New American

Written by **Joe Wolverton, II, J.D.** on March 28, 2014

Facebook Facial Recognition Software Has Almost Human Accuracy

Facebook may soon possess the power to match faces to users with almost human-like accuracy.

According to the social-media giant, sophisticated facial recognition software is currently being tested that would employ 3D face modeling to render with a 97.25 percent success rate what it calls "Labeled Faces in the Wild"; in other words — you.

Using a "nine-layer deep neural network," the software known as DeepFace uses "more than 120 million parameters" to recreate the user's face and then scans millions of photos to match the face to the person.

A *Forbes* article on a story published in the MIT TechnologyReview.com, reports, "DeepFace uses a 3D model for rotating faces virtually so that the person in the photo appears to be looking at the camera. The angle of the face is corrected by using a 3D model of an 'average' forward-looking face."

Forbes adds, "The DeepFace algorithms have also been successfully tested for facial verification within YouTube videos" and that the technology could "improve Facebook's ability to suggest users for tagging in an uploaded photo and for other potential purposes."

Although this program is still being tested (Facebook's Artificial Intelligence Group will present their findings at a conference in June), the prospects of these "other potential purposes" should frighten the 1.3 billion active monthly users of the site.

Particularly as Facebook isn't known for more than token resistance to cooperating with the federal government's quest to put everyone under the National Security Agency's never-blinking eye.

According to a statement posted on the company's website last June, government agencies — including federal, state, and local authorities — requested user data on between 18,000 and 19,000 account holders.

Following the negotiations in 2013 that opened the way for Facebook to report its cooperation with requests to hand over user information, Microsoft made a similar surveillance disclosure. A blog post on the Redmond, Washington-based company's website declared:

> For the six months ended December 31, 2012, Microsoft received between 6,000 and 7,000 criminal and national security warrants, subpoenas and orders affecting between 31,000 and 32,000 consumer accounts from U.S. governmental entities (including local, state and federal).

Altogether, that means the accounts of approximately 50,000 Americans — accounts they believed were secure — were laid open to the eyes of government agents.

These revelations may be nothing more than cover fire to distract users from the collusion of these

corporations with the NSA as disclosed by NSA whistleblower and former NSA subcontractor, Edward Snowden.

Under the PRISM data-gathering program, the NSA and the FBI are "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time," as reported by the *Washington Post*.

The joint venture has been functioning since 2007, but came to light only in a PowerPoint presentation that was part of the cache of documents leaked by Snowden.

Snowden claimed that the program was so invasive that "They [the NSA and the FBI] quite literally can watch your ideas form as you type."

According to the information Snowden released, two of the tech companies that disclosed government surveillance requests — Facebook and Microsoft — were giving the government access to the private information of millions of users.

They were not alone, however. Yahoo, Google, PalTalk, AOL, Skype, YouTube, and Apple all allowed the agents of the federal surveillance state to secretly snoop on their users.

The New American has reported on the story in detail:

> PRISM works in conjunction with another top-secret program, called BLARNEY, which, according to the program's summary, "leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks."
>
> PRISM allows the NSA to enter a company's data stream and extract communications by keying in "selectors" or search items. The agency is mandated by law to conduct surveillance only on foreign operations within the United States, but the selectors are designed to produce at least 51 percent confidence in the "foreignness" of the data it collects, meaning it could be intercepting wholly domestic communications nearly half of the time. Training materials instruct new analysts to submit accidentally collected U.S. content for a quarterly report. But the training instructions also tell the analysts that "it's nothing to worry about," the *Post* said.

Possible details of just how the data flow were recently laid out in a report published online last summer.

Tech news website Mashable examined "press reports, the companies' statements and what the Director of National Intelligence has disclosed" to figure out how PRISM functions. After its investigation, Mashable reckons that PRISM is "probably more like a data ingestion API [application programming interface — the way software components interact] system that allows for streamlined processing of Foreign Intelligence Surveillance Act requests. And Google revealed to *Wired* that its secret system to siphon data to the NSA was nothing more than a secure FTP [File Transfer Protocol]."

Nothing more than a pipe running from Google, whose online and mobile services are nearly ubiquitous, to the federal government's shadowy surveillance corps.

Perhaps the most disturbing revelation coming from the Snowden leaks about the NSA is the fact that it confirms that the government and their corporate partners consider the protections of the Fourth Amendment to be nothing more than a "parchment barrier" that is easily torn through. Now that the Constitution is regarded by the federal government as advisory at best, there is nothing standing between Americans and the construction of a domestic 21st century Panopticon.

In this country, then, every citizen is now a suspect, and the scope of the surveillance is being expanded to likely place every word, every movement, every text, every conversation, every e-mail, and every social media subject to monitoring by the federal domestic spying apparatus.

Imagine the increase of that capacity if a major player such as Facebook successfully deploys software that can almost perfectly match all the millions of photos saved on its servers to a name. Facebook would become a sort of virtual real-time resource for those who would be interested in compiling caches of personal data on everybody in the world.

Add that to the story *The New American* reported in December 2013 that revealed that an elite team of hackers employed by the FBI had developed an application that turns on built-in laptop cameras. According to details provided in a *Washington Post* article, the software can be turned on remotely by the g-men and perhaps most notably, the little green light that typically signals a "live" camera is not illuminated when this application is in use.

In his defense, Facebook founder and CEO Mark Zuckerberg did call President Obama to complain about the government's ham-fisted treatment of the Internet.

"I've called President Obama to express my frustration over the damage the government is creating for all of our future. Unfortunately, it seems like it will take a very long time for true full reform," Zuckerberg writes in a blog post.

"The internet is our shared space. It helps us connect. It spreads opportunity," he added. "This is why I've been so confused and frustrated by the repeated reports of the behavior of the U.S. government. When our engineers work tirelessly to improve security, we imagine we're protecting you against criminals, not our own government."

That all sounds very good, but the fact remains that Facebook has handed over access to user data to the federal government and the company is now near completion of a facial recognition tool that will give it nearly perfect perception.

Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels nationwide speaking on nullification, the Second Amendment, the surveillance state, and other constitutional issues. Follow him on Twitter @TNAJoeWolverton and he can be reached at jwolverton@thenewamerican.com.*