CENTER FOR DEMOCRACY & TECHNOLOGY

March 2017

Section 702: Scope of Collection

Under Section 702, the government can obtain your electronic communications content and metadata . . .

- **. . . even though you're not a terrorist**. Section 702 is not just a counterterrorism statute. It is used to obtain any foreign intelligence information, including information **related to "the conduct of the foreign affairs of the United States."** This category is broad enough to include almost anything – from protests over a foreign government's human rights practices to a country's economic policies. Worse, the statute allows the NSA to collect information for such nebulous reasons so long as foreign intelligence is **a "significant" purpose** of the collection – the primary purpose could be something else entirely, like investigating alleged tax evasion. This means that non-U.S. persons who are not connected in any way to terrorism and pose no threat to national security can be targeted for surveillance nonetheless.

- **. . . without judicial approval**. It's the NSA, not an independent judge, that decides whether to target someone – and it does so **with little guidance or post hoc review**. According to the NSA's Targeting Procedures, for example, one factor the NSA considers when deciding whether to target someone is whether there is "reason to believe" the potential target has contacted someone **"associated with" a foreign power or territory**. It is unclear what it takes to be considered "associated with" a foreign power or territory when it comes to 702 surveillance, but such language could be interpreted quite broadly.

- **. . . even though you're a U.S. person**. Although the NSA can only intentionally target non-U.S. persons located abroad, section **702 nonetheless materially affects Americans in several ways**. First, when a U.S. person communicates with a target, the NSA collects those communications. This allows the NSA to collect, for instance, email chains or chat room logs with tens or hundreds of American participants so long as one participant is foreign. As explained above, this applies even when the target is not a suspected terrorist or spy – imagine, for example, an embassy official in London communicating with American friends, or a foreign scientist located abroad sending emails to colleagues at universities in the U.S. **Those communications, despite their lack of national security connection, may be fair game under section 702**.

  In addition, through the Upstream collection program, the NSA obtains information as it flows across the internet backbone. Unlike the PRISM collection program, **under Upstream the NSA collects communications that are not only to or from a target, but also merely** about **a target**. That is, if a communication between two Americans contains a targeted selector (such as an email address or phone number), the NSA can seize that entirely domestic communication. Moreover, information sometimes travels throughout the different network gateways in the form of "Multi-Communication Transactions" (or MCTs), which are bundles of multiple discreet communications. If a single communication in the bundle is to, from, or about a target, the entire communication is collected. This includes wholly domestic communications.

- **. . . and keep it for several years**. The "Minimization Procedures" adopted by the NSA, CIA, and FBI, permit **U.S. person information to be retained and queried in government databases for several years**. First, "foreign communications" may be kept in databases for two or five years (or longer in some circumstances). Communications are "foreign communications" even if one end of the communication involves a person in the U.S. Moreover, whether U.S. person information must be minimized depends largely on whether the communicant is "known" to be a U.S. person. Even if "known" to be a U.S. person, that communication may be kept unless it is "clearly" not relevant to the authorized purpose of collection or evidence of a crime.

- **. . . and use it for reasons that have nothing to do with national security or counterintelligence**. The FBI can (and routinely does) search databases containing section 702 data for evidence of ordinary crimes. It can search and see who is engaged in particularly sensitive activities, such as smoking marijuana or attending political rallies that turn violent. **So long as there's an authorized purpose—such as looking for evidence of a crime — the query is allowed**. Warrantlessly gathered 702 information may then be used **as evidence in a criminal case against a U.S. person** so long as the case involves one of several "serious" crimes. Even if 702 information cannot be used as actual evidence against a U.S. person, law enforcement can still use the information to obtain other evidence that can be used in court.

For more information, visit https://cdt.org/issue/security-surveillance/section-702-of-fisa/ or contact Gregory T. Nojeim, *CDT's Director of the Freedom, Security & Technology Project, at* gnojeim@cdt.org.