Department of Justice Responses to Frequently Asked Questions on Use of National Security Letters to Obtain Electronic Communication Transactional Records

What are electronic communication transactional records?

The term "electronic communication transactional records" (ECTRs) refers to those categories of information parallel to subscriber information and toll billing records for ordinary telephone service, including addressing, routing, or transmission information for an electronic communication (such as an email or text message). In other words, in the online world, ECTRs include information that is the functional equivalent of toll billing records for telephone calls. Telephone toll billing records include the originating phone number, the phone number called, and the date, time, and length of the call. Similarly, ECTRs for email show the sending email address, the email recipient(s), and the date, time, and size of the email message.

The precise format of the information in an ECTR may vary by provider or service, but the basic concept remains constant: ECTRs show where, when, and with whom an individual is communicating online, but do not include any content of those communications. The courts have held that non-content metadata of this kind, held by third-party service providers, is not protected by the Fourth Amendment.

Why are ECTRs important in national security investigations?

ECTRs can be crucial evidence early in national security investigations, when agents do not yet have a clear indication of a subject's network of contacts. This type of evidence can help the FBI identify others with whom a subject is communicating and thus generate investigative leads. For example, information obtained from ECTRs can help establish the probable cause necessary to get a Foreign Intelligence Surveillance Act (FISA) order or search warrant to allow us to obtain the content of stored communications, identify a potential confidential human source who may be able to provide valuable intelligence to the FBI, or even serve to eliminate a subject from suspicion. As electronic networks have increasingly supplanted telephone networks as the means for terrorists and foreign agents to communicate, our ability to access these records efficiently becomes ever more important to our work.

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. These are routine investigative tools for law enforcement. Just as the record of a telephone call or a letter to a suspected terrorist or spy, or seller of chemicals used to make explosives, may—even without access to the contents of the call or letter—be a critical investigative lead, so too can ECTRs provide key building blocks in developing an investigation.

What is a National Security Letter?

A National Security Letter (NSL) is effectively an administrative subpoena, issued by a federal agency, requiring the production of certain limited types of information held by third-party custodians. NSLs may be issued if the information sought is relevant to an authorized national security investigation, and are used in much the same way as grand jury subpoenas are in routine criminal investigations. NSLs and grand jury subpoenas allow investigators to acquire the sort of very basic information that can serve as the building blocks of an investigation: documents like telephone toll records, and banking and credit records. Unlike grand jury subpoenas, however, NSL authorities are limited to only certain types of records identified in several distinct statutes, each of which has specific rules and restrictions governing the types of records that can be obtained and the nature of the certification that must be provided. And, unlike most grand jury subpoenas, the NSL statutes all contain nondisclosure provisions which, upon certification from a specified government official, restrict the recipient's ability to disclose the NSL.

Can the FBI use an NSL to obtain ECTRs?

One of the NSL statutes, 18 U.S.C. § 2709, allows the FBI to obtain certain records from wire and electronic communication service providers—including "subscriber information and toll billing records information" and "electronic communication transactional records"—where relevant to a national security investigation. The legislative history, which dates back to 1986, indicates that section 2709 was intended to apply "not only to FBI requests for telephone subscriber information and toll billing information, but also to FBI requests for electronic transactional records." S. REP. 99-541, at 43-44 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597-98. It also indicates that section 2709 "ensures that the FBI has the necessary authority with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service." *Id.* at 44, 1986 U.S.C.C.A.N. at 3598. Additionally, although a globally connected internet was still years away in 1986, it is notable that Congress contemplated methods of communication such as "electronic mail" and "electronic bulletin boards" when drafting the statute that provided the FBI with the authority to obtain ECTRs through NSLs. *See id.* at 8-9, 1986 U.S.C.C.A.N. at 3562-63 (providing a glossary of "some of the new telecommunications and computer technologies referred to" in ECPA). Up until 2009, providers routinely complied with their obligations under this statute and produced ECTRs in response to NSLs issued by the FBI under section 2709.

Subsection (a) of section 2709 continues to refer expressly to ECTRs in describing the records that a provider has a duty to disclose in response to an FBI request. However, subsection (b) describes the records the FBI is authorized to request, and due to an apparent drafting error introduced in a 1993 amendment, it omits the term "electronic communication transactional

records." The Department of Justice's Office of Legal Counsel has issued a public opinion indicating that with regard to ECTRs, section 2709 authorizes the FBI to obtain from an electronic communication service provider "those categories of information parallel to subscriber information and toll billing records for ordinary telephone service." "Requests for Information under the Electronic Communications Privacy Act," 32 Op. O.L.C. 145, 147 n.3 (2008). Nevertheless, beginning 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.

Why can't the FBI simply obtain an order under section 215 of FISA or a court order under section 2703(d) instead of an NSL for ECTRs?

Section 215 is a provision of FISA authorizing the government to obtain business records or "tangible things" that are relevant to a national security investigation. This process requires an application to and an order from the Foreign Intelligence Surveillance Court (FISC). Although a 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.

Obtaining a section 215 order necessarily involves five phases: FBI field office initiation and review; FBI Headquarters review; DOJ National Security Division Office of Intelligence review and drafting of an application; FISA Court review and approval; and FBI service of the order. Such a process is not compatible with the role that ECTRs play in a national security investigation: as building blocks to be obtained at the outset of an investigation, not months into it. This is particularly true in the context of fast-paced counterterrorism investigations, where the time when a subject first comes onto the FBI's radar may be only a matter of weeks or days from when he or she is actively engaged in attack planning. In such cases, the FBI's ability to identify and pursue investigative leads without unnecessary procedural burdens is paramount.

