CENTER FOR DEMOCRACY & TECHNOLOGY

Responding to the Department of Justice's FAQ on the Use of National Security Letters to Compel Communications Providers to Produce Electronic Communication Transactional Records

September 28, 2016

The Department of Justice is circulating a "frequently asked questions" document on its proposal to expand the use of "national security letters" (NSLs), which are issued without prior court review, to cover requests for "electronic communication transactional records," or "ECTRs." The DOJ's ECTR proposal could permit the FBI, at its sole discretion, to compel communications providers to turn over, among other things, email header information, text logs, and web browsing history in national security investigations.

The DOJ's FAQ contains a number of misstatements, to which we respond below.

For more information, please contact Gabe Rottman, Deputy Director of the Freedom, Security and Technology Project at CDT, at grottman@cdt.org.

DOJ Statement: *"[I]n the online world, ECTRs include information that is the functional equivalent of toll billing records for telephone calls" (page 1).*

CDT Response: No one actually knows how broadly the definition of "ECTR" will sweep. It is not currently defined in statute, and the DOJ ECTR proposal contains language that implies it would encompass more than just the "functional equivalent" of telephone toll billing records. ECTRs could include web browsing history, email header information, and text logs, which are much more revelatory than phone call records.

The closest there is to an ECTR definition appears in an opinion of the DOJ's Office of Legal Counsel (OLC), which issues binding guidance to the administrative agencies. The OLC said that Congress's intent, when it enacted the NSL authority at issue in 1986, was to ensure that the FBI could secure records that are "parallel" to toll billing records from entities other than just the phone company. The OLC did *not* bless an ECTR definition that encompasses, for instance, web browsing history, which the DOJ expressly says it wants under this warrantless authority.

DOJ Statement: "*The courts have held that non-content metadata of this kind, held by third-party service providers, is not protected by the Fourth Amendment" (page 1).*

CDT Response: Not exactly. This is a reference to the "third-party doctrine," which is extremely controversial. Back in the 1970s, the Supreme Court held in two cases (involving a bank and a telephone company) that there is no "reasonable expectation of privacy" in records voluntarily disclosed to a third party, meaning they can be seized without a warrant. *However*, precisely because

of this outdated doctrine, Congress has stepped in and established protections for phone records, stored email, video rental records, financial information, and much more.

Additionally, many expect the courts to revisit the third-party doctrine in the coming years. In the 2012 Supreme Court case *United States v. Jones*, Justice Sotomayor suggested in concurrence that it "may be necessary to reconsider" the third-party doctrine, which, she said, is "ill suited to the digital age, in which people reveal a great deal about themselves to third parties in the course of carrying out mundane tasks." 565 U.S. __, 132 S. Ct. 945, 957 (2012). And, of particular import in the NSL context, Justice Sotomayor wrote: "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year." *Id.* That is exactly what the DOJ and FBI are proposing here.

DOJ Statement: *"Law enforcement has been able to obtain telephone records with a simple subpoena for decades. Likewise, it has for decades obtained addressing information from physical mail—a so-called 'mail cover'—with a written request" (page 1).*

CDT Response: There are two problems with this statement.

One, national security investigations—concerned as they are with preventing terrorism—are much more wide-ranging than the investigation of past, present, or planned criminal activity. For instance, the DOJ successfully argued that, because terrorists use telephones, every single record of a phone call to, from, or within the United States is "relevant" to a national security investigation (a standard similar to NSLs). The DOJ and National Security Agency used that argument to create the bulk telephone surveillance program under section 215 of the Patriot Act.

Two, it is true that law enforcement can obtain toll billing records or IP addresses using administrative or grand jury subpoenas. *But*, it has to secure a court order under 18 U.S.C. § 2703(d) (2012), after a showing of specific and articulable facts that the records are relevant *and* material to an ongoing criminal investigation, to get much of what the DOJ and FBI now seek in the ECTR proposal.

This is, rightly, a higher standard given the greater sensitivity of our email records and web browsing history, which can reveal, among other things, how we vote, who we associate with, what faith we practice (or if we practice), clues to our health and finances, and a myriad of other private information.

DOJ Statement: *"[NSLs] are used in much the same way as grand jury subpoenas are in routine criminal investigations" (page 2).*

CDT Response: There are two problems with this statement.

