Written by **Joe Wolverton, II, J.D.** on June 14, 2013

Facebook Gives Gov't Access to Nearly 20,000 User Accounts

Have you updated your Facebook account lately? If so, the government may know all about it.

According to a statement posted on the company's website Friday, June 14, government agencies — including federal, state, and local authorities — requested user data on between 18,000 and 19,000 account holders.

The remarkable disclosure of government requests for users' private information follows successful negotiations between Facebook and other tech giants and the federal government.

Over the past few weeks, Facebook, Google, and other technology companies who were implicated in the revelations of the PRISM program have petitioned the feds to allow them to disclose their level of participation in surveillance requests received from government entities.

Most of these requests by government are made under the authority of the Foreign Intelligence Surveillance Act (FISA). Not surprisingly, when the government asks the special surveillance court to approve their snooping, judges give them the go ahead.

In fact, in April, the Department of Justice revealed to Congress the number of applications for eavesdropping received and rejected by the FISA court.

To no one's surprise (least of all to the architects and builders of the already sprawling surveillance state), the letter addressed to Senator Harry Reid (D-Nev.) reports that in 2012, of the 1,789 requests made by the government to monitor the electronic communications of citizens, not a single one was rejected.

That's right. The court, established specifically to judge the merits of applications by the government to spy on citizens, gave a green light to every government request for surveillance.

Not content to be a mere formality for electronic surveillance, the FISA court (officially called the Foreign Intelligence Surveillance Court) also held the coats of the FBI while that agency carried out the searches and seizures set out in 212 applications.

Following the negotiations 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 — accounts they believed were secure — of approximately 50,000 Americans 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 National Security Agency (NSA), as disclosed recently by Edward Snowden, a whistleblower and former network technician working at an NSA station in Hawaii.

Under PRISM, 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 only came to light 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, both companies that disclosed government surveillance requests on Friday — 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.

For its part, Yahoo was apparently dragged into the net kicking and screaming. According to a story published Friday in the *New York Times*, one of the leaked NSA documents reveals that Yahoo reluctantly opened the PRISM porthole after losing a legal challenge to the program.

The *Times* reports that Yahoo fought the NSA in court sometime in 2007 or 2008. Yahoo argued that "the order violated its users' Fourth Amendment rights against unreasonable searches and seizures. The court called that worry 'overblown.'"

Yahoo had to choose: hand over their users' data or violate a court order.

Yahoo chose to open the surveillance spigot.

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

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 revelations 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 the citizens of this nation and the construction of a 21st century Panopticon.

In this country, then, every citizen is now a suspect and the scope of the surveillance is being expanded to place every word, every movement, every text, every conversation, every e-mail, and every social media post under the never-blinking eye of the federal domestic spying apparatus.

The hour is now late if this Republic is to remain a land under the rule of law. To that end, it is critical that Americans recognize that the sweeping surveillance dragnet thrown by the NSA, FBI, and other federal agencies is in direct, open, and hostile violation of the Constitution. The Fourth Amendment to the Constitution clearly states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

As for Congress — every member of which swore an oath to uphold the Constitution, including the Fourth Amendment — Senate Intelligence Committee member Ron Wyden (D-Ore.) claimed that NSA Director General Keith Alexander and Director of National Intelligence James Clapper didn't give "straight answers" when asked by Wyden about the scope of the NSA domestic surveillance activities.

"One of the most important responsibilities a senator has is oversight of the intelligence community," Wyden said in a statement. "This job cannot be done responsibly if senators aren't getting straight answers to direct questions."

While the breadth of the NSA's surveillance programs and the fact that millions of Americans were subject to it regardless of a lack of probable cause would seem to be the last nail in the Obama administration's coffin, a recent Pew poll revealed that 56 percent of Americans say the NSA's tracking of the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism.

Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels frequently nationwide speaking on topics of nullification, the NDAA, and the surveillance state. He can be reached at jwolverton@thenewamerican.com*