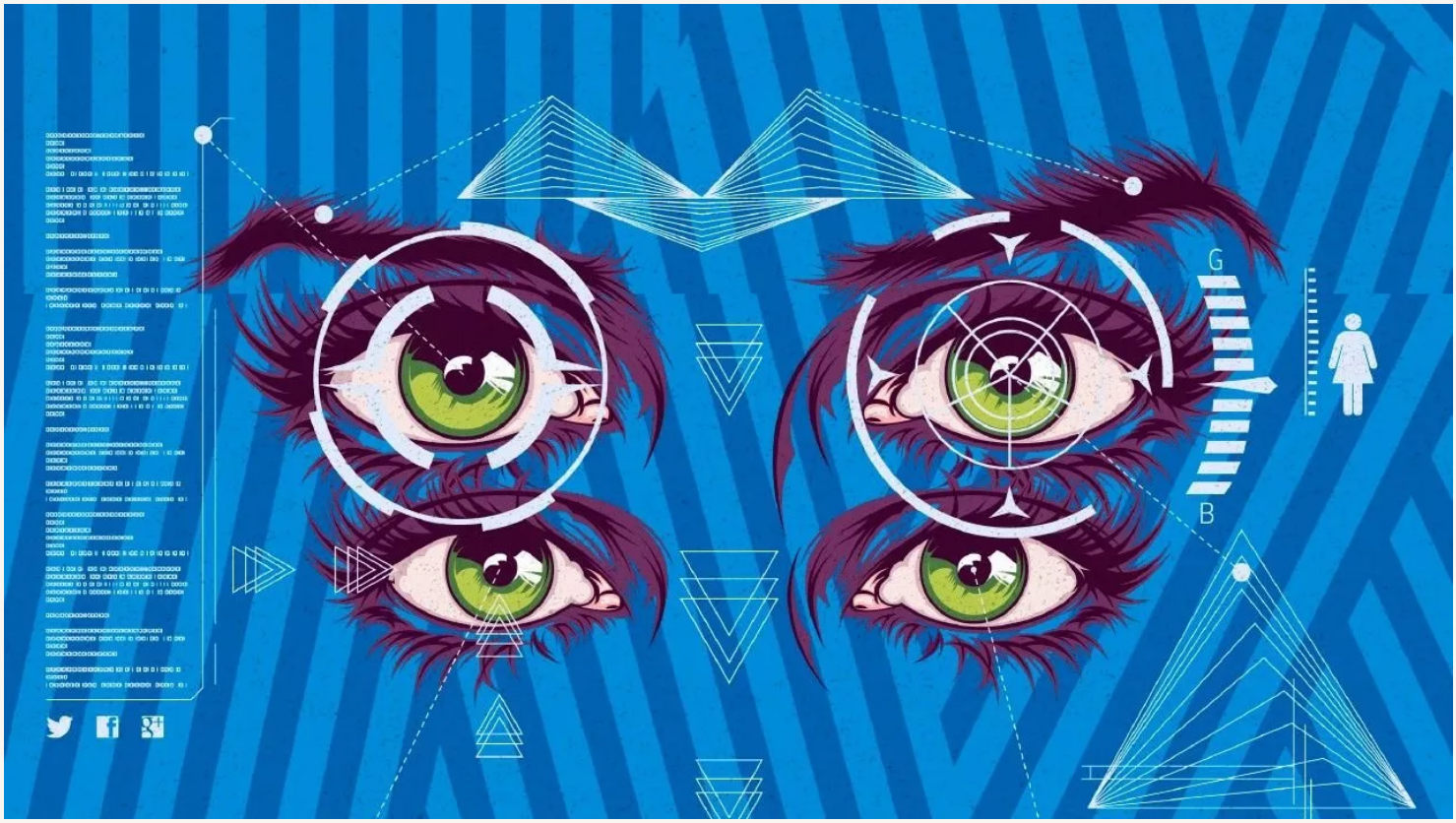
NEWSWEEK MAGAZINE

Biometric Surveillance Means Someone Is Always Watching

Apr 17, 2014 at 6:06 AM EDT



2014-4-18-horiz-cover **PRIEST + GRACE**

By Kyle Chayka

Newsweek Is A Trust Project Member

FOLLOW

Incrimination by selfie can happen.

