FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

Security

What we still don't know about the NSA's Internet surveillance

By ProPublica *Jul 23, 2013*

By Justin Elliott
ProPublica

Among the snooping revelations of recent weeks, there have been tantalizing bits of evidence that the NSA is tapping fiber-optic cables that carry nearly all [submarine-cable-map-2013.telegeography.com/] international phone and Internet data.

The idea that the NSA is sweeping up vast data streams via cables and other infrastructure — often described as the "backbone of the Internet" — is not new. In late 2005 [www.nytimes.com/2005/12/24/politics/24spy.html], the New York Times first described the tapping, which began after the Sept. 11, 2001 attacks. More details emerged in early 2006 when an AT&T whistleblower came forward [www.wired.com/science/discoveries/news/2006/04/70621].

But like other aspects [www.propublica.org/article/nsa-black-hole-5-basic-things-we-still-dont-know-the-governments-snoop] of NSA surveillance, virtually everything about this kind of NSA surveillance is highly secret and we're left with far from a full picture.

Is the NSA really sucking up everything?

It's not clear.

The most detailed, though now dated, information on the topic comes from Mark Klein. He's the former AT&T technician who went public [www.wired.com/science/discoveries/news/2006/04/70621] in 2006 describing the installation in 2002-03 of a secret room in an AT&T building in San Francisco. The equipment, detailed in technical documents [www.wired.com/threatlevel/2007/05/mark_klein_docu/], allowed the NSA to conduct what Klein described as "vacuum-cleaner surveillance of all the data crossing the internet -- whether that be peoples' e-mail, web surfing or any other data."

Klein said [www.wired.com/politics/onlinerights/news/2007/05/kleininterview] he was told there was similar equipment installed at AT&T facilities in San Diego, Seattle, and San Jose.

There is also evidence that the vacuuming has continued in some form right up to the present.

A draft NSA inspector's general report from 2009, recently published [apps.washingtonpost.com/g/page/world/national-security-agency-inspector-general-draft-report/277/] by the Washington Post, refers to [www.propublica.org/documents/item/728006-nsa-ig-report#document/p37/a110288] access via two companies "to large volumes of foreign-to-foreign communications transiting the United States through fiberoptic cables, gateway switches, and data networks."

Recent stories by the Associated Press [bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure] and the Washington Post [www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_print.html] also described the NSA's cable-tapping, but neither included details on the scope of this surveillance.

A recently published NSA slide, dated April 2013 [www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/], refers to so-called "Upstream" "collection" of "communications on fiber cables and infrastructure as data flows past."

These cables carry vast quantities of information, including 99 percent of international phone and Internet data, according to research firm TeleGeography [www.telegeography.com/].

This upstream surveillance is in contrast to another method of NSA snooping, Prism, in which the NSA isn't tapping anything. Instead, the agency gets users' data with the cooperation of tech companies like Facebook and Google.

Other documents leaked by Edward Snowden to the Guardian [www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa/print] provide much more detail about the upstream surveillance by the British Government Communications Headquarters (GCHQ), the NSA's U.K. counterpart.

GCHQ taps cables where they land in the United Kingdom carrying Internet and, phone data. According to the Guardian, unnamed companies serve as "intercept partners" in the effort.

The NSA is listening in on those taps too. By May 2012, 250 NSA analysts along with 300 GCHQ analysts were sifting through the data from the British taps.

Is purely domestic communication being swept up in the NSA's upstream surveillance?

It's not at all clear.

Going back to the revelations of former AT&T technician Mark Klein — which, again, date back a decade — a detailed expert analysis [www.propublica.org/documents/item/727974-expert-analysis-of-nsas-at-amp-t-tapping] concluded that the secret NSA equipment installed at an AT&T building was capable of collecting information "not only for communications to overseas locations, but for purely domestic communications as well."

On the other hand, the 2009 NSA inspector general report refers specifically to [www.propublica.org/documents/item/728006-nsa-ig-report#document/p37/a110288] collecting "foreign-to-foreign communications" that are "transiting the United States through fiber-optic cables, gateway switches, and data networks"

But even if the NSA is tapping only international fiber optic cables, it could still pick up communications between Americans in the U.S.

That's because data flowing over the Internet does not always take the most efficient geographic route to its destination.

Instead, says Tim Stronge of the telecom consulting firm TeleGeography [www.telegeography.com/about/index.html], data takes "the least congested route that is available to their providers."

"If you're sending an email from New York to Washington, it could go over international links," Stronge says, "but it's pretty unlikely."

That's because the United States has a robust domestic network. (That's not true for some other areas [apps.washingtonpost.com/g/page/business/a-connected-world/305/] of the world, which can have their in-country Internet traffic routed through another country's more robust network.)

But there are other scenarios under which Americans' purely domestic communication might pass over the international cables. Google, for example, maintains a network of data centers [www.google.com/about/datacenters/inside/locations/index.html] around the world.

Google spokeswoman Nadja Blagojevic told ProPublica that, "Rather than storing each user's data on a single machine or set of machines, we distribute all data — including our own — across many computers in different locations."

We asked Blagojevic whether Google stores copies of Americans' data abroad, for example users' Gmail accounts. She declined to answer.

Are companies still cooperating with the NSA's Internet tapping?

We don't know.

The Washington Post had a story earlier this month about agreements [www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_print.html] the government has struck with telecoms, but lots of details are still unclear, including what the government is getting, and how many companies are cooperating.

