U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

JUL 16 2013

The Honorable F. James Sensenbrenner, Jr.
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Sensenbrenner:

This responds to your letter to the Attorney General date June 6, 2013, regarding the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act.

As you know, on June 5, 2013, the media reported the unauthorized disclosure of a classified judicial order issued under this provision that has been used to support a sensitive intelligence collection program. Under this program, which has been briefed to Congress and repeatedly authorized by the Foreign Intelligence Surveillance Court (FISC), the Federal Bureau of Investigation (FBI) obtains authorization to collect telephony metadata, including the telephone numbers dialed and the date, time and duration of calls, from certain telecommunications service providers. The National Security Agency (NSA), in turn, archives and analyzes this information under carefully controlled circumstances and provides leads to the FBI or others in the Intelligence Community for counterterrorism purposes. Aspects of this program remain classified, and there are limits to what can be said about it in an unclassified letter. Department of Justice and Intelligence Community staff are available to provide you a briefing on the program at your request.

In your letter, you asked whether this intelligence collection program is consistent with the requirements of section 215 and the limits of that authority. Under section 215, the Director of the FBI may apply to the FISC for an order directing the production of any tangible things, including business records, for investigations to protect against international terrorism. To issue such an order, the FISC must determine that (1) there are reasonable grounds to believe that the things sought are relevant to an authorized investigation, other than a threat assessment; (2) the investigation is being conducted under guidelines approved by the Attorney General under Executive Order 12333; and (3) if a U.S. person is the subject of the investigation, the investigation is not being conducted solely upon the basis of First Amendment protected activities. In addition, the FISC may only require the production of items that can be obtained with a grand jury subpoena or any other court order directing the production of records or tangible things. Finally, the program must, of course, comport with the Constitution.

The telephony metadata program satisfies each of these requirements. The lawfulness of the telephony metadata collection program has repeatedly been affirmed by the FISC. In the years since its inception, multiple FISC judges have granted 90-day extensions of the program after concluding that it meets all applicable legal requirements.

Of particular significance to your question is the relevance to an authorized international terrorism investigation of the telephony metadata collected through this program. First, it is critical to understand the program in the context of the restrictions imposed by the court. Those restrictions strictly limit the extent to which the data is reviewed by the government. In particular, the FISC allows the data to be queried for intelligence purposes only when there is reasonable suspicion, based on specific facts, that a particular query term, such as a telephone number, is associated with a specific foreign terrorist organization that was previously identified to and approved by the court. NSA has reported that in 2012, fewer than 300 unique identifiers were used to query the data after meeting this standard. This means that only a very small fraction of the records is ever reviewed by any person, and only specially cleared counterterrorism personnel specifically trained in the court-approved procedures can access the records to conduct queries. The information generated in response to these limited queries is not only relevant to authorized investigations of international terrorism, but may be especially significant in helping the government identify and disrupt terrorist plots.

The large volume of telephony metadata is relevant to FBI investigations into specific foreign terrorist organizations because the intelligence tools that NSA uses to identify the existence of potential terrorist communications within the data require collecting and storing large volumes of the metadata to enable later analysis. If not collected and held by NSA, the metadata may not continue to be available for the period that NSA has deemed necessary for national security purposes because it need not be retained by telecommunications service providers. Moreover, unless the data is aggregated by NSA, it may not be possible to identify telephony metadata records that cross different telecommunications networks. The bulk collection of telephony metadata—i.e. the collection of a large volume and high percentage of information about unrelated communications—is therefore necessary to identify the much smaller subset of terrorist-related telephony metadata records contained within the data. It also allows NSA to make connections related to terrorist activities over time and can assist counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. Because the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications, there are "reasonable grounds to believe" that the data is relevant to an authorized investigation to protect against international terrorism, as section 215 requires, even though most of the records in the dataset are not associated with terrorist activity.

The program is consistent with the Constitution as well as with the statute. As noted above, the only type of information acquired under the program is telephony metadata, not the content of any communications, not the identity, address or financial information of any party to

the communication, and not geolocational information. Under longstanding Supreme Court precedent, there is no reasonable expectation of privacy with respect to this kind of information that individuals have already provided to third-party businesses, and such information therefore is not protected by the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 739-42 (1979).

Moreover, it is important to bear in mind that activities carried out pursuant to FISA, including those conducted under this program, are subject to stringent limitations and robust oversight by all three branches of government. As noted above, by order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata it acquires. Instead, all information that is acquired is subject to strict, court-imposed restrictions on review and handling that provide significant and reasonable safeguards for U.S. persons. The basis for a query must be documented in writing in advance and must be approved by one of a limited number of highly trained analysts. The FISC reviews the program approximately every 90 days.

The Department of Justice conducts rigorous oversight to ensure the telephony metadata is being handled in strict compliance with the FISC's orders, and the Department of Justice and the Office of the Director of National Intelligence (ODNI) conduct thorough and regular reviews to ensure the program is implemented in compliance with the law.

The program is also subject to extensive congressional oversight. The classified details of the program have been briefed to the Judiciary and Intelligence Committees on many occasions. In addition, in December 2009, the Department of Justice worked with the Intelligence Community to provide a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress regarding the telephony metadata collection program. It is our understanding that both Intelligence Committees made this document available to all Members prior to the February 2010 reauthorization of section 215. That briefing paper clearly explained that the government and the FISC had interpreted Section 215 to authorize the collection of telephony metadata in bulk. An updated version of the briefing paper was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year.

Finally, we do not agree with the suggestion in your letter that the Department's March 9, 2011 public testimony on section 215 conveyed a misleading impression as to how this authority is used. Quoting a portion of that testimony, your letter states that it "left the committee with the impression that the Administration was using the business records provision sparingly and for specific materials. The recently released FISA order, however, could not have been drafted more broadly." In fact, key language in the testimony in question noted that orders issued pursuant to section 215 "have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately

briefed." We hope that the explanation above regarding the use of this authority to identify specific terrorism-related telephony metadata records helps to clarify the point.

The recent unauthorized disclosure of this and other classified intelligence activities has caused serious harm to our national security. Since the disclosure of the telephony metadata collection program, the Department of Justice and the Intelligence Community have worked to ensure that Congress and the American people understand how the program operates, its importance to our security, and the rigorous oversight that is applied. As part of this effort, senior officials from ODNI, NSA, DOJ and FBI provided a classified briefing for all House Members on June 11, 2013 and separate classified briefings to the House Democratic Caucus and the House Republican Conference on June 26, 2013.

The Department of Justice is committed to ensuring that our efforts to protect national security are conducted lawfully and respect the privacy and civil liberties of all Americans. We look forward to continuing to work with you and others in the Congress to ensure that we meet this objective.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance with this or any other matter.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General