U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 15, 2014

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of Deputy Attorney General James M. Cole before the Committee on July 31, 2013, at a hearing entitled "Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs."

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Peter J. Kadzik
Acting Assistant Attorney General

Enclosures

cc: The Honorable Charles E. Grassley
Ranking Minority Member

Hearing Before the
Committee on the Judiciary
United States Senate

Entitled
"Strengthening Privacy Rights and National Security:
Oversight of FISA Surveillance Programs"
July 31, 2013

Questions for the Record Addressed to
James M. Cole
Deputy Attorney General
Department of Justice

Questions Posed by Chairman Leahy

1. Please provide a summary of the legal arguments that the United States government has submitted to the Foreign Intelligence Surveillance Court in support of conducting bulk collection of telephone and Internet metadata under Section 215 of the USA PATRIOT Act and Section 402 of the Foreign Intelligence Surveillance Act.

Answer:

The Government has published a white paper summarizing its views on the legal basis for the collection of bulk telephony metadata under Section 215. *See Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act*, available at http://publicintelligence.net/doj-bulk-telephony-collection/. The Government's classified brief on this subject, which was submitted to the Foreign Intelligence Surveillance Court (FISC) in 2006, was provided to this committee in 2010, and was declassified and made publicly available by the Director of National Intelligence on November 18, 2013.

Section 402 of FISA, which governs installation and use of pen registers and trap and trace devices for foreign intelligence and international terrorism investigations, has different requirements and standards than Section 215 of the USA PATRIOT Act. The Government's classified brief on collection of bulk Internet metadata under Section 402 has also been provided to this committee.

2. Marc Zwillinger represented Yahoo! in its challenge to the Protect America Act, and he submitted written testimony for the record of the hearing. In his testimony, he expressed the view that the Yahoo! challenge was not a fully adversarial process because the government submitted *ex parte* filings even though only cleared counsel were involved in the proceeding.

Q: Please describe what government *ex parte* submissions were made in that case, why those filings were not disclosed to opposing counsel, and whether you believe opposing counsel would have been better able to litigate the challenge with access to those submissions.

Answer:

On August 5, 2007, Congress enacted the Protect America Act (PAA), the predecessor to Section 702 of FISA. In general, the PAA authorized the Attorney General and the Director of National Intelligence to authorize, for periods of up to one year, the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States and to compel, through the issuance of directives, the assistance of communications services providers in accomplishing such acquisitions. A directive was issued to Yahoo! requiring Yahoo! to provide such assistance. Yahoo! refused to comply with the directive. The Government then moved the FISC to compel Yahoo!'s compliance with the properly issued directive. Classified adversarial litigation ensued in both the FISC and the Foreign Intelligence Surveillance Court of Review (FISC-R) over several months, culminating in a classified oral argument before the FISC-R. Both the FISC and the FISC-R ruled that Yahoo! was required to comply with the directive, and Yahoo! ultimately complied in the wake of these rulings.

The Yahoo! challenge to the PAA was, in the Government's view, a full and fair adversarial proceeding that resulted in thoughtful and comprehensive presentations of the legal issues involved to the FISC and, on appeal, to the FISC-R. Although counsel for Yahoo! had been granted security clearances by the Government and was provided access to some classified information in government submissions based on his need to know that information, those clearances did not entitle counsel access to certain sensitive compartmented information related to sources and methods. Although in certain limited circumstances the Government, compelled by requirements pertaining to the protection of classified national security information, submitted certain pleadings/information *ex parte* and in camera to the FISC and the FISC-R, the more typical practice was for the Government to serve counsel for Yahoo! with appropriately redacted versions of briefs and other filings. The Government redacted information in a manner consistent with governing law and Executive Orders on the protection of classified information in order to protect sensitive sources and methods and other classified matters that counsel for Yahoo! had no need to know. Moreover, the information withheld was not material to their ability to mount a vigorous legal challenge to the PAA. For example, Yahoo!'s counsel did not need to know certain details about internal government processes and procedures that were used by the Government in implementing PAA authorities, and their litigation of these matters was in no way prejudiced by the redaction of that information. Briefing on the core legal issues was presented unredacted to Yahoo!'s counsel. Both the FISC and FISC-R had full visibility into the redactions. The lengthy and well-reasoned opinions of the FISC and the FISC-R on Yahoo!'s challenge to the PAA (including the FISC-R's published opinion) are evidence of the sufficiency of the legal process afforded to Yahoo! in that matter.

