Related article:

Farivar, C. (Aug. 27, 2014). The executive order that led to mass spying as told by NSA alumni. *ArsTechnica*.

LAW & DISORDER / CIVILIZATION & DISCONTENTS

It’s official—NSA *did* keep its e-mail metadata program after it “ended” in 2011

The New York Times gets a new NSA doc confirming what some had long suspected.

by **Cyrus Farivar** - Nov 20, 2015 6:30pm EST

Trevor Pagjen

Though it was revealed by Edward Snowden in June 2013, the National Security Agency's (NSA) infamous secret program to domestically collect Americans’ e-mail metadata in bulk technically ended in December 2011. Or so we thought. A new document obtained through a lawsuit filed by *The New York Times* confirms

that this program effectively continued under the authority of different government programs with less scrutiny from the Foreign Intelligence Surveillance Court (FISC).

The bulk electronic communications metadata program was initially authorized by the government under the Pen Register and Trap and Trace (PRTT) provision, also known as Section 402 of the Foreign Intelligence Surveillance Act. The *Times*’ document, a previously-top secret National Security Agency Inspector General (NSA IG) report from January 2007, contains a lot of intelligence jargon but crucially notes: "Other authorities can satisfy certain foreign intelligence requirements that the PRTT program was designed to meet."

The bulk electronic communications metadata program was initially authorized by the government under the Pen Register and Trap and Trace (PRTT) provision, also known as Section 402 of the Foreign Intelligence Surveillance Act. The *Times*’ document, a previously-top secret National Security Agency Inspector General (NSA IG) report from January 2007, contains a lot of intelligence jargon but crucially notes: "Other authorities can satisfy certain foreign intelligence requirements that the PRTT program was designed to meet."

While such a theory had been pushed previously by some national security watchers, including Marcy Wheeler, this admission had yet to be officially confirmed. Wheeler argued that not only do the post-PRTT programs achieve the same goal, but she believed they were in fact more expansive than what was previously allowed.

The bulk metadata program, which began in secret under authorization from the FISC in 2004, allowed the NSA to collect all domestic e-mail metadata including to, from, date, and time. When this program was revealed by the Snowden leaks in *The Guardian*, the government said that the PRTT program had been shut down 18 months earlier for "operational and resource reasons."

It was believed that the FISC imposed a number of restrictions on the PRTT program, according to the Office of the Director of National Intelligence (ODNI) itself.

> The databases could be queried using an identifier such as an email address only when an analyst had a reasonable and articulable suspicion that the email address was associated with certain specified foreign terrorist organizations that were the subject of FBI counterterrorism investigations. The basis for that suspicion had to be documented in writing and approved by a limited number of designated approving officials identified in the Court’s Order. Moreover, if an identifier was reasonably believed to be used by a United States person, NSA’s Office of General Counsel would also review the determination to ensure that the suspected association was not based solely on First Amendment-protected activities.

The PRTT program was designed to help the intelligence community intercept and analyze "one-end foreign" communication—in other words, people in the US communicating with people outside the US.

EO 12333 strikes again

The newly public document cites two legal authorities that govern foreign data collection: Section 702 of the FISA Amendments Act and the Special Procedures Governing Communications Metadata Analysis (SPCMA), which sits under Executive Order (EO) 12333.

Section 702 largely governs content collection wholly outside the United States (it’s what PRISM falls under). Meanwhile, EO 12333, which ex-government officials (including Snowden himself) have complained about, is a broad Reagan-era authority that allows data collection on Americans even when Americans aren't specifically targeted. Without this executive order, such actions would be forbidden under the Foreign Intelligence Surveillance Act (FISA) of 1978.

FURTHER READING

THE EXECUTIVE ORDER THAT LED TO MASS SPYING, AS TOLD BY NSA ALUMNI

Feds call it “twelve triple three”; whistleblower says it's the heart of the problem.

