Written by **Joe Wolverton, II, J.D.** on March 13, 2014

Sophisticated Surveillance Lets Gov't Watch Every Movement

On March 10, Apple, Inc. released its latest update to its iOS mobile operating system (iOS 7.1). Within hours 6 percent of users had already downloaded the upgrade.

It was a bug discovered in the previous versions, however, that caused some to suspect the NSA had a hand in the hole, however.

A "vulnerability" in iOS 7 potentially left iPhone users' encrypted data accessible to hackers, or to NSA agents, if the opinions of some are to be believed. The story connecting the NSA to the Apple operation system flaw was explained by Jacob Siegal:

> John Gruber gathered the evidence over at Daring Fireball and has come to a startling conclusion — the NSA might have something to do with the bug.
>
> According to a tweet from Jeffery Grossman, this vulnerability has been present in the software since iOS 6. Based on the leaked PowerPoint document which exposed PRISM, Apple and its devices were added to the NSA program in October 2012, just one month after the release of iOS 6. Whether or not the NSA planted the exploit itself, Gruber believes there is a chance the government agency was aware of it and took advantage of it to gain access to private information.
>
> "Once the bug was in place, the NSA wouldn't even have needed to find the bug by manually reading the source code," wrote Gruber. "All they would need are automated tests using spoofed certificates that they run against each new release of every OS. Apple releases iOS, the NSA's automated spoofed certificate testing finds the vulnerability, and boom, Apple gets "added" to PRISM."

While millions of iPhone and iPad owners rejoice over each new iOS update, they pay little if any attention to the shocking level of sophistication of the government's surveillance of all Americans.

To overcome some of the under-reporting, we present a brief outline of the various surveillance tactics in use by our own government.

First, there is the social media surveillance.

In a report published in August, 2013 by In-Q-Tel (IQT), the technology research and development company founded by the CIA, the government's use of social media as a tracking device is highlighted:

> Governments are increasingly finding that monitoring social media is an essential component in keeping track of erupting political movements, crises, epidemics, and disasters, not to mention global trends.

And then, this, regarding In-Q-Tel's efforts to infiltrate social media companies (investing money in

them, for example) in order to make information gleaned from these accounts more accessible to government:

> IQT has made several investments in the social media space, and we will continue to refine our social media investment strategy to focus on providing relevant social media data and technologies to our government customers. We will keep exploring the social media landscape, looking for ways these technologies can be used to effectively address government challenges.

Challenges, one imagines, such as how to keep track of everybody all the time using data the targets themselves willingly provide on Facebook, Twitter, etc.

Have you updated your Facebook or Twitter accounts lately? If so, the government likely knows what you posted, when you posted it, and who read what you wrote.

According to a statement posted on Facebook's website on June 14 of last year, 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.

Last year, Facebook, Google, and other technology companies who were implicated in the revelations of the covert NSA surveillance program known as PRISM petitioned the feds to allow them to disclose their level of participation in surveillance requests received from government entities.

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*.

One document in the Snowden revelations indicated that PRISM was "the number one source of raw intelligence used for NSA analytic reports." Snowden claimed that the program was so invasive that the NSA and the FBI "quite literally can watch your ideas form as you type."

Most of these requests by the 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, 2013 the Department of Justice revealed to Congress the number of applications for eavesdropping received and rejected by the FISA court: In 2012, of the 1,789 requests made by the government to monitor the electronic communications of citizens, not a single one was rejected.

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).

According to the information Snowden released, both 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.

What's perhaps most disturbing is the information revealed in *The New American* recently that intelligence agents in Britain developed and shared with their American counterparts a plan "to manipulate and control online discourse with extreme tactics of deception and reputation-destruction."

In a nutshell, the governments of the United States and Great Britain currently employ teams of agents whose responsibility is to ruin the lives of those individuals who've had the misfortune to run afoul of the establishment.

Then, there is the telephone monitoring.

Among the most disturbing disclosures found within the reams of former NSA subcontractor Edward Snowden's revelations was the surrender by major telecommunications companies of the otherwise private phone records of millions of Americans — none of whom was, as required by the Constitution, suspected of committing any sort of crime.

According to a court order labeled "TOP SECRET," federal judge Roger Vinson ordered Verizon to turn over the phone records of millions of its U.S. customers to the NSA.

The order, issued in April by the U.S. Foreign Intelligence Surveillance Court and leaked on the Internet by The Guardian, compels Verizon to provide these records on an "ongoing daily basis" and to hand over to the domestic spy agency "an electronic copy" of "all call detail records created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."

This information includes the phone numbers involved, the electronic identity of the device, the calling card numbers (if any) used in making the calls, and the time and duration of the call.

In other words, millions of innocent Americans have had their call records shared with a federal spy agency in open and hostile defiance of the Fourth Amendment's guarantee of the right of the people to be free from such unreasonable searches and seizures.

What is reasonable? Legally speaking, "the term reasonable is a generic and relative one and applies to that which is appropriate for a particular situation."

Even if the reasonableness threshold is crossed, though, there must be a warrant and suspicion of commission of or intent to commit a crime. Neither the NSA nor telecommunication companies have asserted that even one of the millions whose phone records were seized fits that description.

E-mails are being read, too.

On July 31, 2013, Glen Greenwald published another drip in the ocean of Snowden leaks. Under a program known as "XKeyscore," the NSA monitors and records every e-mail written by every American, again without a warrant and without probable cause, in direct defiance of the Fourth Amendment.

Greenwald, after examining a PowerPoint presentation included in the information he received from Snowden, explained the scope of XKeyscore: "One presentation claims the [XKeyscore] program covers 'nearly everything a typical user does on the internet,' including the content of emails, websites visited and searches, as well as their metadata." "Analysts can also use XKeyscore and other NSA systems to obtain ongoing 'real-time' interception of an individual's internet activity," he added.

How does it work? Greenwald explained that, too: "An NSA tool called DNI Presenter, used to read the

content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages. Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used."

Cyberspace isn't the only area of human life under constant surveillance by the government, however.

Beyond the internet and electronic communications, the federal government's capacity for keeping an eye on the real world comings and goings of citizens is immensely more jarring and far less publicized.

The U.S. government exercises control over a massive and technologically advanced camera-based surveillance system that has the capacity to keep the urban population of this country under the watchful eye of government 24 hours a day.

TrapWire is the name of this network of cameras and other surveillance tools. Unlike other elements of the central government's cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this nearly unbelievable surveillance scheme were made public by WikiLeaks, the anti-secrecy group founded by Julian Assange.

Exactly what is TrapWire? According to one description of the program, from the online Russia Today:

> Former senior intelligence officials have created a detailed surveillance system more accurate than modern facial recognition technology — and have installed it across the US under the radar of most Americans, according to emails hacked by Anonymous.

For a fuller report on TrapWire and similar "real world" surveillance schemes, see this article from *The New American.*

Every few seconds, data picked up at surveillance points in major cities and landmarks across the United States are recorded digitally on the spot, then encrypted and instantaneously delivered to a fortified central database center at an undisclosed location to be aggregated with other intelligence.

The Constitution's protection on the life, liberty, and property of all people must be enforced on every issue, every time or the gradual erosion predicted by our Founders will eventually create a generation of Americans without a foundation in freedom, a generation that does not question their status as suspects.

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.*