From 2008 to 2010, as Edward Snowden has revealed, the National Security Agency (NSA) collaborated with the British Government Communications Headquarters to intercept the webcam footage of over 1.8 million Yahoo users.

The agencies were analyzing images they downloaded from webcams and scanning them for known terrorists who might be using the service to communicate, matching faces from the footage to suspects with the help of a new technology called face recognition.

The outcome was pure Kafka, with innocent people being caught in the surveillance dragnet. In fact, in attempting to find faces, the Pentagon's Optic Nerve program recorded webcam sex by its unknowing targets—up to 11 percent of the material the program collected was "undesirable nudity" that employees were warned not to access, according to documents. And that's just the beginning of what face recognition technology might mean for us in the digital era.

Over the past decade, face recognition has become a fast-growing commercial industry, moving from its governmental origins—programs like Optic Nerve—into everyday life. The technology is being pitched as an effective tool for securely confirming identities, with the financial backing of a new Washington lobbying firm, the Secure Identity & Biometrics Association (SIBA).

To some, face recognition sounds benign, even convenient. Walk up to the international checkpoint in a German airport, gaze up at a camera, and walk into the country without ever needing to pull out a passport—your image is on file, the camera knows who you are. Wander into a retail store and be greeted with personalized product suggestions—the store's network has a record of what you bought last time.

Facebook already uses face recognition to recommend which friends to tag in your photos.

But the technology has a dark side. The U.S. government is in the process of building the world's largest cache of face recognition data, with the goal of identifying every person in the country. The creation of such a database would mean that anyone could be tracked wherever his or her face appears, whether it's on a city street or in a mall. Today's laws don't protect Americans from having their webcams scanned for facial data.

Security CCTV. 2013 **PETER MARLOW/MAGNUM**

Not That Perfect

Face recognition systems have two components: an algorithm and a database. The algorithm is a computer program that takes an image of a face and deconstructs it into a series of landmarks and proportional patterns—the distance between eye

centers, for example. This process of turning unique biological characteristics into quantifiable data is known as biometrics.

Together, the facial data points create a "face-print" that, like a fingerprint, is unique to each individual. Some faces are described as open books; at a glance, a person can be "read." Face recognition technology makes that metaphor literal. "We can extrapolate enough data from the eye and nose region, from ear to ear, to build a demographic profile," including an individual's age range, gender and ethnicity, says Kevin Haskins, a business development manager at the face recognition company Cognitec.

Face-prints are collected into databases, and a computer program compares a new image or piece of footage with the database for matches. Cognitec boasts a match accuracy rate of 98.75 percent, an increase of over 20 percent over the past decade. Facebook recently achieved 97.25 percent accuracy after acquiring biometrics company Face.com in 2012.

So far, the technology has its limits. "The naive layman thinks face recognition is out there and can catch you anytime, anywhere, and your identity is not anonymous anymore," says Paul Schuepp, the co-founder of Animetrics, a decade-old face recognition company based in New Hampshire. "We're not that perfect yet."

The lighting and angle of faces images must be strictly controlled to create a usable face-print. *Enrollment* is the slightly Orwellian industry term for making a print and entering an individual into a face recognition database. "Good enrollment means getting a really good photograph of the frontal face, looking straight on, seeing both eyes and both ears," Schuepp explains.

How face recognition is already being used hints at just how pervasive it could become. It's being used on military bases to control who has access to restricted areas. In Iraq and Afghanistan, it was used to check images of detainees in the field against Al-Qaeda wanted lists. The Seattle police department is already applying the technology to identify suspects on video footage.

