Written by **Joe Wolverton, II, J.D.** on August 22, 2013

NSA Surveillance Covers 75 Percent of Internet Traffic, WSJ Reports

When does 1.6 percent equal 75 percent? When the math is being done by the National Security Agency (NSA).

On Wednesday, August 21, citing information provided by unnamed "current and former officials," the *Wall Street Journal* reported on a slate of NSA surveillance operations that are broader and more invasive than previously admitted by the federal intelligence community.

"The system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say," write Siobhan Gorman and Jennifer Valentino-Devries for the *Wall Street Journal*.

How does the NSA conduct such wide-reaching monitoring? With the help of the country's telecommunication companies, which give the agency direct access to the lines of communication. Again, from the *Wall Street Journal article*:

> The programs, code-named Blarney, Fairview, Oakstar, Lithium and Stormbrew, among others, filter and gather information at major telecommunications companies. Blarney, for instance, was established with AT&T Inc. former officials say. AT&T declined to comment.
>
> This filtering takes place at more than a dozen locations at major Internet junctions in the U.S., officials say. Previously, any NSA filtering of this kind was largely believed to be happening near points where undersea or other foreign cables enter the country.

The New American reported recently on the NSA's tapping of the undersea cables that conduct data internationally.

Writing for the *Atlantic*, Olga Khazan reported:

> In addition to gaining access to web companies' servers and asking for phone metadata, we've now learned that both the U.S. and the U.K. spy agencies are tapping directly into the Internet's backbone — the undersea fiber optic cables that shuttle online communications between countries and servers. For some privacy activists, this process is even more worrisome than monitoring call metadata because it allows governments to make copies of everything that transverses these cables, if they wanted to.

The amount of data being grabbed by British and American snoops is astounding. The information provided by Snowden reveals that the taps on the undersea fiber-optic cables collect around "21 million gigabytes per day." The bulk data is then sent on to 550 NSA and British intelligence agents who will comb through and collate the material collected from the "at least 200 fiber optic cables so far."

As noted in the *Washington Post*, "more than 550,000 miles of flexible undersea cables about the size of

garden watering hoses carry all the world's emails, searches, and tweets. Together, they shoot the equivalent of several hundred Libraries of Congress worth of information back and forth every day."

What type of communication is flowing from this global fountain of information? The *Guardian* (U.K.) reported that the collection "includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites — all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets."

When the surveillance activities revealed in the *Wall Street Journal* story are combined with those disclosed in the documents leaked by former NSA contractor Edward Snowden, it becomes obvious that there is not a single phone call, a single text message, a single social media post, or a single e-mail sent by a single American that is not collected, collated, and cataloged by the federal government.

In a story covered by *The New American*, the NSA refutes this claim. In a seven-page memo, the agency admits to only "touching" 1.6% of internet traffic, adding of only "0.025% is actually selected for review." Seems that surveillance ciphering is a bit more fuzzy math.

The *Wall Street Journal's* estimate of the amount of private data being watched is much higher:

> The surveillance system is built on relationships with telecommunications carriers that together cover about 75% of U.S. Internet communications. They must hand over what the NSA asks for under orders from the secret Foreign Intelligence Surveillance Court. The firms search Internet traffic based on the NSA's criteria, current and former officials say.
>
> Verizon Communications Inc., for example, has placed intercepts in the largest U.S. metropolitan areas, according to one person familiar with the technology. It isn't clear how much information these intercepts send to the NSA. A Verizon spokesman declined to comment.

Verizon's willingness to give the federal government unfettered access to its customers' phone records is paying off handsomely for the telecommunications giant.

Verizon announced on August 16:

> The U.S. Department of the Interior has selected Verizon to participate in a $10 billion, 10-year contract to provide cloud and hosting services. This is potentially one of Verizon's largest federal cloud contracts to date.
>
> Verizon is one of 10 companies that will compete to offer cloud-based storage, secure file transfer, virtual machine, and database, Web, and development and test environment hosting services. The company is also one of four selected to offer SAP application hosting services.
>
> Each of the 10 agreements awarded under the Foundation Cloud Hosting Services contract has a potential maximum value of $1 billion.

Put simply, not only has Verizon not suffered a loss of customers since revelations of its collusion with the National Security Agency's dragnet surveillance of millions of Americans' phone records, but now the company is being paid billions for its cooperation.

Verizon isn't the only telecommunication company colluding with the NSA to expose its customers' private electronic communications to the surveillance of the federal government, however.

During the 2002 Winter Olympics hosted by Salt Lake City, Utah, the NSA and FBI "arranged with Qwest Communications International Inc. to use intercept equipment for a period of less than six months around the time of the event. It monitored the content of all email and text communications in

the Salt Lake City area."

Century Link — the company that acquired Qwest Communications in 2010 — refused to comment on the Wall Street Journal story when contacted by The New American.

All e-mail and text communication. That description alone is enough to justify an immediate suspension of all surveillance programs carried on by an agency whose authority specifically forbids monitoring of purely domestic communication.

Then, of course, there is the constitutional standard that is no longer applied to the federal government generally and federal snooping particularly.

The Fourth Amendment guarantees that "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."

"It is difficult to know how much domestic data NSA is inadvertently retaining," the *Wall Street Journal* piece claims. It is not difficult to know, however, that nearly all of it is being retained in open and hostile violation of the Constitution and that these officially sanctioned deprivations of Americans' fundamental civil liberties will continue until Americans and their elected representatives demand that the Constitution be applied and that without a qualifying warrant, not a single second of a telephone conversation, a single social media post, a single e-mail, or a single text message be searched and seized.

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.*