Written by **Joe Wolverton, II, J.D.** on July 24, 2013

NSA Taps Directly Into Undersea Fiber-optic Data Cables

Despite promises from a few federal lawmakers to hold the Obama administration and the National Security Agency (NSA) accountable for the recently revealed practice of wholesale surveillance of millions of Americans, to date, nothing has been done.

In fact, as *The New American* reported last week, congressional impotence is likely to let Director of National Intelligence James Clapper escape any accountability for the lies he told under oath while testifying about the scope of the domestic spying program.

Of course, as the mainstream media maintains its attention laser-locked on Edward Snowden — the former NSA contractor who leaked the documents last month — Americans recognize that neither Snowden's whereabouts nor his love life are of the slightest importance.

What matters is that one branch of the federal government (the executive) is unconstitutionally spying on Americans, another branch of the federal government (the legislative) is refusing to check that exercise of power, and a third branch (the judicial) is rubber-stamping all requests to keep the data pipeline open.

And, as the *Atlantic* reports, in many cases, a pipeline is exactly what is being tapped by the NSA. Writing for the *Atlantic*, Olga Khazan reports:

> 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 kind of communication is flowing from this global fountain of information? *The Guardian* (U.K.) reports 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."

The takeaway: 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.

While tapping undersea cables sounds a bit James Bond-esque, the truth is more impressive than fiction. Again, from the *Atlantic*:

> The easiest place to get into the cables is at the regeneration points — spots where their signals are amplified and pushed forward on their long, circuitous journeys. "At these spots, the fiber optics can be more easily tapped, because they are no longer bundled together, rather laid out individually," Deutsche Welle reported.
>
> But such aquatic endeavors may no longer even be necessary. The cables make landfall at coastal stations in various countries, where their data is sent on to domestic networks, and it's easier to tap them on land than underwater.

The next step in the process is almost unbelievable given the name of the NSA's Internet surveillance program: PRISM. According to the story in the *Atlantic*, the snoops use an actual prism to collect the data and keep those on the look out for interception off the agency's trail. Olga Khazan reports:

> The tapping process apparently involves using so-called "intercept probes." According to two analysts I spoke to, the intelligence agencies likely gain access to the landing stations, usually with the permission of the host countries or operating companies, and use these small devices to capture the light being sent across the cable. The probe bounces the light through a prism, makes a copy of it, and turns it into binary data without disrupting the flow of the original Internet traffic.

Capture the light, but keep it all in darkness.

As the data comes in, it is scoured by agents on both sides of the Atlantic Ocean who are looking for any occurrence of one of the more than 40,000 search terms that the intelligence community has determined are evidence of evil intent.

Terrorism, as legally defined, is a tactic, not a crime. Since the attacks of September 11, 2001, however, everyone is a potential suspect, regardless of the reason for the use of the words that trigger the alarms.

Lest anyone think that President Obama drew up the plans for the construction of the surveillance state, the *Atlantic* reminds readers that the previous administration is more properly identified as the architect.

> It's also worth noting that this type of tapping has been going on for years — it's just that we're now newly getting worked up about it. In 2007, the *New York Times* thus described President Bush's expansion of electronic surveillance: "the new law allows the government to eavesdrop on those conversations without warrants — latching on to those giant switches — as long as the target of the government's surveillance is 'reasonably believed' to be overseas."

All these activities violate the Fourth Amendment requirement that "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." In practical terms, that means that the federal government cannot purposely monitor the phone or Internet communications carried on by an American or a person inside the United States without a qualifying warrant.

Of course, by tapping directly into the beams of light transferring this data around the globe — apparently with the cooperation of the world's chief technology companies — the federal government

bypasses all legal and constitutional restraints on its already immense power.

Remarkably, as the depths of the surveillance are plumbed by *The New American* and other outlets of the liberty movement, there does not seem to be a corresponding flight by Americans from the devices or services being monitored by the federal government.

According to BNAMericas online:

> Worldwide smartphone sales are expected to reach 1bn units in 2013, compared to 675mn in 2012, research and consultancy firm Gartner said in a release.
>
> Meanwhile, tablets are also expected to see continued rapid growth this year, with unit sales increasing 69.8% to 197mn.

As one brick after another is stacked on the ever-growing walls of the 21st-century Panopticon, it appears that nothing will dissuade Americans from growing increasingly reliant on the very tools being used in the construction.

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.*