Written by **Warren Mass** on June 2, 2014

NSA Matches Texted Images With Facial Recognition Software

The National Security Agency (NSA) is using its controversial domestic surveillance program to gather millions of images from text messages and social media (e.g, Facebook) and then running the images against its facial recognition programs to identify those pictured.

The latest revelations about the NSA's continued violations of citizens' privacy were made public from documents leaked to the *New York Times* by the former NSA contractor and whistleblower Edward Snowden.

The Snowden documents stated that the NSA intercepts "millions of images per day" — including about 55,000 "facial recognition quality images" — which translate into "tremendous untapped potential."

"It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information" that can help "implement precision targeting," the *Times* quoted from a 2010 document.

Snowden first began leaking information about what he considered to be the NSA's abuses in late 2012, when he first made contact with Glenn Greenwald of Britain's *Guardian* newspaper. Snowden contacted American documentary filmmaker Laura Poitras (who resides in Berlin) in January 2013 after seeing her *New York Times* documentary about NSA whistleblower William Binney. The *Guardian* reported that Snowden was attracted to both Greenwald and Poitras after reading a *Salon* article Greenwald wrote detailing how Poitras' controversial films had made her a "target of the government."

The June 1 article reporting on Snowden's latest revelations was co-written by Poitras and the *Times*' James Risen. Russia's RT News observed that Poitras and Greenwald are the only two journalists to have received the leaked NSA documents. The *Times* article noted some recent trends that privacy-conscious Americans will find disturbing:

> The N.S.A. has accelerated its use of facial recognition technology under the Obama administration, the documents show, intensifying its efforts after two intended attacks on Americans that jarred the White House. The first was the case of the so-called underwear bomber, in which Umar Farouk Abdulmutallab, a Nigerian, tried to trigger a bomb hidden in his underwear while flying to Detroit on Christmas in 2009. Just a few months later, in May 2010, Faisal Shahzad, a Pakistani-American, attempted a car bombing in Times Square.

The released documents reveal several methods used by the NSA to expand and improve its use of facial recognition software. These include joint operations with NSA's British counterpart, General

Communications Headquarters, to retrieve webcam images. The NSA has also matched images stored in two databases — the extensive NSA database code-named Pinwale, and the government's main terrorist watch list database, code-named Tide. In addition, the agency was working with the CIA and the State Department on a program called Pisces, collecting biometric data on border crossings from a wide range of countries.

Another facial recognition program used by the NSA, called Wellspring, extracts images from e-mails and other electronic communications and displays those that might contain passport images. The NSA also uses commercially available facial recognition technology from companies such as PittPatt, which is owned by Google.

When asked about the information released from Snowden's reports published by the *Times*, Vanee M. Vines, the NSA's spokeswoman, said "We would not be doing our job if we didn't seek ways to continuously improve the precision of signals intelligence activities — aiming to counteract the efforts of valid foreign intelligence targets to disguise themselves or conceal plans to harm the United States and its allies."

The NSA is not the only government agency that is gathering and analyzing images of people, we reported last September. In an article about the Department of Homeland Security's test of a new facial recognition system at a hockey game in Kennewick, Washington, we noted that DHS had contracted with a private firm, Pacific Northwest National Laboratory (PNNL), to videotape fans attending the game — video that would be used by the government to test the capabilities of facial recognition software.

Patty Wolfhope, a program manager at the Department of Homeland Security, said at the time that no names of people videotaped would be collected during the test and that "only" government researchers, not the technology developers, would see the video. Wolfhope's statement was not likely to reassure those most concerned about facial recognition software, since the threat to liberty comes not from private technology developers, but from potentially totalitarian government.

While the local newspaper in Kennewick, Washington, and most of the other media reporting the story gave cursory descriptions of the procedures and technology involved in the test, RT alone addressed potential abuses and mentioned Homeland Security's (DHS) role much more often than the other reports. RT also has taken an active role in covering Snowden's leaked documents. Perhaps Russians, having lived under a totalitarian police state that monitored their every move, are more familiar than Americans with what can happen when the government takes too strong an interest in its citizens' whereabouts.

