BRENNAN CENTER
FOR JUSTICE at New York University School of Law

# Are They Allowed to Do That?
# A Breakdown of Selected Government Surveillance Programs

Here are answers to some widely-asked questions about the FBI's and National Security Agency's surveillance programs revealed last week.

**Q: What is the National Security Agency doing?**

**A:** Two major surveillance programs have been revealed:

1. Since 2006, the National Security Agency (NSA) has been secretly collecting the phone records of millions of Americans from some of the largest telecommunications providers in the United States, via a series of regularly renewed requests by the Federal Bureau of Investigation (FBI). Although the NSA is not collecting the contents of all phone calls, it is collecting records of who called whom, when and for how long. There are also reports that the NSA has been collecting similar information about e-mails, internet searches, and credit card transactions. The government has acknowledged some aspects of this collection program, but claims that officials do not actually look at the collected data in more detail without reasonable suspicion that some element of it concerns a foreign terrorist organization.

2. Over the past six years, the NSA has obtained unprecedented access to the data processed by nine leading U.S. internet companies. This was facilitated by a computer network named PRISM. The companies involved include Google, Facebook, Skype, and Apple. Limitations on the NSA's access are the source of current debate. Initial reports, which have since been qualified, said that the NSA can "pull anything it likes" from the companies' servers. Government officials and corporate executives have responded that the NSA only obtains data with court approval and with the knowledge of the companies. Some companies have also denied knowledge of PRISM.

**Q: What are the legal justifications for the programs?**

**A:** The government claims that the telephone records program that was the subject of the leaked Verizon court order is authorized under the so-called "business records" provision of the Foreign Intelligence Surveillance Act (FISA), first enacted in 1978. That provision was amended by Section 215* of the Patriot Act in 2001. Section 215 allows the government to obtain a secret court order requiring third parties, such as telephone companies, to hand over any records or other "tangible thing" if deemed "relevant" to an international terrorism,

* The provisions of FISA have been codified under the United States Code, and are commonly cited as provisions of the U.S. Code (e.g. 50 U.S.C. § 1801). Section 215 of the Patriot Act amended 50 U.S.C. § 1861, and Section 702 of the FISA Amendments Act amended 50 U.S.C. § 1881a. Section 216 of the Patriot Act amended 18 U.S.C. § 3121, a provision of the Pen Register Act.

counterespionage, or foreign intelligence investigation. Section 215 orders may have been combined with requests under other provisions of the Patriot Act, such as Section 216, which governs access to online activity, such as email contact information or Internet browsing histories.

With respect to PRISM, the government cites Section 702 of the FISA Amendments Act, a law first passed in 2008 and reauthorized in 2012. Section 702 allows the government to acquire foreign intelligence by targeting non-U.S. persons "reasonably believed" to be outside U.S. borders. The law explicitly prohibits intentionally targeting people known to be located inside the U.S. at the time the government acquires the data. It also requires the government to establish certain "targeting procedures" to ensure that the government is targeting people "reasonably believed" to be outside the United States (which can be difficult to ascertain when dealing with internet or cell phone communications). In addition, the government must adopt "minimization procedures" to guard against the inadvertent collection, retention, and dissemination of information about U.S. persons.

**Q: Is there any oversight?**

**A:** To collect the kind of phone records it did from Verizon, the government must obtain a Section 215 order from the Foreign Intelligence Surveillance Court (FISA court) — a federal court established under FISA which oversees government applications to conduct surveillance for the purposes of obtaining foreign intelligence. The request for the order, and the court's ruling, are classified. The number of Section 215 orders has soared in recent years, from just 21 applications in 2009 to 212 applications in 2012. None of the applications in 2012 were denied by the FISA court. Classified reports about these applications are submitted to Congress's intelligence and judiciary committees. Unclassified aggregate numbers, such as the above, are sent to Congress annually.

When it comes to Section 702, the law cited for PRISM, the FISA court's role is more limited. Even though Section 702 does not allow the intentional surveillance of U.S. persons, the government is *not* required to go before the court to obtain individual surveillance orders. Instead, the court approves the "targeting" and "minimization" procedures described above to limit the amount of information about law-abiding Americans that is intercepted, retained, and disseminated. In deciding whether to approve the procedures, the court reviews whether they are consistent with the Fourth Amendment to the Constitution. But it has no ongoing authority to determine if the government is complying with these procedures, and both the procedures and the court orders relating to them are classified. Some information about Section 702 programs must be reported to Congress's intelligence and judiciary committees, including significant legal opinions of the FISA court. However, these reports are generally classified and not shared.

**Q: Do communications providers have a say?**

**A:** Theoretically, yes. If served with an order under Section 215 or Section 702 demanding records, a communications provider can challenge it. Yet like all proceedings before the

FISA court, such a challenge would be secret (as is compliance with the court's orders). In addition, companies are prohibited from disclosing information about the government's requests to the public through so-called "gag orders." Companies may challenge these gag orders in court, but the secrecy of the court's proceedings makes it impossible to know whether any company has mounted such a challenge.

**Q: What about individuals?**

**A:** Persons whose records are targeted do not have the right to appear before the FISA court. Moreover, since the surveillance programs are classified, targeted persons generally have no way of knowing that their records are the subject of specific government scrutiny. Although individuals or organizations can submit requests under the Freedom of Information Act or the Privacy Act asking for information about whether the government has been spying on them or others, these requests are likely to be denied.

**Q: If these laws were passed by Congress, and the FBI and NSA are securing the required court approval and making the required disclosures to Congress, what's the problem? Isn't everything working the way it's supposed to?**

**A:** It is debatable whether Congress intended the sort of dragnet information collection of phone records that the FISA court has approved under Section 215. Section 215 is dangerously broad, but its plain language does not permit wide-scale surveillance on an ongoing basis. Under the provision, the government is allowed to collect only records that are "relevant" to an authorized investigation. It is difficult to believe that the phone records of millions of Americans are actually "relevant" to a specific terrorist or foreign intelligence investigation. Nor does Section 215 appear to allow the government to collect first and determine relevance later, which is what the government claims it is doing.

Even if the government's actions are consistent with Section 215, the constitutionality of the statute itself is questionable. Some courts have held that the Fourth Amendment's restriction on searches and seizures means the government must get a warrant to obtain certain types of records, such as cell phone location data. These rulings are at odds with the wide-ranging, warrantless surveillance program that has been allowed under Section 215.

The same questions can be raised about PRISM. Like Section 215, Section 702 is remarkably broad, allowing the government to target non-U.S. persons "*reasonably believed* to be outside the United States." However, the NSA has reportedly interpreted that to mean that it need only ensure "51 percent confidence of the target's 'foreignness.'" Even if the process works as advertised, it could be wrong nearly half the time. Consequently, one of every two people targeted by the NSA may be an American citizen or located in the U.S. The NSA's training materials call such collection "nothing to worry about." And even if this practice is deemed consistent with Section 702, it is difficult to see how it comports with the Fourth Amendment, which requires the government to obtain a warrant for much of the information about U.S. persons that is being "inadvertently" collected.