The Post pointed to a 2003 "Network Security Agreement" between the U.S. government and the fiber optic network operator Global Crossing, which at the time was being sold to a foreign firm.

That agreement, which the Post says became a model for similar deals with other companies, did not authorize surveillance. Rather, the newspaper reported, citing unnamed sources, it ensured "that when U.S. government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely."

Global Crossing was later sold to Colorado-based Level 3 Communications [www.level3.com/], which owns many international fiber optic cables [maps.level3.com/default/#.Uehp8WTF1FA], and the 2003 agreement was replaced in 2011.

Level 3 released a statement [level3.mediaroom.com/2013-07-11-Level-3-Issues-Statement] in response to the Post story saying that neither agreement requires Level 3 "to cooperate in unauthorized surveillance on U.S. or foreign soil."

The agreement [apps.fcc.gov/ecfs/document/view;jsessionid=knJvRpVh8tHQJGXLFC16ghK8pGNg3JNqG6BcYDvs1Gr6J95WTntl%21-1272756975%211291806534?id=7021711201] does, however, explicitly require the company to cooperate with "lawful" surveillance.

More evidence, though somewhat dated, of corporate cooperation with NSA upstream surveillance comes from the 2009 inspector general report.

"Two of the most productive [signals intelligence] collection partnerships that NSA has with the private sector are with COMPANY A and COMPANY B," the report says [www.propublica.org/documents/item/728006-nsa-ig-report#document/p37/a110288]. "These two relationships enable NSA to access large volumes of foreign-to-foreign communications transiting the United States through fiber-optic cables, gateway switches, and data networks."

There's circumstantial evidence [news.cnet.com/8301-13578_3-57591391-38/surveillance-partnership-between-nsa-and-telcos-points-to-at-t-verizon/] that those companies may be AT&T and Verizon.

It's also worth noting that the NSA might not need corporate cooperation in all cases. In 2005, the AP reported on [www.nytimes.com/2005/02/20/politics/20submarine.html] the outfitting of the submarine Jimmy Carter to place taps on undersea fiber-optic cables in case "stations that receive and transmit the communications along the lines are on foreign soil or otherwise inaccessible."

What legal authority is the NSA using for upstream surveillance?

It's unclear, though it may be a 2008 law that expanded the government's surveillance powers.

The only evidence that speaks directly to this issue is the leaked slide on upstream surveillance, and in particular the document's heading: "FAA702 Operations." That's a reference to Section 702 of the 2008 FISA Amendments Act. That legislation amended the Foreign Intelligence Surveillance Act, the 1970s law [projects.propublica.org/graphics/surveillance-timeline] that governs government surveillance in the United States.

Under Section 702 [www.propublica.org/documents/item/729378-fisa-amendments-act-of-2008#document/p4], the attorney general and director of national intelligence issue one-year blanket authorizations to for surveillance of non-citizens who are "reasonably believed" to be outside the U.S. These authorizations don't have to name individuals, but rather allow for targeting of broad categories of people.

The government has so-called minimization procedures that are supposed to limit the surveillance of American citizens or people in the U.S. Those procedures are subject to review [www.propublica.org/documents/item/729378-fisa-amendments-act-of-2008#document/p9/a110656] by the FISA court.

Despite the procedures, there is evidence that in practice American communications are swept up by surveillance under this section.

In the case of Prism, for example, which is authorized under the same part of the law, the Washington Post reported [www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html] that the NSA uses a standard of "51 percent confidence" in a target's foreignness.

And according to minimization procedures [www.documentcloud.org/documents/716634-exhibit-b.html#document/p5] dating from 2009 published by the Guardian, there are also exceptions when it comes to holding on to American communications. For example, encrypted communications — which, given the routine use of digital encryption, might include vast amounts of material — can be kept indefinitely [www.documentcloud.org/documents/716634-exhibit-b.html#document/p5].

The government also has the authority to order communications companies to assist in the surveillance [www.propublica.org/documents/item/729378-fisa-amendments-act-of-2008#document/p7/a110655], and to do so in secret.

How much Internet traffic is the NSA storing?

We don't know, but experts speculate it's a lot.

"I think that there's evidence that they're starting to move toward a model where they just store everything," says Dan Auerbach [www.eff.org/es/about/staff/dan-auerbach], a staff technologist at the Electronic Frontier Foundation. "The Utah data center [www.sltrib.com/sltrib/news/56515678-78/data-nsa-http-www.html.csp] is a big indicator of this because the sheer storage capacity has just rocketed up."

We know more details about how the GCHQ operates in Britain, again thanks to the Guardian's reporting. A breakthrough in 2011 allowed GCHQ to store metadata from its cable taps for 30 days and content for three days. The paper reported on how the spy agency — with some input from the NSA — then filters what it's getting:

> The processing centres apply a series of sophisticated computer programmes in order to filter the material through what is known as MVR – massive volume reduction. The first filter immediately rejects high-volume, low-value traffic, such as peer-to-peer downloads, which reduces the volume by about 30 percent. Others pull out packets of information relating to "selectors" – search terms including subjects, phone numbers and email addresses of interest. Some 40,000 of these were chosen by GCHQ and 31,000 by the NSA.

How does the NSA do filtering of the data it gets off cables in the United States?

"I think that's the trillion dollar question that I'm sure the NSA is working really hard at all the time," said Auerbach, the EFF expert. "I think it's an incredibly difficult problem."

About the Author

ProPublica is an independent, non-profit newsroom that produces investigative journalism in the public interest.