Senator Sheldon Whitehouse
Written Questions for the Record
Hearing on "Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy, and Civil Liberties"

Questions for Elizabeth Goitein and the Honorable David Medine

1. In your testimony, you expressed concern about so-called "back door searches" by law enforcement of data collected pursuant to Section 702. Do you believe there should be restrictions on the FBI's ability to search Section 702 data for evidence in terrorism and national security investigations? And if, hypothetically, Section 702 were limited to terrorism and national security investigations, what should those restrictions be?

As I noted in my testimony, Section 702 allows the government to target any foreigner overseas regardless of whether that person is believed to pose any threat to the United States. If, however, Section 702 were limited – per your hypothetical – to terrorism and national security investigations, and the pool of permissible foreign targets were limited accordingly, then I do not believe any substantive restrictions on the FBI searching Section 702 data using identifiers associated with the non-U.S. person targets would be required, as long as the individual was not targeted or searched for improper purposes (e.g., discrimination or political persecution).

Under the same hypothetical, the appropriate restrictions on conducting searches using U.S. person identifiers would depend on the nature of the investigation. When the government wishes to search a U.S. person's communications in a foreign intelligence investigation (which includes international terrorism investigations), Congress has indicated the appropriate standard and procedure under Title I of FISA: The government must demonstrate probable cause to the Foreign Intelligence Surveillance Court that the target is a foreign power or agent of a foreign power (which includes those acting for or on behalf of international terrorist organizations) and obtain an individual court order.[1]

When the government wishes to search an American's *wire* communications in a domestic national security investigation not involving foreign intelligence (including domestic terrorism investigations), the Supreme Court has held that it must first obtain a warrant,[2] and Congress has indicated the appropriate standard and procedure under Title III of the Omnibus Crime Control and Safe Streets Act of 1968: The government must demonstrate probable cause to a federal judge that the subject of the search is committing, has committed, or is about to commit a crime specified in the law (which includes crimes of domestic terrorism); that particular communications concerning the offense will be obtained through the search; and that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[3]

---

[1] 50 U.S.C. § 1805(a)(2).
[2] United States v. U.S. Dist. Court for the E. Dist. Of Mich. (*Keith*), 407 U.S. 297 (1972).
[3] 18 U.S.C. § 2518(3).

When the government wishes to search an American's *stored* communications in a domestic national security investigation, the standards are less well-settled. The Stored Communications Act permits requires the government to obtain a warrant based on probable cause when obtaining unopened e-mails stored for 180 days or less, but allows the government to obtain already-opened or older e-mails using merely a subpoena.[4] However, the U.S. Court of Appeals for the Sixth Circuit held in *United States v. Warshak* that the Fourth Amendment requires a warrant for all e-mail content,[5] and the U.S. House of Representatives recently voted 419-0 to codify this requirement.[6] I believe the Sixth Circuit's analysis was correct, and I would support a warrant requirement for government access to e-mail content.

The fact that the government already has obtained the communications under Section 702 should not change these standards, because the constitutional and statutory prerequisite for obtaining the communications without a probable cause order was the government's representation that foreigners and only foreigners would be targeted. Once the target becomes an American, the justification for a warrantless search evaporates, and a search may not take place without judicial approval.

Nonetheless, some have suggested that if the initial collection of the data is lawful, then the data may be searched or used for any purpose. This is wrong both as a statutory matter and a constitutional one. Section 702 requires the government to *minimize* the sharing and retention of incidentally-acquired U.S. person data; this requirement makes clear that the data may not be searched or used at will. Moreover, Judge Bates of the FISA Court, when reviewing the government's handling of purely domestic communications obtained through "upstream" collection, stated unequivocally that "the procedures governing retention, use, and dissemination [of U.S. person information] bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[7]

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant. The fact that the government lawfully obtained and is in possession of the computer's contents does not give it license to conduct any search it wishes; that would violate the terms on which the government obtained the computer's contents in the first place.

The same principle holds true in the analog world. When the police obtain a warrant to search a house for a murder weapon, they may enter the house and, in appropriate cases, search every room. But after they find (or fail to find) the murder weapon, they are not allowed to continue searching for other items they may have some interest in, simply because they are now in the house. Their entrance into the house was legal, but that does not entitle them to search for anything inside it. That would be exceeding the terms accompanying their initial access to the house.

---

[4] 18 U.S.C. § 2703.
[5] 631 F.3d 266 (6th Cir. 2010).
[6] *See* Dustin Volz, *Email Privacy Bill Unanimously Passes U.S. House*, REUTERS (Apr. 27, 2016), http://www.reuters.com/article/us-usa-congress-email-idUSKCN0XO1J7.
[7] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011).

Under Section 702, the terms on which the government is authorized to collect data *without* a warrant include a limitation on whom the government may target – i.e., the government may only target foreigners overseas. To obtain access to the data on those terms and then search for Americans' data is the equivalent of seizing a computer to search for child pornography and then searching for evidence of tax fraud, or obtaining access to a house to search for a murder weapon and then conducting a search for drugs.

If, in the course of searching a house for a murder weapon, the police happen upon drugs, they are entitled to seize them under the "plain view" doctrine. A similar argument could be made that the government should be entitled to use U.S. person information that constitutes foreign intelligence or evidence of a crime that agents happen across while searching foreigners' communications (although the breadth of Section 702 collection weakens the analogy here; the argument would be much stronger if Section 702 were in fact limited to terrorism and national security investigations). But that is very different from claiming the entitlement to search the data for particular Americans' communications.