When the feds come knocking: The tale of a Utah ISP, a secret court order, and a little black box

Summary: *When the NSA secures a secret FISA court warrant to tap into a customer's data, what can the ISP do? Not much, one ISP owner said, who came forward to tell his story.*

By Zack Whittaker for Zero Day | July 21, 2013 -- 21:04 GMT (14:04 PDT)

(Image: CNET)

A secret court, based in a small, soundproof, and secured room (http://www.washingtonpost.com/wp-dyn/content/article/2009/03/01/AR2009030101730.html) in the E. Barrett Prettyman United States Courthouse in Washington, D.C., meets regularly to decide on new and renew existing federal surveillance orders.

Over the course of the last month and a half, the world has begun to find out more about this shadowy court, the Foreign Intelligence Surveillance Court (FISC), which was set up in 1978 under its namesake law, the Foreign Intelligence Surveillance Act (FISA). FISA authorizes some of the U.S. government's most secretive programs, including wiretapping and domestic surveillance.

Former National Security Agency (NSA) contractor turned whistleblower Edward Snowden's leaks (http://www.zdnet.com/u-s-govt-files-charges-against-snowden-over-nsa-leak-7000017165/) brought to light some details, albeit not many, relating to these secretive warrants and orders handed down by the court.

Read this

But little did we know of logistics; specifically, how they are handed to companies that hold data on terrorism suspects and foreign spies who are living and working in the United States. It was unclear how such orders remained secret, whose hands exchanged these secretive orders, and

how complicit Internet providers and Web companies holding this data were in the collection of vast amounts of citizen data.

NSA: All up in your privacy junk since 1952

Read more

Until Friday, when the chief executive of one Utah-based Internet service provider (ISP) spoke out.

XMission is one of Utah's largest, and one of few independent, Internet providers in the state. Pete Ashdown, the company's chief executive, spoke to BuzzFeed on Friday (http://www.buzzfeed.com/justinesharrock/what-is-that-box-when-the-nsa-shows-up-at-your-internet-comp) about how he received a warrant under FISA in 2010.

He also received a "broad" gagging order, likely a National Security Letter, under Section 505 of the Patriot Act (https://www.eff.org/issues/national-security-letters) .

For nine months, XMission was forced to install a "little black box" that was capturing all the traffic to one particular customer: "Everything they were sending and receiving," he said.

It's a solid, well-written, and informative read. And you should take 10 minutes to put a pot of coffee on and have a read. It's not often that we effectively point to another news site's work and say, "go, read!" but this is certainly one of those times.

There are, however, some additional things to know, before or after you read the BuzzFeed piece (http://www.buzzfeed.com/justinesharrock/what-is-that-box-when-the-nsa-shows-up-at-your-internet-comp) .

FISA court orders so secret, they are served but not handed over

The Verizon order served by the FISA court (http://www.zdnet.com/verizons-secret-data-order-timed-to-expire-but-nsa-spying-likely-to-carry-on-7000018321/) was likely not given to anyone outside the intelligence community. Leaked by Snowden, the process described in the BuzzFeed article (http://www.buzzfeed.com/justinesharrock/what-is-that-box-when-the-nsa-shows-up-at-your-internet-comp) suggests that these orders are so secret that even those served with a FISA court order aren't allowed to keep it. The NSA and others likely keep these orders for their own records for legal justification.

Who knows about the FISA court order?

The process in which the FISA court order is handed down is interesting. Again, the Verizon order (http://www.zdnet.com/verizon-records-vacuumed-up-by-nsa-under-top-secret-patriot-act-order-7000016441/) was to be served to the "custodian of the records."

In June, Verizon declined to comment to ZDNet on what this job title meant. In some cases, it's the company's chief security, privacy, or information officer (CSO, CPO, CIO, respectively). In some case, it's the chief counsel or company lawyer, but not always the chief executive or even members of the board.

This is wiretapping. How does this play with PRISM?

It does and it doesn't. PRISM and "Upstream," the second named program in the NSA spying scandal. The slides noted that NSA analysts "should use both" systems (http://www.guardian.co.uk/world/2013/jun/08/nsa-surveillance-prism-obama-live?guni=Network%20front:network-front%20full-width-1%20bento-box:Bento%20box:Position1:sublinks#block-51b36893e4b0cc6424372292) .

