KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

NSA SPYING UNDER SECTION 215 OF THE PATRIOT ACT: ILLEGAL, OVERBROAD, AND UNNECESSARY

June 19, 2013

An order of the super secret Foreign Intelligence Surveillance Court (FISC) that came to light on June 5 has lead to revelations that the National Security Agency (NSA) has for seven years been collecting metadata about virtually all telephone and cell phone calls made within the United States and between the United States and foreign countries. The program is inconsistent with the statutory authorization under which it is conducted, and has grave implications for other surveillance programs and for privacy in the United States. We describe the program more fully below, the statute on which it is based, how intelligence and law enforcement officials deceived the public about the program, and what we think should be done about it.

I. The Program

The FISA Court has ordered communications carriers that handle most of the telephone calls made in the U.S. – Verizon, AT&T, Sprint, and presumably others – to turn over to the NSA "telephony data" on a daily, ongoing basis on all of the calls they handle, both cellular and landline. The FBI filed the applications for the orders; the call records go directly to a military intelligence agency, the NSA. The call records include: (i) numbers dialed to and from each telephone or cell phone, (ii) the time at which each call was made; (iii) the duration of each call; (iv) the number that uniquely identifies any cell phone (the International Mobile Station Equipment Identity number, or IMEI number), and (v) the number that uniquely identifies the SIM card used in the phone (the International Mobile Subscriber Identity number, or IMSI number).

With this data, the government can track who called whom, when, and for how long. Attaching a name to the phone numbers involved is a trivial exercise that can be accomplished through public databases and with the assistance of providers. If a person purchases a new cell phone and switches out the SIM card from her old phone, the calls she made from her old phone can be tracked against the calls she makes on the new one, thus establishing unbroken continuity of tracking capability. The data are then used to establish associations among people.

This data is collected in bulk without any particularized suspicion about an individual, phone number or device. Instead of obtaining particularlized calling data from providers only when the government provides to the FISC facts establishing that a specific person, piece of equipment, or phone number is relevant to an investigation, the NSA has collected information on everyone's

phone calls on a massive scale. Intelligence officials admit that less than 1% of the data gathered is actually used, making the collection of personal calling information all the more troubling and of questionable utility. The records are held for five years so they can be queried later.

The records are queried not when the FISA Court has determined that any particular record or any particular query is relevant to an investigation, but when an intelligence agent has determined that ,"… there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." This convoluted standard, which appears nowhere in any law, was first publicly articulated in talking points the Director of National Intelligence circulated on June 6.

In other words, the NSA obtains information on all calls to, from, and within the United States, then it queries the information when it decides it has met a convoluted standard that it created and that appears in no statute. The FISC has signed off on this "collect everything" approach.

II. The Law

The law under which this surveillance is conducted, Section 215 of the PATRIOT Act,[1] contemplates the opposite: The restriction is on gathering the data, not just on its use.

An order under Section 215 may not be issued unless the FISA Court finds, based on an FBI application, that:

> …there is a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with [guidelines for intelligence investigations approved by the Attorney General] to obtain foreign intelligence information not concerning a [U.S. citizen or lawful permanent resident] or to protect against international terrorism or clandestine intelligence activities….

Absent a finding that facts establish reasonable grounds to believe the things sought are relevant to an investigation, the order requiring those things be produced cannot issue. This is a restriction both on the information the government can gather and on how it can be used.

Prior to the PATRIOT Act, this provision[2] was narrower in four ways. First, only information that pertained to a terrorist, spy or other agent of a foreign power could be collected. Because few Americans qualify as an "agent of a foreign power," the provision was seldom used to obtain business records pertaining to Americans. Second, the records had to pertain to a particular person or entity; mere pertinence to an investigation would not suffice. Third, only "business records" could be sought. Finally, the records could only be sought from common carriers (such as airlines, trains and bus services), hotels, car rental agencies, and physical storage facilities. The PATRIOT Act removed all of these limitations. Now, Section 215 orders can seek any "tangible thing," not just business records. These "tangible things" can be sought from any person or entity, not just from travel and storage-related businesses. Finally, the "tangible

[1] Codified at 50 USC Section 1861a.

[2] In 1998, Congress adopted section 602 of the Intelligence Authorization Act of 1999. It created a very limited authority to obtain business records under FISA.

things" sought need not pertain to a suspected terrorist or spy; they only need pertain to an investigation, the scope of which is in the government's control. Most of the amendments proposed to Section 215 focus on requiring ties between the records sought and a terrorist, spy, or other agent of a foreign power.

III. The Illegality

The FBI and NSA have chosen to go beyond even the broad authority that Section 215 confers. Using Section 215 to obtain records of every phone call made to, from or within the U.S. is inconsistent with Section 215 in three ways: it is overbroad, prospective and without meaningful judicial control.