An outspoken critic of intrusive government surveillance has been Jennifer Lynch, a lawyer and expert on facial recognition and privacy at the Electronic Frontier Foundation (EFF) in San Francisco, who stated: "The government leads the way in developing huge face recognition databases, while the private sector leads in accurately identifying people under challenging conditions."

EFF filed a lawsuit against the FBI last year because of the Bureau's Next Generation Identification program (NGI), scheduled to be launched this year. Said Lynch:

> NGI will result in a massive expansion of government data collection for both criminal and noncriminal purposes. Biometrics programs present critical threats to civil liberties and privacy. Face-recognition technology is among the most alarming new developments, because Americans cannot easily take precautions against the covert, remote and mass capture of their images.

A description of Next Generation Identification on the FBI's website states: "The FBI has initiated the Next Generation Identification (NGI) program. This program will further advance the FBI's biometric identification services, providing an incremental replacement of current IAFIS technical capabilities, while introducing new functionality."

Part of NGI is something the FBI calls Interstate Photo System (IPS) Enhancements. The FBI says, "The IPS will also allow for easier retrieval of photos, and include the ability to accept and search for photographs of scars, marks, and tattoos. In addition, this initiative will also explore the capability of facial recognition technology."

All of this government snooping is needed, Homeland Security and other government agencies claim, not only to apprehend common criminals but to prevent terrorist attacks like those that occurred on September 11, 2001.

The Foreign Intelligence Surveillance Act of 1978, — which prescribed procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" — was amended in 2001 by the USA Patriot Act to include terrorism on behalf of groups that are not specifically backed by a foreign government.

Public attention was focused on the Act following publication by the *New York Times* on December 16, 2005 of an article that described a program of warrantless domestic wiretapping ordered by the Bush administration and carried out by the National Security Agency since 2002.

The Patriot Act has been so abused by government agencies that the bill's original sponsor in 2001, Rep. Jim Sensenbrenner (R-Wis.), posted a statement on his congressional webpage on June 6, 2013 expressing severe reservations about where the Act had led:

> As the author of the Patriot Act, I am extremely troubled by the FBI's interpretation of this legislation. While I believe the Patriot Act appropriately balanced national security concerns and civil rights, I have always worried about potential abuses. The Bureau's broad application for phone records was made under the so-called business records provision of the Act. I do not believe the broadly drafted FISA order is consistent with the requirements of the Patriot Act. Seizing phone records of millions of innocent people is excessive and un-American.

But Sensenbrenner's change of heart will not undo the damage. It will take a complete repeal of the Patriot Act and all other unconstitutional usurpations of power that took place following the terrorist attacks of September 11, 2001 to prevent our nation into morphing into a clone of Orwell's Oceania — a nation where Big Brother was constantly watching you.

Related articles:

NSA Revelations Prove Abuse Is the Rule, Not the Exception

NSA: We Will Illegally Spy on Citizens Only When Absolutely Necessary

California and Washington Set to Stop NSA at the State Border

Is the NSA Using Google to Spy on Account Holders?

Rep. King Says Sen. Paul Tells "Absolute Lies" About NSA Surveillance

The NSA Domestic Surveillance Lie

NSA Admits Spying on Congressional Phone Habits

NSA Uses Loophole to Justify Collecting Domestic E-mail, Phone Calls

NSA Collects “Untargeted” Texts, Controls “Unconnected” Computers

Document Reveals NSA Monitored 125 Billion Phone Calls in One Month

NSA Ignores Laws and Constitution to Conduct Domestic Surveillance

Snowden Slams U.S. NSA and British GCHQ for Uncontrolled Surveillance

The Case of Edward Snowden: Reason v. Rhetoric

Latest Snowden Leak Shows NSA Wants More Scope and Flexibility