Written by **Joe Wolverton, II, J.D.** on October 27, 2013

Document Reveals NSA Monitored 125 Billion Phone Calls in One Month

The Fourth Amendment protects 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."

Based on reports of the number of domestic phone calls being recorded by the National Security Agency, the Obama administration must have probable cause to suspect millions of us of threatening national security.

According to recent news reports (see here), documents obtained by former NSA contractor turned whistleblower Edward Snowden reveal that, in a 30-day period earlier this year, the NSA recorded data on 124.8 billion phone calls, about 3 billion of which originated within the United States.

The program, first reported by *The Guardian*, is appropriately code-named "Boundless Informant," and it involves the monitoring and recording of phone calls and Internet communication. *The Guardian* reports that Boundless Informant "allows users to select a country on a map and view the meta data volume and select details about the collections against that country."

While it is unlikely that the actual conversations themselves were recorded by the NSA, the fact that any information on a phone call was recorded without conforming to the Constitution is alarming. Regardless of the volume of recordings or the amount or type of data stored, a single act of warrantless surveillance violates the Constitution and everyone who ordered or participated in the program should be held accountable.

Of course, Boundless Informant isn't the only such unconstitutional program being carried out by the snoops.

Among the most disturbing disclosures found within the reams of 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 Verizon has asserted that even one of the millions whose phone records were seized fits that description.

Glen Greenwald, formerly of *The Guardian*, details the type of data being seized by the NSA:

> The information is classed as "metadata," or transactional information, rather than communications, and so does not require individual warrants to access. The document also specifies that such "metadata" is not limited to the aforementioned items. A 2005 court ruling judged that cell site location data — the nearest cell tower a phone was connected to — was also transactional data, and so could potentially fall under the scope of the order.
>
> While the order itself does not include either the contents of messages or the personal information of the subscriber of any particular cell number, its collection would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively.

Perhaps the most disturbing take-away from the leak of this secret court document ordering Verizon to hand over customer call logs and other data to a federal surveillance agency is the fact that the government considers the protections of the Fourth Amendment to be nothing more than a "parchment barrier" that is easily torn through. The Obama administration regards the Constitution — as did the Bush administration before it — as advisory at best.

Of course, being a subcontractor in the construction of the surveillance state pays handsomely. As reported by *The New American*, on August 16 Verizon announced that it was awarded a 10-year, $10-billion contract "to provide cloud and hosting services" to the U.S. Department of the Interior.

Apparently, crimes against the Constitution pay, and they pay very well.

Over the past few weeks, Facebook, Google, and other technology companies which were implicated in the revelations of the covert NSA surveillance program known as PRISM have 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, 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.

On July 31, Glen Greenwald revealed another NSA surveillance tactic similar in scope to Boundless Informant.

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."

It is important to note that like Boundless Informant, XKeyscore doesn't record phone conversations. There is evidence, however, that the NSA records every one of those, as well, and stores the content in one of its many data warehouses, such as the one in Utah that goes online within weeks.

Of course, there is no doubt that mobile phone conversations are being recorded.

The federal government is remotely activating the microphones and cameras in Android smartphones and Windows laptops, according to a report published by the *Wall Street Journal* on August 3.

Citing a "former US official," the *Journal* says court documents reveal that the FBI is using a variety of "hacking" tools to ramp up the scope of the surveillance of millions of Americans, keeping many unwittingly under the watchful eye of Washington.

One of the *Journal's* anonymous sources described a part of the FBI called the "Remote Operations Unit." Agents in this specialized unit prefer, if possible, to install the remote control software by uploading to the target's computer using a USB flash drive. When the g-men-cum-hackers can't get access to the target's computer, they install the surveillance software over the Internet "using a document or link that loads software when the person clicks or views it."

It is not only possible for the federal government to listen to your conversations using the microphone in your Android smartphone and watch you while you sit in your own home on your own computer, but they do so regularly and can do so very easily.

Purportedly, the FBI has been using these methods of surveillance "for over a decade," but their use

has come to light only recently by way of "court documents and interviews" with people familiar with the programs.

Details of the surveillance conducted under the Boundless Informant program provided by the website Cryptome are illuminating and incriminating. They are available here.

There is no excuse for this type of unconstitutional sanctioned surveillance. One unwarranted wiretap, one unwarranted seizure of a phone record, one search of records of an individual's digital communications is too many. If we are a Republic of laws, then the supreme constitutional law of the land must be adhered to. The standard is not whether or not the spies or their bosses think the violations are keeping us safe. The standard is the Constitution — for every issue, on every occasion, with no exceptions. Anything less than that is a step toward tyranny.

Taken together, the roster of snooping programs in use by the federal government places every American under the threat of constant surveillance. The courts, Congress, and the president have formed an unholy alliance bent on obliterating the Constitution and establishing a country where every citizen is a suspect and is perpetually under the never-blinking eye of the government.

The establishment will likely continue construction of the surveillance until the entire country is being watched around the clock and every monitored activity is recorded and made retrievable by agents who will have a dossier on every American.

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 is the host of* The New American Review *radio show that is simulcast on YouTube every Monday. Follow him on Twitter @TNAJoeWolverton and he can be reached at jwolverton@thenewamerican.com*