A. Overbreadth

First, the program collects data on virtually all calls in the U.S. The only way this can be squared with Section 215 is if the investigation for which these records are sought has been defined so broadly as to make the telephone calls of every person in the U.S. relevant to the investigation. This is fantastically overbroad, and was not contemplated by Congress when Section 215 was adopted.[3] CDT has long warned that intelligence investigations to protect against terrorism can be much broader than investigations of criminal activity, and therefore warrant additional safeguards. However, this investigation seems even broader even than we could have imagined.

Such overbroad investigation may be occurring under other authorities that do not even have any level of judicial review. For example, a National Security Letter (NSL) statute codified at 18 USC 2709 permits every FBI field office to demand of a communications service provider the name, address, length of service and local and long distance toll billing records of a person or entity upon mere certification that the information sought is relevant to an investigation to protect against international terrorism. Similar "relevant to an investigation" language appears in the NSL statutes that govern collection of customer financial records and credit records held by financial institutions and credit agencies. The same reasoning that makes all phone calls relevant to an investigation to prevent terrorism may make financial and credit records of every one relevant as well, and the NSA is reportedly collecting this information as well. The difference, of course, is that the FBI can compel financial institutions and credit bureaus to disclose the credit and financial information simply by writing a letter and without any level of judicial involvement.

B. Prospective collection

Section 215 authorizes the FBI to obtain tangible things, but it is being used to obtain records that do not even exist when the order is issued. That is, the FBI uses Section 215 – a business records provision – for prospective surveillance. The Section 215 order that *The Guardian* published directs the provider to produce telephone metadata "on an ongoing daily basis" for the duration of the order. Congress did not contemplate prospective surveillance when it enacted Section 215. During the debate on the PATRIOT Act, no member of

[3] Senator Jeff Merkley (D-OR), for example, pulled out his Verizon-served smart phone at a June 13 hearing before the Senate Appropriations Committee and demanded that NSA Director Keith Alexander explain how Senator Merkley's cell phone records could be relevant to an FBI investigation to prevent terrorism.

Congress and no intelligence official seeking the Section 215 authority cited an example of prospective surveillance that Section 215 would authorize.

Instead, Congress gave the FBI intelligence authority to obtain telephony metadata prospectively in the pen register statute, 50 USC Section 1842. This section permits the FBI to obtain an order from the FISC authorizing the installation of a pen register (which records numbers dialed by a telephone or cell phone) or trap and trace device (which, like caller ID, records the numbers of incoming calls) for the same kinds of investigations for which a Section 215 order can be sought. But it has one important difference: particularity. A pen/trap order must specify the attributes of the communications to which the order applies, such as the number or other identifier, the location of the telephone line if known (or other facility to which the pen/trap device would be attached or applied). Particularity focuses prospective surveillance on a target, thus protecting everyone else. It is an element of every prospective electronic surveillance authority, whether criminal or intelligence-related.[4] The particularity requirements of the statute Congress enacted to govern prospective surveillance could not be met, so the FBI sought to evade them by requiring daily disclosures from storage – thereby obtaining the same information on an ongoing, prospective basis that it could obtain under a pen/trap order without meeting the particularity requirements of the law governing such prospective surveillance.

Using authorities for stored records to obtain access to records generated in the future is a dangerous road down which to travel. An order for the disclosure of the contents of records under 18 USC 2703(d) could instead require the communications service provider to disclose records "on an ongoing daily basis" effectively creating a wiretap without meeting the stringent requirements for a wiretap in the Wiretap Act. In the physical world, it could mean that a warrant to search a home could specify that the search would be conducted "on an ongoing daily basis."

C. Judicial Control

Under Section 215, the FISC, not the NSA, decides whether there are specific facts giving reason to believe the tangible things sought with the Section 215 order are relevant to an investigation. Under the phone call records program, this crucial protection is lost: Instead, the FISC orders allow the NSA to obtain everyone's phone records. An intelligence agent then accesses the records when the intelligence agent believes that, "… there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." An intelligence agent, not the court, decides whether the facts involving any particular query meet this standard. This so reduces the role of the court as to make its review insufficient: Instead of the FISC determining whether facts show that particular information is relevant to an investigation, an agent makes a different determination based on a convoluted standard that is not prescribed by law.

[4] *See*, 18 USC 2518(1)(b) (particularity for criminal wiretaps), 18 USC 3123 (particularity for criminal pen register and trap and trace surveillance), and 50 USC 1804(a) (particularity for intelligence wiretaps). Even "roving" surveillance orders issued when the identity of the target is not known require particularity. For example, a roving wiretap under 18 USC 2518(11) must "identify the person believed to be committing the offense and whose communications are to be intercepted."