PRISM is a tool that allowed the U.S. government to send FISA Section 702 orders to acquire intelligence for judicial purposes. Upstream is an umbrella program, consisting of various working elements and separate programs — codenamed FAIRVIEW, BLARNEY, and others (http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet-7000016565/) — which mostly involve collecting data from Tier 1 fiber network operators under FISA court orders.

Equipment would be installed at specific points outside the reach of the seven named companies, and would siphon off vast amounts of data.

It's possible that filters are applied to data collected by Upstream, as described by the leaks showing how the U.K. intelligence agency GCHQ filters peer-to-peer and other unnecessary data by up to 30 percent (http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101) . From there, specific data can be pulled out and PRISM could be used to serve companies with Section 702 orders for judicial purposes, in order to preserve the bulk intelligence collection by the NSA on Tier 1 networks.

Did the chief executives of the seven named technology companies know about the FISA court orders?

Regarding PRISM, there was talk of how much the companies actually knew. Were they complicit in allowing the feds in? Or were they forced under law?

The likely case, as we can see from the Utah-based Internet provider, is that FISA forces companies to comply. FISA is like the "sonic screwdriver" (to use a *Doctor Who* analogy) to all data protection barriers in the United States.

Read this

PRISM: Here's how the NSA wiretapped the Internet

The National Security Agency's "PRISM" program is able to collect, in realtime, intelligence not limited to social networks and email accounts. But the seven tech companies accused of opening 'back doors' to the spy agency could well be proven innocent.

Read more

Electronic Frontier Foundation (EFF) senior staff attorney Kurt Opsahl told ZDNet last month on the phone that existing law — specifically Section 215(d) (http://www.law.cornell.edu/uscode/text/50/1861) of the Patriot Act, which amended FISA 1978 for this reason, among others — allows companies that are handed FISA court orders the opportunity to challenge the "gagging" clauses. These clauses that govern the use of National Security Letters were proven unconstitutional (http://www.zdnet.com/google-fails-to-strike-down-fbis-secret-gagging-orders-despite-constitutionality-concerns-7000016185/) in 2008. The law was changed to allow for these gagging orders to be appealed (http://arstechnica.com/tech-policy/2008/12/appeals-court-puts-restrictions-on-nsl-gag-orders/) .

Section 215(d) allows three provisions for disclosure. The first is to disclose the FISA court order to "those persons to whom disclosure is necessary to comply with such order." Technically, as the Buzzfeed piece notes (http://buzzfeed.com/justinesharrock/what-is-that-box-when-the-nsa-shows-up-at-your-internet-comp) , a company chief executive counts.

Secondly, companies are allowed to "obtain legal advice or assistance with respect to the production of things in response to the order," which, Opsahl noted, translates as hiring a lawyer to specifically oversee the legal handover of data to U.S. authorities.

Thirdly, the director of the Federal Bureau of Investigation (FBI) can specifically designated a person who may be informed of the FISA court order. This may or may not include the chief executive, who may or may not have to authorize internal company matters.

"Everyone sees a different interpretation," Opsahl said on the phone.

But this is where it gets interesting. The chief executive of a company doesn't have to know, in order to maintain a level of plausible deniability. This prevents — particularly in cases of publicly traded companies — chief executives and senior staff from effectively lying to shareholders and investors, if asked, about government requests for data.

A company chief executive can presume that their company is receiving FISA court orders, and can set in motion with CPOs, CSOs, or chief legal officers or counsel to take care of the details held within those orders. This distances the chief executive, and others — such as spokespeople — in a company from misinforming the public about what they know.

Did the seven named technology companies know about these FISA orders?

Essentialy, yes and no. The likelihood is that the chief executives did not know about the specifics of FISA court orders. But these companies, like any other company or business operating in the U.S., must comply with the law nonetheless.

While there are no figures to support this — the chances are such figures would be classified — in the lawyers and privacy groups that ZDNet spoke to over the last few months, it is not known whether a company has successfully challenged a FISA court order.

Topics: Security, Privacy

About Zack Whittaker

Zack Whittaker writes for ZDNet, CNET and CBS News. He is based in New York City.