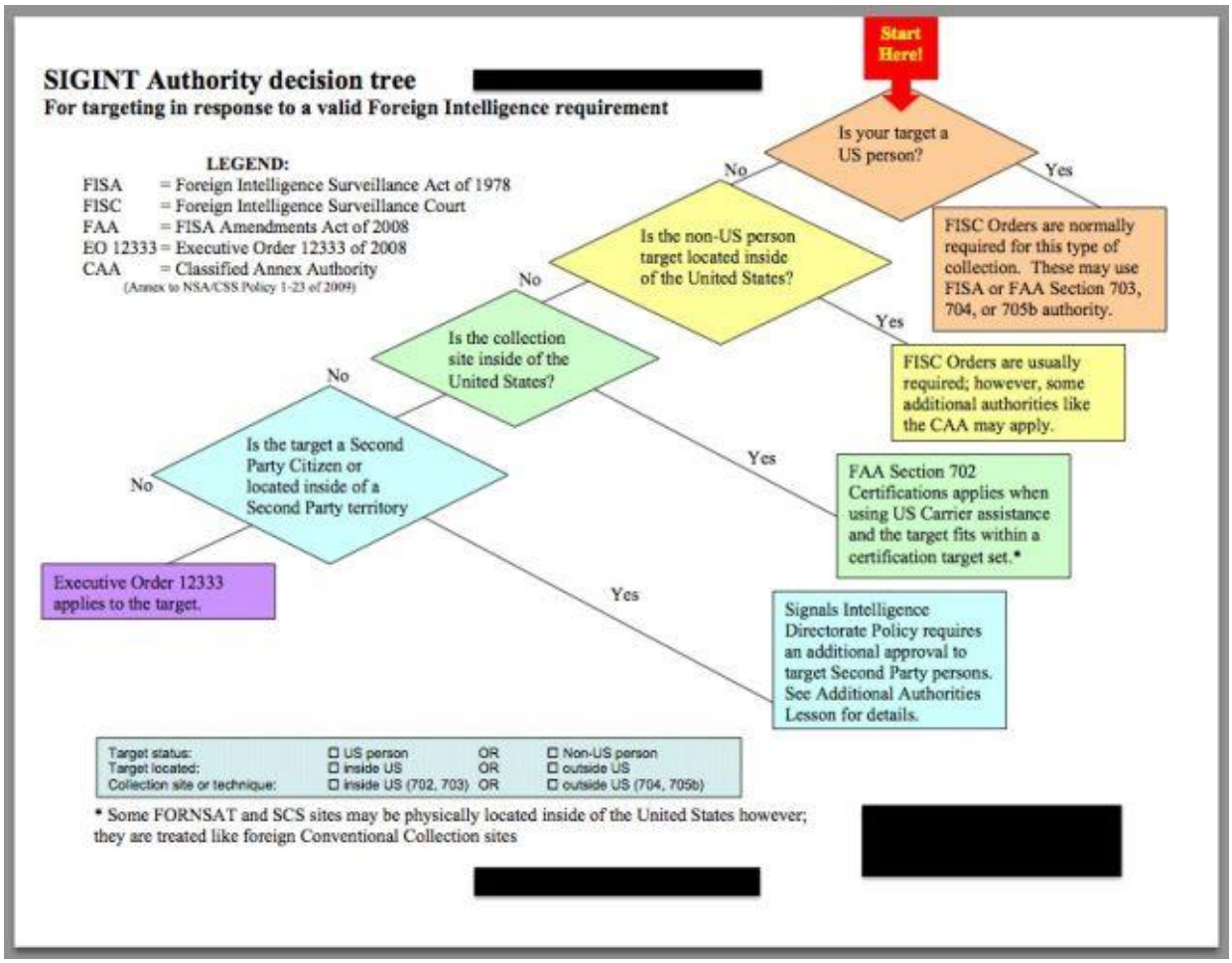

Figure 1: EdwardSnowden.com

EO 12333 specifically allows the intelligence community to "collect, retain, or disseminate information concerning United States persons" if that information is "obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation.'"

According to John Tye, a former State Department official who spoke with Ars in August 2014, EO 12333 has the potential to be abused as it could "incidentally" collect foreign-held data on Americans. "12333 is used to target foreigners abroad, and collection happens outside the US," he told Ars. "My complaint is not that they’re using it to target Americans, my complaint is that the volume of incidental collection on US persons is unconstitutional."

Tye continued:

> There are networks of servers all over the world and there have been news stories on Google and Yahoo—the minute the data leaves US soil it can be collected under 12333. That’s true not just for Google and Yahoo, that’s true for Facebook, Apple iMessages, Skype, Dropbox, and Snapchat. Most likely that data is stored at some point outside US or transits outside the US. Pretty much every significant service that Americans use, at some point it transits outside the US.
>
> Hypothetically, under 12333 the NSA could target a single foreigner abroad. And hypothetically if, while targeting that single person, they happened to collect every single Gmail and every single Facebook message on the company servers not just from the one person who is the target, but from everyone—then the NSA could keep and use the data from those three billion other people. That’s called 'incidental collection.' I will not confirm or deny that that is happening, but there is nothing in 12333 to prevent that from happening.

UPDATE Saturday 12:55pm ET: Tye also e-mailed Friday evening, adding:

> Yes, this is consistent with what I've been saying. One of the key points is that section 215 provides only a small part of the data that the NSA collects on US persons; most such data is collected outside the borders of the US under EO 12333.
>
> There is a lot more than even the Savage article explains. We're beginning to scratch the surface.