Written by **Joe Wolverton, II, J.D.** on March 14, 2014

NSA Creates Fake Facebook Server to Trap Targets

In order to install malware on the computers of various supposedly hard to reach targets, the National Security Agency (NSA) pretends to be Facebook, giving them instant access to the computers, webcams, microphones, and files of those fooled by the ruse.

This is just one of the several revelations in the latest leak by Edward Snowden to be made public by Glenn Greenwald.

In his new outlet, The Intercept, Greenwald and his colleague Ryan Gallagher also describe how documents obtained by the former NSA subcontractor reveal the NSA's plan to "infect millions of computers with malware."

The pair describe the outline of the plot:

> The clandestine initiative enables the NSA to break into targeted computers and to siphon out data from foreign Internet and phone networks.
>
> The covert infrastructure that supports the hacking efforts operates from the agency's headquarters in Fort Meade, Maryland, and from eavesdropping bases in the United Kingdom and Japan. GCHQ, the British intelligence agency, appears to have played an integral role in helping to develop the implants tactic.

Beyond masquerading as a Facebook server, the intelligence agency would send out spam e-mail "laced with the malware, which can be tailored to covertly record audio from a computer's microphone and take snapshots with its webcam."

Although originally purportedly developed to target specific individuals the NSA identified as worthy of electronic surveillance, Greenwald reports that the information he and Gallagher reviewed reveals that leadership of the agency worked feverishly to reduce the amount of human participation in the program. The reason for the haste?

According to the NSA's own report on the system, codenamed "Turbine," it was rapidly automated in order to "allow the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually."

In other words, to allow the spooks to more quickly and easily bypass the constitutional restrictions on such surveillance tactics. The Fourth Amendment reads:

> 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.

Operation Turbine, then, is a direct violation of these protections, especially that mandating that a warrant "particularly describe" the target of the search.

Unsurprisingly, the NSA had no comment when The Intercept asked about the hacking program. Instead, they referred Greenwald to a statement made by President Obama.

"As the president made clear on 17 January," the agency said in a statement published in Greenwald's story, "signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes."

While the NSA's efforts to hack the computers of "millions" of members of "groups" using Facebook is just being publicized, the social media site's collaboration with the government is nothing new.

As *The New American* reported last year, in 2012 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 summer, 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, another secret NSA program brought to light by Edward Snowden, 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 first reported by the *Washington Post*.

Another document in the Snowden cache 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."

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.

Apart from the collusion of tech giants in the construction of the surveillance state, the federal government's ability to hack individual computers and assume remote control of targets' webcams and microphones has been previously reported, as well.

In December 2013, *The New American* reported on a *Washington Post* story that revealed that an elite team of hackers employed by the Federal Bureau of Investigation (FBI) had developed an application that turns on built-in laptop cameras. According to details provided in the *Post's* 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.

Another critical and constitutionally offensive aspect of Turbine is described in The Intercept report:

> TURBINE was designed to make deploying malware much easier for the NSA's hackers by reducing their role in overseeing its functions. The system would "relieve the user from needing to know/care about the details," the NSA's Technology Directorate notes in one secret document from 2009. "For example, a user should be able to ask for 'all details about application X' and not need to know how and where the application keeps files, registry entries, user application data, etc."

There is something very sinister in this design. Keeping humans as removed as possible from the surveillance decision making provides an easy out for NSA leadership should Congress ever develop a spine and attempt to exercise genuine oversight. Any future witness could simply claim that the surveillance was carried out by computer and thus no human was ever guilty of violating constitutional proscriptions.

While we wait for Congress to call the NSA to the carpet and answer for the programs and policies made public in the Snowden files, states can and must thwart the agency's efforts to spy on citizens by refusing to cooperate in the scheme. Several such efforts are currently underway.

Although Facebook has had no official response to these latest revelations of the NSA's co-opting of its brand as a surveillance tool, CEO and founder Mark Zuckerberg reported Thursday that he called 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."

Confused or not, there is little doubt that as Facebook users become aware that NSA agents are pretending to be Facebook in order to download tracking malware to their computers, the Facebook brand and its value will diminish.

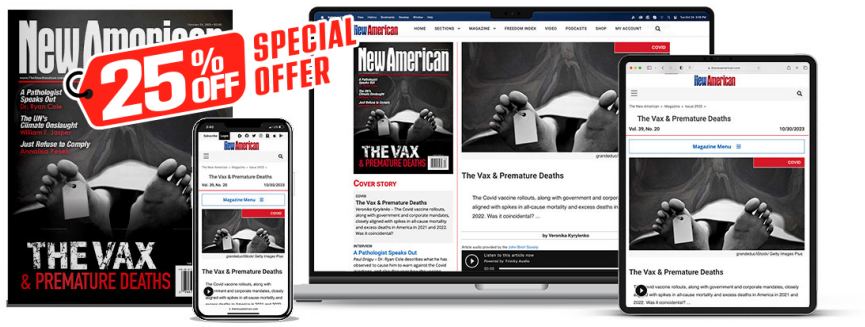
Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels nationwide speaking on nullification, the Second Amendment, the surveillance state, and other constitutional issues. Follow him on Twitter @TNAJoeWolverton and he can be reached at jwolverton@thenewamerican.com.*

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

Subscribe