IV. The Deception

Government officials repeatedly misled Congress and the public about this program. This slanted the debate about reauthorization of Section 215 of the Patriot Act: The public, and many members of Congress who voted for reauthorization, did not know how the law was being used because government officials made misleading statements about that use and also refused to release their legal interpretations of the statute even after Senators objected and sounded alarm bells.

For example, on September 21, 2011, Senators Wyden and Udall wrote Attorney General Holder complaining about, "… the repeated claims by Justice Department officials that the government's authority to obtain business records or other 'tangible things' under section 215 of the USA Patriot Act is analogous to the use of a grand jury subpoena. This comparison – which we consider highly misleading, has been made by Justice Department officials on numerous occasions, including in testimony before Congress."

On October 19, 2011, Assistant Attorney General Ron Weich wrote back and defended the analogy of Section 215 to a grand jury subpoena. He cited 50 USC Section 1861(c)(2)(D) which provides that a court order under Section 215 can only require production of a tangible thing that can be obtained with a subpoena. But he failed to mention one key difference: A grand jury subpoena is not used to compel continuing disclosures into the future as the Section 215 orders have been used. Grand jury subpoenas compel disclosure of what you have, not of what you create in the future. The analogy to grand jury subpoenas was misleading to say the least.

As another example, at a public hearing of the Senate Intelligence Committee on March 12, 2013, about threats the United States faces around the world, Senator Wyden asked Director of National Intelligence James Clapper:

> "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"
>
> Director Clapper responded, "No sir."
>
> Senator Wyden pressed him, "It does not."
>
> Director Clapper responded, "Not wittingly. There are cases where they could, inadvertently perhaps, collect, but not wittingly."

Director Clapper may have been taking the position that a call record, though acquired by the NSA and stored in an NSA database is not "collected" until it is searched upon, or until it turns up in a search. Without such clarification, his statement was misleading, and it has not been retracted or sufficiently clarified.

These deceptions are possible only because surveillance conducted under Section 215 is shrouded in secrecy. There is no notice when a person's phone call records are obtained. The communications service provider who renders up your phone records to a military intelligence agency is gagged, by law, indefinitely and cannot provide notice. The government need make no showing of harm in order to impose the gag. Finally, the FISC legal opinions that show the legal basis for authorizing the surveillance have been withheld.

V. The Alternatives

Collecting records of all of the telephone calls made in the United States, or to or from the United States, is not necessary to prevent terrorism. Records indicating whom a suspected terrorist has contacted could be useful in an investigation to prevent terrorism, but the records of everyone else are not. Section 215 should be reformed to give the government the authority to obtain tangible things that pertain to people with respect to whom the FISC finds there are specific and articulable facts creating reasonable suspicion that the person is a terrorist, spy or other agent of a foreign power.

Ironically, as Senator, Mr. Obama co-sponsored legislation that would have implemented this reform. Section 4 of the Security and Freedom Ensured ("SAFE") Act, S. 737 in the 109th Congress, would have amended Section 215 to require that showing. The amendment that *Senator* Obama sought would have precluded the overbroad investigation that *President* Obama now defends. As Congress considers how to amend Section 215 to prevent abuse, it may alter the SAFE Act formulation to include other records that pertain to specific individuals who are under investigation (as with the Amash-Conyers LIBERT-E Act, HR 2399), to ensure that each tangible thing sought is relevant to a terrorism investigation (as with the Restore Our Privacy Act, S. 1168, introduced by Sen. Bernie Sanders (I-VT)), to encourage disclosure of significant FISC interpretations of Section 215 (as with the Merkely-Wyden-Tester bill, S. 1130) and to guard against Section 215 orders that require disclosure of tangible things not yet in existence when the order is served. All of these changes would improve Section 215 and end the unparticularized acquisition of calling records under that statute.

Finally, the secrecy surrounding Section 215 should be lifted in part. To get a gag order, the government should have to make a showing of harm that would result absent the gag, and the gag order should expire by a date certain, but be renewable for additional periods upon a showing of harm. Companies that receive Section 215 orders should be freed to disclose on an annual basis both the number of orders they receive and the number of customer accounts affected by those orders. The latter disclosure would trigger inquiry when there is a huge discrepancy between the number of orders issued and the number of accounts impacted. This should be accomplished by statute, but even without an amendment to Section 215, the Department of Justice could work with companies to permit them to make the disclosures now through agreements filed with the FISC.

Conclusion

The FBI and NSA have abused Section 215 of the PATRIOT Act to compel disclosure of phone records of calls made to, from, and within the United States. This surveillance is not permitted by the statute, and was hidden from the public by deception. The legal basis for the program should be disclosed, and the program should be replaced by targeted phone call collection that focuses on suspected terrorists and spies.

For further information, please contact Gregory T. Nojeim, Director of the CDT Project on Freedom Security & Technology, 202/637-9800, gnojeim@cdt.org.