The technology's presence is subtle, and as it gets integrated into devices we already use, it will be easy to overlook. The most dystopian example might be NameTag, a

startup that launched in February promising to embed face recognition in wearable computers like Google Glass. The software would allow you to look across a crowded bar and identify the anonymous cutie you are scoping out. The controversial company also brags that its product can identify sex offenders on sight.

As the scale of face recognition grows, there's a chance it could take its place in the technological landscape as seamlessly as the iPhone. But to allow that to happen would mean ignoring the increasing danger that it will be misused.

Monitors show imagery from security cameras seen at the Lower Manhattan Security Initiative on April 23, 2013 in New York, NY. At the counter-terrorism center, police and private security personnel monitor more than 4,000 surveillance... More **JOHN MOORE/GETTY**

Inescapable Security Net

By licensing their technology to everyone from military defense contractors to Internet start-ups, companies like Cognitec and Animetrics are churning a global biometrics

industry that will grow to $20 billion by 2020, according to Janice Kephart, the founder of SIBA. With funding from a coalition of face recognition businesses, SIBA launched in February 2014 to "educate folks about the reality of biometrics, bridging the gap between Washington and the industry," says Kephart, who previously worked as a counsel to the 9/11 Commission. "The Department of Homeland Security hasn't done anything on this for 16 years. America is falling way behind the rest of the world."

Kephart believes biometric technology could have prevented the 9/11 attacks (which she says "caused a surge" in the biometrics industry) and Edward Snowden's NSA leaks. She emphasizes the technology's protective capabilities rather than its potential for surveillance. "Consumers will begin to see that biometrics delivers privacy and security at the same time," she says.

It's this pairing of seeming opposites that makes face recognition so difficult to grapple with. By identifying individuals, it can prevent people from being where they shouldn't be. Yet the profusion of biometrics creates an inescapable security net with little privacy and the potential for serious mistakes with dire consequences. An error in the face recognition system could cause the ultimate in identity theft, with a Miley Cyrus look-alike dining on Miley's dime or a hacker giving your digital passport (and citizenship) to a stranger.

Some in government express concern over the potential for abuse. U.S. Senator Al Franken, D-Minn., has become a leading figure in the debate, noting in 2013 that face recognition "has profound implications for privacy"—namely, that there won't be any. In a February 2014 letter to NameTag, he urged the company to delay its product "until best practices for facial recognition technology are established."

Franken's suggestion points out the biggest problem with face recognition's future. Legal boundaries for the technology have not been set; we know that public face recognition data is being collected, but we don't know how it is being accessed or used.

Contrary to Kephart's assertions, the federal government has been quite busy with biometrics. This summer, the FBI is focusing on face recognition with the fourth step of its Next Generation Identification (NGI) program, a $1.2 billion initiative launched in

2008 to build the world's largest biometric database. By 2013, the database held 73 million fingerprints, 5.7 million palm prints, 8.1 million mug shots and 8,500 iris scans. Interfaces to access the system are being provided free of charge to local law enforcement authorities.

Jennifer Lynch, staff attorney for the privacy-focused Electronic Frontier Foundation (EFF), notes there were at least 14 million photographs in the NGI face recognition database as of 2012. What's more, the NGI database makes no distinction between criminal biometrics and those collected for civil service jobs. "All of a sudden, your image that you uploaded for a civil purpose to get a job is searched every time there's a criminal query," Lynch says. "You could find yourself having to defend your innocence."

Through a federal lawsuit, EFF obtained redacted NGI documents that it will soon publish. documents show that by 2015, the FBI estimates that NGI will include 46 million criminal face images and 4.3 million civil face images. The vendor building the face recognition system, MorphoTrust, was asked to design it to receive up to 55,000 direct photo enrollments per day and 2,300 per hour, as well as process 34,000 photo retrievals per day and 1,400 per hour. The statistics hint at the sheer scale of the face recognition infrastructure under construction—in one year, over 20 million Americans could be put into the system.

