TESTIMONY OF STEVEN G. BRADBURY

Before the
HOUSE COMMITTEE ON THE JUDICIARY

Oversight Hearing into
The Administration's Use of FISA Authorities

July 17, 2013

Thank you, Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the Committee.

I appreciate the opportunity to appear before the Committee today to address the statutory authorities and constitutional principles governing the two National Security Agency programs that have been the subject of recent disclosures. These are:

> First, the acquisition of telephone call-detail records that involves only telephone metadata, not the content of any phone calls or the names or addresses of any phone subscribers; and
>
> Second, the surveillance, including the so-called "PRISM" Internet collection, that is targeted at the communications of foreign persons reasonably believed to be located outside the United States.

I believe it is most useful to discuss the legal basis for each of these two programs separately, since they are authorized under two different provisions of the Foreign Intelligence Surveillance Act, or FISA, though of course the programs can and should work together as part of the overall counterterrorism efforts of the United States.

Section 215 Order for Acquisition of Telephone Metadata

Let me focus first on the telephone metadata program. As the Government has stated, this program is supported by a business records order issued under the provision of FISA added by section 215 of the USA PATRIOT Act. *See* 50 U.S.C. § 1861. This section 215 order must be reviewed and reapproved by the federal

judges who sit on the FISA court every 90 days. I understand that 14 different federal judges have approved this order since 2006.

The metadata acquired consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. ***This order does not give the government access to any information about the content of calls or any other subscriber information, and it doesn't enable the government to listen to anyone's phone calls.***

Access to the data is limited under the terms of the court order. Contrary to some news reports, there's no data mining or random sifting of the data permitted. The database may only be accessed through queries of individual phone numbers and only when the government has reasonable suspicion that the number is associated with a foreign terrorist organization. If it appears to be a U.S. number, the suspicion cannot be based solely on activities protected by the First Amendment, such as statements of opinion, books or magazines read, Web sites visited, or places of worship frequented. Any query of the database requires approval from a small circle of designated NSA officers.

A query will simply return a list of any numbers the suspicious number has called and any numbers that have called it and when those calls occurred. Nothing more.

The database includes metadata going back five years, to enable an analysis of historical connections. Any records older than five years are continually purged from the system and deleted.

In analyzing links to suspicious numbers, any connections that are found to numbers inside the United States will of course be of most interest, because the analysis may suggest the presence of a terrorist cell in the U.S. Based in part on that information, the FBI may seek a separate FISA order for surveillance of a U.S. number, but that surveillance would have to be supported by individualized probable cause.

The NSA has confirmed that in all of 2012, there were fewer than 300 queries of the database, and only a tiny fraction of the data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

In addition to court approval, the 215 order is also subject to oversight by the executive branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When section 215 was reauthorized in 2011, I understand the leaders of Congress and members of these Committees were briefed on this program, and all members of Congress were offered the opportunity for a similar briefing.

Legal Basis and Constitutional Standards

Now let me address the statutory and constitutional standards applicable to the acquisition of this telephone metadata.

Section 215 permits the acquisition of business records that are "relevant to an authorized investigation." Here, the telephone metadata is "relevant" to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers described above, and this type of analysis is a critical building block in these investigations. In order to "connect the dots," we need the broadest set of telephone metadata we can assemble, and that's what this program enables.

The legal standard of relevance in section 215 is the same standard used in other contexts. It does not require a separate showing that every individual record in the database is "relevant" to the investigation; the standard is satisfied if the use of the database as a whole is relevant. As I've indicated, the acquisition of this data and the creation and use of this database are not only relevant to ongoing counterterrorism investigations; they're necessary to those investigations, because they offer the only means to conduct the critical analysis that provides links to new phone numbers used by agents of foreign terrorist organizations.

In terms of the background constitutional principles, it's important to remember that the Fourth Amendment itself would not require a search warrant or other individualized court order for such data acquisition. A government request for a company's business records is not a "search" within the meaning of the Fourth Amendment. Government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents that are "relevant" to an authorized inquiry. In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also don't require court approval. In the modern world of electronic storage and data compilation, reliance on the same "relevance" standard in these other contexts can also result in extremely expansive requests for business records.

In addition, the Fourth Amendment does not require a warrant when the government seeks purely transactional information, or metadata, as distinct from the content of communications. This information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore said there's no reasonable expectation that it's private. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008).

I would stress, however, that section 215 is more restrictive than the Constitution demands, because it requires the approval of a federal judge. In this way, Congress in the PATRIOT Act adopted a requirement for judicial review and approval of FISA business records orders that is more protective of privacy and civil liberties interests than the Constitution would otherwise demand. And while the 215 order for metadata is extraordinary in terms of the amount of data acquired, it's also extraordinarily narrow and focused in terms of the strict limitations placed on accessing the data at the back end.

Section 702 Order Targeting Foreign Communications

Let me now turn to the other NSA program at issue: The surveillance program targeting the Internet and other communications of foreign persons reasonably believed to be outside the United States. This program, which includes the so-called "PRISM" collection, is supported by a FISA court order issued under section 702 of FISA, the provision for "programmatic" foreign-targeting authority

that was added by the FISA Amendments Act of 2008. *See* 50 U.S.C. § 1881a. Similar authority was initially provided on a temporary basis in the Protect America Act of 2007.

The best way to understand this foreign-targeting program is to review the provisions of section 702, which lays out the governing framework approved by Congress.

Section 702 provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year at a time, targeted surveillance of the communications of non-U.S. persons who are reasonably believed to be located outside the United States to acquire foreign intelligence information, provided the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern use of the acquired information.

Under section 702, the surveillance may not (1) intentionally target any person, of any nationality, known to be located in the United States, (2) target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S., (3) intentionally target a U.S. person anywhere in the world, and (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 requires the Attorney General to adopt, and the FISA court to approve, targeting procedures reasonably designed to ensure compliance with these limitations, as well as detailed minimization procedures designed to ensure that any information about U.S. persons captured through this surveillance will not be retained or disseminated except as necessary for foreign intelligence reporting purposes.

Any foreign intelligence surveillance that is targeted at a particular U.S. person or any person believed to be in the United States requires a traditional individualized FISA order supported by probable cause.

Like the business records provision of FISA, section 702 goes beyond the baseline protections of the Fourth Amendment. Federal courts have consistently held that the Constitution permits the executive branch to conduct intelligence

surveillance within the United States without court involvement, provided the surveillance is focused on foreign threats. *See, e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980). By establishing a detailed procedure for court approval and congressional oversight, section 702 therefore provides a system of foreign intelligence surveillance that is more restrictive than the Constitution would otherwise require.

The PRISM Internet collection is precisely the type of court-approved foreign-targeted intelligence surveillance that Congress intended to authorize when it enacted and reauthorized section 702 by overwhelming majorities. This program is subject to extensive reviews and periodic reports to Congress by inspectors general, in addition to the oversight of the FISA judges. Moreover, I understand that in advance of the reauthorization of section 702 in 2012, the leaders and full membership of the Intelligence Committees of both Houses of Congress were briefed on the classified details of this program and all members of Congress were offered the opportunity for such a briefing.

* * *

For these reasons, I think these two programs are entirely lawful and are conducted in a manner that appropriately respects the privacy and civil liberties of Americans and the principles enshrined in the Constitution. Thank you, Mr. Chairman.