One, as the DOJ notes, NSLs come with a broad gag order that prevents the recipient from telling anyone about the NSL, save counsel (who is, in turn, gagged) and individuals to whom disclosure is necessary to carry out the order. By contrast, the First Amendment right of the recipient of a grand jury subpoena to talk about the subpoena and her testimony is firmly established.

Two, again, national security investigations are an entirely different beast than criminal investigations. In the bulk telephone metadata program, the DOJ successfully argued that "relevance" to such an investigation is broad enough to encompass records of every phone call made to, from, and within the United States.

DOJ Statement: *"[B]eginning in 2009, most providers have refused to produce ECTRs in response to NSLs, citing the statutory omission from subsection (b). Consequently, the FBI's ability to obtain ECTRs in national security investigations has been substantially impaired since 2009" (page 3). (The DOJ refers to the OLC opinion, noted above, in this passage.)*

CDT Response: The DOJ's statement omits any explanation of why the providers interpret the DOJ OLC opinion to preclude disclosure of ECTRs. In point of fact, as late as 2013, the FBI was demanding ECTRs that are not "parallel" to ordinary phone records, including all email header information, screen names, URLs assigned to the subscriber, and much more.

Toll billing records, while extremely sensitive, are not nearly as revelatory as email header information, text logs, web browsing history, or all of the other digital breadcrumbs we drop as we interact with the internet. Toll billing records could suggest, for instance, a mental health issue (one calls a suicide prevention hotline) or how one votes (a lot of solicitation calls from the RNC). ECTRs provide a detailed picture of everyone and everything we interact with at virtually every moment.

Accordingly, providers appropriately reasoned, with support from the OLC's conclusion that section 2709 only covers those ECTRs that are "parallel" to toll billing records, that the FBI's requests for ECTRs that are not "parallel" to toll billing records were unlawful.

Also, and importantly, although the DOJ has had express authority to seek a court order compelling a provider to comply with a section 2709 NSL since 2006, it has never, to our knowledge, taken a provider to court to force it to hand over the broad categories of ECTRs—email headers, text logs, web browsing history, etc.—that it now claims should be within the scope of the authority.

DOJ Statement: *"Although a [section 215] business records order could be used to obtain ECTRs in certain circumstances, preparing and submitting an application for such an order requires significant time and resources; in recent years, the process can take months from the time the FBI initiates a request to the time the FISC issues an order" (page 3).*

CDT Response: In many ways, this is a feature, not a bug. Section 215 of the Patriot Act expanded the FBI's authority to compel the production of any "tangible thing" relevant to a terrorism investigation, including ECTRs, but with prior court review from the Foreign Intelligence Surveillance Court ("FISC"). In practice, the FISC very rarely denies business records requests under this section.

Much of the time it takes to get a section 215 order is the result of the DOJ's failure to put in place an efficient process (on the criminal side, law enforcement can get a criminal warrant, under a much higher standard, in much less time).

More importantly, the judicial authorization aspect of the process for getting a section 215 order reflects the greater sensitivity of ECTRs as compared to toll records. As noted, ECTRs are much more revealing, both because of volume, and because, unlike most phone calls, emails can be "one-to-many." One email thread in Gmail, for instance, could reveal your five closest friends or 20 close business relationships. Relatedly, it's notable that the DOJ is arguing that the FISC process can't "scale" to meet the *hundreds* of NSLs issued every day. Indeed, that's an argument *against* the ECTR proposal given the sensitivity of these records and the sheer volume of email and web browsing history that would be available under this extraordinary authority if expanded in the manner the DOJ seeks.

DOJ Statement: *"The emergency provision in section 215 (50 U.S.C. § 1861(i)) is an important authority, but does not adequately address the ECTR problem for at least two reasons. First, especially at the preliminary stages of an investigation when ECTRs are often sought, the application to obtain ECTRs would often not qualify as an 'emergency'" (page 4).*

CDT Response: Again, this is a feature, not a bug. Absent an emergency, the DOJ and FBI should not be able to compel providers to disclose email header information, web browsing history, text logs, or other ECTRs the DOJ's proposal seeks without at least going to a neutral magistrate first. That's why it's *emergency* authority (that requires after the fact judicial review).

DOJ Statement: *"A Uniform Resource Locator (URL) designating a particular website could qualify as an ECTR that could be obtained with an NSL, but only if limited to the information that courts have considered to be non-content: the 'fully qualified domain name' (FQDN) portion, which is the information before the first 'slash' in a URL" (page 5).*

CDT Response: Here, the DOJ is saying that, under its proposal, it would be able to compel an ISP to disclose a log of web browsing history, but only the sites you visit, not which pages you click on. In other words, the FBI could demand records showing one visited www.aclu.org, but not www.aclu.org/issues/hiv.

