deployed by, for instance, law enforcement and border agencies, false matches can lead to wrongful arrests and detainment," Rispoli warns.

It should be pointed out that there have been a number of recent success stories around facial recognition technology. In August, the FBI caught a fugitive who had been on the run for over a decade, thanks to a positive match between an old passport photo and a Nepalese visa application. In the same week, researchers in China claimed to have developed a kit that can match faces with up to 99.15 percent accuracy, even when dealing with various camera angles and lighting environments. More recently, another team from China has boasted 99.8 percent accurate results, after working on a database that contains 50 million Chinese faces.

As artists, they feel a certain inherent obligation to both caution and provoke.

But as law enforcement agencies expand their use of the technology, the potential for error will likely increase. That's especially alarming considering that one of the FBI's biometric databases will soon store millions of ordinary citizens' faces.

"There are no meaningful protections in place when it comes to the collection, storage, security, and future use of that data," Rispoli stresses. "Without strict and clear regulations of the databases that store faceprints, these systems threaten our right to privacy, not only when an initial scan takes place, but also what happens to that data after."

At the moment, it's not clear what happens to footage once it's been collected if it isn't part of a criminal investigation, and there aren't any laws specifically crafted for facial biometric data. But there's an even more fundamental issue that is particular to face-detecting.

"Biometric surveillance systems are problematic," Rispoli says, "but facial recognition is of a different breed, since faceprints can be taken without our knowledge or consent."

To caution and provoke

Unlike fingerprints or iris scans, which presumably have to be done either with your participation or by physical force, facial scanning can be done remotely and surreptitiously.

In their own way, independent artists are taking back control from a system that didn't ask to track their identities.

Adam Harvey, a New York-based artist with a long list of privacy-focused projects, has developed Computer Vision Dazzle (or CV Dazzle), which aims to undermine surveillance algorithms by emphasizing and obscuring certain features on a participants face. His line of fashion products include an "anti-drone" burqa, Hijab, and hoodie.

Unlike fingerprints or iris scans, facial scanning can be done remotely and surreptitiously.

“It turns out that there is a vulnerability in the way 2D face recognition happens that allows someone to block it by creatively using hair, makeup, or other fashion accessories,” he writes via email. “Of course, it’s not an appropriate look for all occasions. But neither is a tuxedo.”

Harvey, who protects his online privacy by using virtual private networks (VPNs) and avoiding Google products, says that his “grand vision is to change the way we think about privacy, and by extension technology. I want to see more discussion and accountability for the technology choices we make.”

Another artist, Zach Blas, an assistant professor at the Department of Art at the University at Buffalo, wants to highlight the structural prejudices in biometric surveillance systems, such as race and gender.

The overall goal, at least according to Selvaggio is “to get people to engage with how fast the technology is moving, and how disproportionate the power is.” He also wants “to have people increase their amount of civil engagement.”

As artists, they feel a certain inherent obligation to both caution and provoke; Selvaggio calls them “the watchdogs of the future,” and those who campaign for changes in the law seem to agree.

“These projects seem like powerful ways to challenge our preconceived notions about privacy in public spaces,” offered Christopher Calabrese, legislative counsel from the American Civil Liberties Union (ACLU) via email.

“Artists are right to draw attention to this powerful technology. Now it’s incumbent on lawmakers to give consumers back control over how it is used.”

Photo by ahprojects | Remix by Max Fleishman
Legal Information