Documents also show that Michigan, Florida, Kansas, South Carolina, South Dakota, Hawaii and Maryland likely have already incorporated their criminal mug-shot databases into the system and that 11 more states are in discussions to work with NGI, including New York.

"Americans cannot easily take precautions against the covert, remote and mass capture of their images," Lynch said in the EFF's lawsuit statement. In a world where any camera could be used to grab a face-print, it's impossible to know where your identity will end up. To assert control, we must determine if we have a right to our own faces.

Elevator sign with surveillance monitor. **JPM/CORBIS**

Warrantless Collection

Some legal precedents suggest that we do have a modicum of control over personal biometric data. The 1969 Supreme Court case *Davis v. Mississippi* determined that using fingerprints (a form of biometrics) obtained without a warrant or probable cause for arrest cannot be used in court. Likewise, "the warrantless collection and use of face-prints by law enforcement is unlikely to overcome the hurdle of the Fourth Amendment," Kirill Levashov writes in *The Columbia Science and Technology Law Review*. (The collection of biometrics from individuals who have been legally arrested is protected under cases like 2013's *Maryland v. King*.)

Yet despite cases like *Davis v. Mississippi*, noncriminal biometric information is already being included in criminal investigations, according to Lynch. "Law enforcement agencies are already using Department of Motor Vehicles databases,"

she says. "We know that law enforcement agencies including the FBI are searching those databases for criminal purposes"—meaning that any time citizens have their photo taken in a governmental capacity, whether it's a background check or a driver's license, their faces are liable to be analyzed by NGI.

In the private sector, efforts are being made to ensure face recognition isn't abused, but standards are similarly vague. A 2012 Federal Trade Commission report recommends that companies should obtain "affirmative express consent before collecting or using biometric data from facial images." Facebook collects face-prints by default, but users can opt out of having their face-prints collected.

Technology entrepreneurs argue that passing strict laws before face recognition technology matures will hamper its growth. "What I'm worried about is policies being made inappropriately before their time," Animetrics's Schuepp says. "I don't think it's face recognition we want to pick on." He suggests that the technology itself is not the problem; rather, it's how the biometrics data are controlled.

Yet precedents for biometric surveillance must be set early in order to control its application. "I would like to see regulation of this before it goes too far," Lynch says. "There should be laws to prevent misuse of biometric data by the government and by private companies. We should decide whether we want to be able to track people through society or not."

Impossible to Be Anonymous

What would a world look like with comprehensive biometric surveillance? "If cameras connected to databases can do face recognition, it will become impossible to be anonymous in society," Lynch says. That means every person in the U.S. would be passively tracked at all times. In the future, the government could know when you use your computer, which buildings you enter on a daily basis, where you shop and where you drive. It's the ultimate fulfillment of Big Brother paranoia.

But anonymity isn't going quietly. Over the past several years, mass protests have disrupted governments in countries across the globe, including Egypt, Syria and Ukraine. "It's important to go out in society and be anonymous," Lynch says. But face

recognition could make that impossible. A protester in a crowd could be identified and fired from a job the next day, never knowing why. A mistaken face-print algorithm could mark the wrong people as criminals and force them to escape the specter of their own image.

If biometric surveillance is allowed to proliferate unchecked, the only option left is to protect yourself from it. Artist Zach Blas has made a series of bulbous masks, aptly named the "Facial Weaponization Suite," that prepare us for just such a world. The neon-colored masks both disguise the wearer and make the rest of us more aware of how our faces are being politicized.

"These technologies are being developed by police and the military to criminalize large chunks of the population," Blas says of biometrics. If cameras can tell a person's identity, background and whereabouts, what's to stop the algorithms from making the same mistakes as governmental authorities, giving racist or sexist biases a machine-driven excuse? "Visibility," he says, "is a kind of trap."

Correction: An earlier version of this story misnamed the state in which Al Franken is a senator.