Adding resources to the FBI, DOJ, and the FISC in the hope of shortening the length of time needed to obtain a business records order is not the answer. Based on the historical data on the thousands of NSLs issued annually seeking ECTRs, we assess that it is simply not practical for the FBI, DOJ, and the FISC to scale up their processing of business records applications to meet the FBI's needs for ECTRs in national security investigations. If the FBI, DOJ, and the FISC were to begin processing the same number of business records requests as the number of ECTR NSLs issued by the FBI in 2009, the caseload of the FISC would increase dramatically beyond its already heavy dockets, and the resulting number of business records orders would

significantly dwarf the number of full content FISA orders issued by the court.[1] Even if FBI, DOJ, and FISC resources could be scaled up to meet this volume, it is unlikely that these additional resources would sufficiently reduce the time frame, as the procedural requirements and centralized process for obtaining a business records order would remain the same. Such a process is excessive where the data to be produced is non-content metadata that is not protected by the Fourth Amendment.

Acquiring ECTRs pursuant to court orders issued under 18 U.S.C. § 2703(d) is also not the answer. Section 2703(d) is a criminal authority, available only in ongoing criminal investigations and not in exclusively intelligence gathering matters, and it does not provide equivalent mechanisms to protect classified information that would form the basis for such an order in national security cases. Moreover, although the burdens associated with obtaining 2703(d) orders can be spread to DOJ/FBI offices and courts across the country rather than concentrated in the FISC process, use of this tool would inevitably impose additional resource demands to process the significantly increased volume of section 2703(d) orders that would substitute for ECTR NSLs.

The 2015 USA Freedom Act amended section 215 to add an emergency provision. Why doesn't that give the FBI the flexibility it needs?

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." Second, even where the emergency provision can be used, the government must seek the approval of the Attorney General, and is required to submit a full application for a business records order to the FISC within seven days. As discussed above, given the time and associated resources normally required to prepare and file a business records application, the FBI could not use the section 215 emergency authority to obtain ECTRs on the scale needed for all of its national security investigations, including counterterrorism, counterintelligence, and cyber investigations.

[1] As reflected in the transparency report issued by the Office of the Director for National Intelligence for 2015, the FISC approved 142 business records applications under section 215 that year. The increase to the FISC's caseload would number in the thousands if DOJ submitted a comparable number of applications under section 215 as the number of ECTR NSLs issued annually. For comparison, in 2015 the FISC issued 1,585 orders under Titles I and III and sections 703 and 704 of FISA combined.

If section 2709 were amended to make clear that ECTRs can be obtained with an NSL, could the FBI obtain historical records of the websites visited by the target of an investigation?

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. Courts have concluded that a visit to a URL constitutes a communication between the visitor and the website's host. The FQDN portion of the URL is akin to a telephone number dialed by the visitor. In contrast, the files identified after the first "slash" may be akin to the substance of the telephone conversation and thus may constitute "content." For example, in http://www.public.improvisedexplosivedevices.com/components/online-purchase.html, the FBI would only seek to obtain the string www.public.improvisedexplosivedevices.com with an NSL.

It is important to note that Internet service providers (such as cable Internet services or mobile data providers) do not typically collect or retain historical records reflecting the websites visited by their customers, including the FQDN. The NSL statute does not require providers to produce such information if they do not otherwise collect or retain it, or if it would be unduly costly or burdensome to cull the data they do retain into a (non-content) form requested by the government. *See* 32 Op. O.L.C. at 155-57. Thus it is not common for the government to receive such information using either an NSL or a 215 order. Where such information is produced, however, it has the potential to be valuable to FBI's investigations.

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 real-time tracking. With respect to WiFi information in particular, there is no central repository of records showing the WiFi access points used by a given mobile device. If the FBI knows that a certain suspect frequents a particular coffee shop, it *might* be possible, depending on a number of factors, to approach that shop owner and obtain data showing when the target's phone used that shop's wireless access point and for how long.

But the acquisition of such information would no more be "tracking" than if the FBI were to, for instance, ask a suspect's employer for the dates and times he punched a time clock at work. Nor would it be more revealing than a telephone toll billing record indicating that a subject used the landline at his or her residence to place a 23-minute phone call to an associate. These and other types of records (e.g. credit card records) have always been available with subpoena-like legal process—whether an NSL or an ordinary subpoena—even though they may reveal some information about a target's whereabouts at a particular time in the past.

Given how much ECTRs can reveal about a person's online activities, shouldn't court authorization be required for the government to collect them?

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. It is true that any of these types of records can reveal important information about a person's associations and activities—that is why they are of investigative value. But it would upend decades of practice and undermine law enforcement's ability to conduct investigations and protect public safety if court approval were uniformly required for access to non-content records held by third-party custodians in which there is no Fourth Amendment-protected privacy interest, particularly where national security investigations are at issue.

How will the FBI handle instances where a company overproduces information in response to an NSL for ECTRs, such as by providing content?

The FBI has instituted in its Domestic Investigations and Operations Guide (DIOG) procedures that govern the collection, use, and storage of NSL-derived information. In order to ensure that the FBI receives only information responsive to its NSL request, the DIOG mandates the review of all information received from a provider for overproduction before it is used in furtherance of any investigation. DIOG § 18.6.6.3.9. If a company provides information to the FBI that is not covered by the NSL or that cannot lawfully be provided in response to a NSL, then the FBI must take certain specified steps to correct the overproduction. DIOG § 18.6.6.3.10. Where the FBI has no right to seek or retain the information it has been provided, *e.g.*, a company provided the contents of communications, the FBI must either destroy the information or return it to the company that provided it. If the response contains both relevant information within the scope of the NSL, and overproduced information, then an FBI employee may choose to redact the overproduced information from the documents. In no case can the FBI retain and use information received from a company if it did not have the legal authority to seek that information in the first place.