There are two issues here. One, the information available is extraordinarily sensitive, and is much more revelatory than phone records. Two, there's nothing stopping the DOJ from changing its position following passage of the ECTR proposal. The DOJ's forbearance is a matter of discretion, not law.

Not incidentally, the question posed by the DOJ refers to the "target" of an investigation. There is nothing in section 2709 that limits NSL issuance to the target; all relevant records that qualify as ECTRs would be made available, including records of non-targets.

CENTER FOR DEMOCRACY & TECHNOLOGY

DOJ Statement: *"If section 2709 were amended to make clear that ECTRs can be obtained with an NSL, could the FBI track someone's location using Wi-Fi addresses? No. NSLs are requests for historical records; by definition, they do not enable any form of realtime tracking" (page 5).*

CDT Response: First, as the DOJ concedes, it may be possible to fix location based on Wi-Fi, even if not prospectively. Second, IP or other network addresses generally may be used to roughly determine a device's location over time. There is nothing stopping the DOJ from issuing periodic NSLs to the same provider (every day, week, or month), to build up a map of an individual's location over time.

Additionally, assigned network addresses in the mobile space present a special case. With the caveat that every network is engineered differently, a number of technical experts have advised that at least some mobile networks both segment temporarily assigned network addresses by geography (10.1.x.x is, say, California, and 10.2.x.x is New York) and retain that information for some time. Notably, this geographic segmentation can become more granular the larger the number of devices there are in a given area. For instance, the segmentation may be more locative in midtown Manhattan than Wyoming.

Further, as the number of devices connected to mobile networks grows (think cars and wearables), the need to segment the network more narrowly grows. So, even if this information is not particularly locative now, it may become more locative in the future.

DOJ Statement: *"ECTRs do not include the content of communications and are not protected by the Fourth Amendment. They are functionally similar to telephone records, credit card records, or bank records that law enforcement has for decades been able to obtain without court authorization" (page 6).*

CDT Response: They are not functionally similar. They are much more revealing than even telephone records, which themselves are quite revealing. Most ECTRs are the functional equivalent of records that can be obtained with a court order under 18 U.S.C. § 2703(d) (2012). And, as the DOJ notes, when web browsing history is content, it should be obtainable only pursuant to a warrant based on probable cause.

DOJ Statement: *"The FBI has instituted in its Domestic Investigations and Operations Guide (DIOG) procedures that govern the collection, use, and storage of NSL-derived information" (page 6).*

CDT Response: Ironically, the DOJ's reliance on the DIOG highlights—in stark relief—how deficient the checks on NSL abuse would be under its ECTR proposal. Crucially, the Domestic Investigations and Operations Guide is just that—a *guide*. It is not legally binding on the DOJ and is changeable at the discretion of the attorney general. It was last changed in 2013 (posted in 2016).

Also, the DIOG is itself quite weak in terms of checks against abuse. For instance, following controversy over two overly aggressive "leak" investigations in 2013, the DOJ instituted new protections on the

criminal side for subpoenas to members of the news media. These new regulations require attorney general approval for any subpoena and require notice to the target, with limited exceptions.

By contrast, the recently leaked classified appendix to the DIOG governing when NSLs can be issued for the same records is much less protective. When the FBI is expressly seeking to identify confidential media sources, the NSL need only be approved by senior FBI officials, in consultation with the assistant attorney general in charge of the DOJ's National Security Division. In all other cases, the FBI can approve the NSL on its own. These are extremely weak checks against misuse.

***

In sum, the DOJ is seeking an extraordinary expansion of an already extraordinary power. As the Supreme Court stated in 1948 (three years after the end of World War II), "[t]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *United States v. Johnson*, 333 U.S. 10, 14 (1948).

NSLs already run counter to that basic concept of checks and balances, and the ECTR expansion is thus a severe threat to civil liberties and privacy.

Further Resources:

CDT blog:
https://cdt.org/blog/expansion-of-secret-national-security-letters-a-poison-pill-for-email-privacy/

CDT "correcting the record":
https://cdt.org/insight/correcting-the-record-the-ectr-fix/

CDT letter opposing the ECTR proposal:
https://cdt.org/insight/letter-opposing-ectr-fix/