3. I appreciate Judge Walton's letter explaining the FISA Court procedures when considering applications by the Government for orders under FISA. While it is important for the public to understand the FISA Court process, it is even more important that we have an open debate

about the legal rationale used to justify such broad authorities as the bulk collection of telephone metadata – particularly if these opinions stretch the understanding of existing law.

Q: Would declassifying and releasing the portions of FISA Court opinions that include significant interpretations of existing law, with appropriate redactions to protect intelligence sources or methods, be harmful to our national security?

Answer:

The Administration has committed to reviewing significant FISC opinions for declassification, recognizing that, as Judge Walton has explained, the facts presented in applications to the FISC almost always involve classified intelligence activities, the disclosure of which could be harmful to national security and, in most cases, the facts and legal analysis are so inextricably intertwined that excising the classified information from the FISC's analysis would result in a remnant void of much or any useful meaning. In connection with the recent unauthorized disclosures of information concerning intelligence activities carried out under sections 501 and 702 of FISA, the President has directed that as much information as possible be made public about these activities, consistent with the need to protect sources and methods and national security, including relevant FISC opinions related to these activities. In recent months, the Government has declassified several FISC opinions concerning these activities, with appropriate redactions for national security purposes.

Q: Now that certain information has been declassified about Section 215 bulk collection, is there any objection to releasing any FISA Court opinions that support and explain the legal basis for these programs?

Answer:

See response above.

4. Please provide a full description of the ways in which information obtained by the NSA is shared with law enforcement components of the Department of Justice, including but not limited to, the Drug Enforcement Administration, and how, if at all, that information is used in criminal investigations and proceedings.

Answer:

For information collected under FISA, NSA shares information in accordance with the applicable provisions of that statute. The USA PATRIOT Act amended FISA to facilitate information sharing, and to ensure an end to the FISA "wall" inhibiting information sharing between intelligence and law enforcement components of the Government. Thus FISA provides that federal officials conducting electronic surveillance under FISA "may consult" with law enforcement officials "to coordinate efforts to investigate or protect against" international terrorism, espionage, and other threats. 50 U.S.C. § 1806(k). FISA also requires that dissemination of information about U.S. persons comply with minimization procedures, and

FISA contemplates that these procedures will permit the dissemination of foreign intelligence information and evidence of a crime, including to law enforcement authorities. *See, e.g.*, 50 U.S.C. § 1801(h)(3) (defining minimization procedures for electronic surveillance in part as "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes"). The Attorney General and the FISA Court (or, in certain circumstances, like emergency authorization, the Attorney General alone) must approve the minimization procedures. FISA also has provisions governing the use of most kinds of information obtained under FISA authorities in criminal and other proceedings. *See, e.g.*, 50 U.S.C. §§ 1806(c)-(h) (governing the use of information obtained from electronic surveillance in proceedings).

For information collected under Executive Order 12333, NSA shares information about U.S. persons in accordance with procedures established by the Secretary of Defense and approved by the Attorney General. Those procedures generally permit the dissemination of information to "[a]n agency of the federal government authorized to receive such information in the performance of a lawful governmental function" and to a federal, state, or local law enforcement agency if "the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce." *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons (DOD Reg. 5240.1-R), Procedure 4—Dissemination of Information About United States Persons* § C4.2.2 (Dec. 1982). *See also Classified Annex to Department of Defense Procedures Under Executive Order 12333* § 4.A.4 (May 27, 1988).

Information received from NSA is used in a variety of ways, depending on the nature of the information. It may be used to generate leads to further an investigation, in discovery as part of a criminal proceeding, or as evidence at trial.