Summary of National Security Agency Domestic Spying Revelations, Summer 2013

- **Section 215 of the Patriot Act is used to collect all U.S. phone call records, even purely domestic ones, without a warrant or any evidence of terrorist connections**. On June 6, 2013, *The Guardian* disclosed a secret Foreign Intelligence Surveillance Act (FISA) court order issued to Verizon. It directed the company to turn over "records" or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls" directly to the National Security Agency (NSA) on an ongoing daily basis for 90 days.[1] Senate Select Committee on Intelligence Chairman Diane Feinstein (D-Cal.) stated that this program includes other phone companies and has been in effect for seven years.[2] While the administration asserts that the information was "queried" 300 times last year, it is not clear what that means and how many phone numbers or U.S. persons were affected in those queries. It's also impossible to know if the information is being used in other ways that haven't been publicly disclosed.

  FISA has long allowed the government to obtain court orders for certain records that pertain to agents of foreign powers –such as international terrorists or spies. But Section 215 of the Patriot Act expanded that more tailored authority so that it could obtain "any tangible thing" deemed relevant to an investigation. No allegation that the information relates to terrorists or their contacts is necessary. FISA and Patriot Act Section 215 were once again expanded in 2006 to reduce judicial discretion and presumptively declared several categories of information as relevant.

- **The FISA Amendments Act (FAA) of 2008 is used to collect the internet records and the content of online communications of Americans**. Several documents published in June 2013 demonstrate that the FAA is being broadly used to collect wide swaths of internet data, including the content of communications under annual orders to collect foreign intelligence.[3]

[1] Secondary Order, In Re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services Inc. on Behalf of MCI Communication Serv., Inc. D/B/A Verizon Business Serv., Docket No. BR (Foreign Intelligence Surveillance Ct. Apr. 25, 2013), *available at* http://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.

[2] Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss explain, defend NSA phone records program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/.

[3] Exhibit A, Procedures Used by the Nat'l Sec. Agency for Targeting Non-U.S. Persons Reasonably Believed to Be Located Outside the U.S. to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, *available at*

While the "target" must reasonably be believed to be overseas, "target" is a term of art describing the subject about which information will be obtained, not necessarily a specific known individual terrorist. So while the target could be al Qaeda-associated organizations overseas, the program is permitted to collect communications where one or both parties are in the U.S. While the administration calls this American surveillance "incidental," reports say that even one data stream can provide records in the trillions.[4]

These broad authorities were supposed to be kept in check by secret targeting procedures to prevent the intentional collection of US information and secret "minimization" procedures that limit the collection, retention, and use of U.S. information. But those documents were leaked also,[5] and they confirm that if there is any doubt about the location of a person, he or she is assumed to be outside of the United States and his or her information can be collected. The NSA "maintains records of telephone numbers and electronic communications accounts/ addresses/ identifiers that NSA has reason to believe are being used by United States persons."[6] Once in the government's possession, records and communications can be kept (even entirely domestic communication) until an analyst determines they are "clearly not relevant to the authorized purpose of the acquisition" and can even be used in criminal investigations.[7] Any encrypted record may also be retained.

- **The FISA Court has created a secret body of law interpreting the surveillance laws and the constitution itself**. The programs have been authorized by the FISA court. The court was created in 1978 to hear wiretap applications based on probable cause for specific terrorists or spies. After 9/11, the court has gone far beyond its original mandate by approving invasive surveillance programs that collect information on people not suspected of wrongdoing. *The New York Times* reports that there are over a dozen major opinions, some reaching 100 pages long.[8] The Senate Intelligence Committee confirmed that these opinions discuss the privacy protections required – or not – to keep the programs constitutional. While the court has released three opinions in its 35 year history, none of those discussing the broad new interpretation of the Patriot Act or the FISA Amendments Act of 2008 have even been described to Congress or the public.

---

http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document [hereinafter *Exhibit A*]; *and* Exhibit B, Minimization Procedures Used by the Nat'l Sec. Agency in connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended *available at* http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document [hereinafter *Exhibit B*]. *See also* Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST, June 6, 2013, http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers.

[4] Glenn Greenwald & Spencer Ackerman, *How the NSA is still harvesting your online data*, THE GUARDIAN, June 27, 2013, http://www.guardian.co.uk/world/2013/jun/27/nsa-online-metadata-collection.

[5] Exhibit A *and* Exhibit B, *supra* note 3.

[6] Exhibit A, *supra* note 3.

[7] Exhibit B, *supra* note 3.

[8] Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times, July 7, 2013, at A1, *available at* http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all.

- **For a decade, the government conducted bulk collection of email records, including those sent to or from a person in the United States.** *The Guardian* published an internal DOJ memo and a draft Inspector General report confirming that the government also collected vast amounts of email data, such as the to/from information and the IP addresses associated with email from 2001 to 2011. The government only stopped after Senators Ron Wyden (D-Ore.) and Mark Udall (D-Colo.) pressed the administration for tangible examples of how the broad authority was successfully being used.[9] The FISA pen register /trap and trace statute was amended by sections 214 and 216 of the Patriot Act to clarify that it could obtain email and internet records, and that it no longer needed to be limited to collection on suspected spies and terrorists. While the program was voluntarily halted, the legal authority for it remains on the books, and it is not clear if it currently exists under other authorities or in a more limited fashion.

[9] Glenn Greenwald & Spencer Ackerman, *NSA collected US email records in bulk for more than two years under Obama*, THE GUARDIAN, June 27, 2013, http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama.