TECHNOLOGY

Who Owns Your Face?

Advertising companies, tech giants, data collectors, and the federal government, it turns out.

ADRIENNE LAFRANCE MARCH 24, 2017



A woman wears Snapchat Spectacles on the floor of the New York Stock Exchange, on March 2, 2017. (LUCAS JACKSON / REUTERS)

It takes a feast of facial imagery to teach a machine how to recognize an individual person.

This is why computer scientists so often use the faces of Hollywood celebrities in their research. Tom Hanks, for example, is in so many publicly available photographs that it's fairly easy to build a Hanks database for algorithm-training purposes.

Depending on a researcher's needs, there are many other available databases of human faces—some featuring tens of thousands of images. These collections of faces draw from public records like mugshots, surveillance footage, news photos, Google images, and university studies.

It's entirely possible that your face is in one of these databases. There's no way to say for certain that it isn't.

Your face is yours. It is a defining feature of your identity. But it's also just another datapoint waiting to be collected. At a time when cameras are ubiquitous and individual data collection is baked into nearly every transaction a person can make, faces are increasingly up for grabs.

Data brokers already buy and sell detailed profiles that describe who you are. They track your public records and your online behavior to figure out your age, your gender, your relationship status, your exact location, how

much money you make, which supermarket you shop at, and on and on and on. It's entirely reasonable to wonder how companies are collecting and using images of you, too.

Facebook already uses facial recognition software to tag individual people in photos. Apple's new app, Clips, recognizes individuals in the videos you take. Snap's famous selfie filters work by mapping detailed points on individual users' faces. (Snap says on its website that its technology doesn't take the additional step of recognizing the faces it maps.) That's similar to how software by the Chinese startup Face++ works. Its software maps dozens of points on a person's face, then stores the data it collects. The idea is to be able to use facial recognition systems for keyless entry to office buildings and apartment complexes, for example. Jie Tang, an associate professor at Tsinghua University, described to *MIT Technology Review* how he uses his faceprint

to pay for meals: “Not only can he pay for things this way, he says, but the staff in some coffee shops are now alerted by a facial recognition system when he walks in,” and they greet him by name.

It’s understandable, then, that as these technologies rapidly advance, they have become fodder for some conspiracy theories—like the unsubstantiated claim that Snap is building a secret facial recognition database with the images of people who use its popular Snapchat app.

But such conspiracies aren’t as outlandish as they’re made out to be. Experts have been warning against facial-recognition systems for decades. The F.B.I.’s latest facial recognition tools give the agency the ability to scan millions of photos of ordinary Americans. “To be clear, this is a database—or a network of databases—comprised primarily of law-abiding Americans,” said Congressman Jason Chaffetz, a Utah Republican, in a House

Committee on Oversight and Government Reform hearing on Wednesday. "Eighty percent of the photos in the F.B.I.'s facial recognition network are of non-criminal entries." The F.B.I. is able to access images from driver's licenses in at least 18 states, as well as millions of mugshots.

"Most people have no idea that this is happening," said Alvaro Bedoya, the executive director of the Center on Privacy and Technology at Georgetown Law, in testimony at the hearing. "The latest generation of this technology will allow law enforcement to scan the face of every man, woman, and child walking in front of a street surveillance camera… Do you have the right to walk down the street without the government secretly scanning your face? Is it a good idea to give government so much power with so few limits?"

The accuracy of the agency's system is also a matter of debate. According to Chaffetz, roughly one in seven searches of the FBI

system returned a list of entirely innocent candidates, even though the actual target was in the database. And the agency doesn't track its own rate of false positives, according to the Government Accountability Office, which underscores one of the most troubling scenarios for how facial recognition technology could create problems. "It would be one thing if facial-recognition technology were perfect, or near-perfect," Chaffetz said, "but it clearly is not."

"An inaccurate system will implicate people for crimes they didn't commit," said Jennifer Lynch, an attorney for the Electronic Frontier Foundation, in testimony at the hearing, "and it will shift the burden onto innocent defendants to show that they are not who the system says they are. This threat will disproportionately impact people of color. Face recognition misidentifies African Americans and ethnic minorities at higher rates than whites."

The F.B.I. insists that its use of facial recognition technology is for investigative leads only, and that a faceprint isn't so different than a fingerprint—or an in-person line-up for that matter. Facial recognition software is merely an extension of the work that law enforcement already does, said Kimberly Del Greco, the deputy assistant director at the F.B.I.'s Criminal Justice Information Services Division

"It is a search of law enforcement photos by law enforcement agencies for law enforcement purposes," she said in the hearing. "Law enforcement has performed photo lineups and manually reviewed mugshots for decades. Face recognition software allows this to be accomplished in an automated manner."

Not just automated, but automatic—meaning that camera systems outfitted with facial recognition software would identify anyone in the frame. Privacy advocates and members of Congress agree that what

happens to this sort of data is a complicated and urgent question. A smart surveillance camera may capture and identify attendees of a political rally, for instance, which could have a chilling effect on civic participation.

Eventually, it may be impossible for people to avoid targeted surveillance. “We might get to a point where you just don’t have the option to opt out,” said Alvaro Hoyos, the chief information security officer at the password and identity management firm OneLogin. “People might not want to think about or talk about it, but we’re going toward a state of constant surveillance.”

Actually, we may already be there.

Data-tracking systems are already able to follow your behavior—online and off—to produce a detailed portrait of you. “Websites do it already, but there’s a perception of the anonymity of being behind your keyboard,” Hoyos told me. And yet, he says, “there’s something

about the human image, your image, that is a lot more intimate to us than pretty much anything else. It's who you are."

We want to hear what you think about this article. Submit a letter to the editor or write to letters@theatlantic.com.