THE NSL TO 215 COLLECTION: DATA FLOWS AND URLS

Since last summer, I have been noting that majority of Section 215 production now consists of Internet data the government used to collect using National Security Letters but — after the Internet companies successfully refused compliance under NSLs anymore in light of an Office of Legal Counsel ruling limiting what could be obtained under NSLs — the government started using Section 215 to obtain.

> We know most Section 215 orders are for Internet records because someone reliable — DOJ's Inspector General in last year's report on National Security Letters — told us that a collection of Internet companies successfully challenged FBI's use of NSLs to collect this stuff after DOJ published an opinion on ECPA in 2008.
>
> > The decision of these [redacted] Internet companies to discontinue producing electronic communication transactional records in response to NSLs followed public release of a legal opinion issued by the Department's Office of Legal Counsel (OLC) regarding the application of ECPA Section 2709 to various types of information. The FBI General Counsel sought guidance from the OLC on, among other things, whether the four types of information listed in subsection (b) of Section 2709 — the subscriber's name, address, length of service, and local and long distance toll billing records — are exhaustive or merely illustrative of the

> > information that the FBI may request in an NSL. In a November 2008 opinion, the OLC concluded that the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL.
> >
> > Although the OLC opinion did not focus on electronic communication transaction records specifically, according to the FBI, [redacted] took a legal position based on the opinion that if the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL, then the FBI does not have the authority to compel the production of electronic communication transactional records because that term does not appear in subsection (b).

That report went on to explain that FBI considered fixing this problem by amending the definition for toll records in Section 2709, but then bagged that plan and just moved all this collection to Section 215, which takes longer.

> > In the absence of a legislative amendment to Section 2709, [2.5 lines redacted]. [Deputy General Counsel of FBI's National Security Law Branch] Siegel told us that the process of generating and approving a Section 215 application is similar to the NSL process for the agents and supervisors in the field, but then the applications undergo a review process in NSLB and the

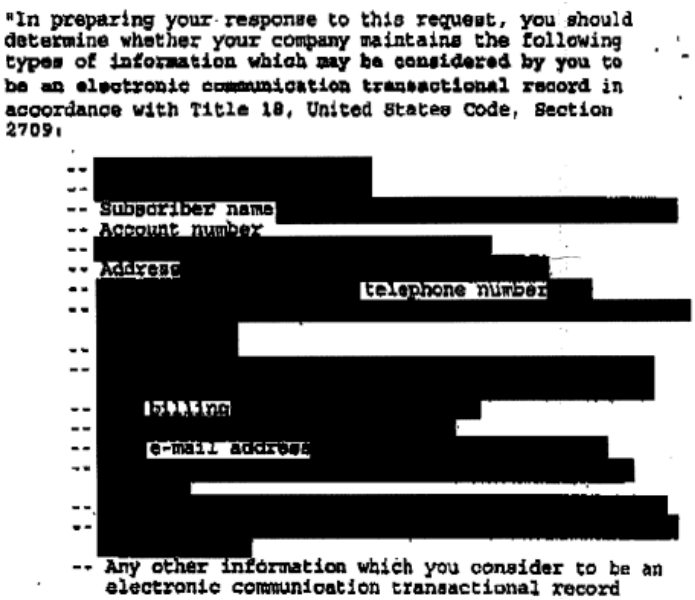
> > Department's National Security Division, which submits the application to the Foreign Intelligence Surveillance Court (FISA Court). According to Siegel, a request that at one time could be accomplished with an NSL in a matter of hours if necessary, now takes about 30-40 days to accomplish with a standard Section 215 application.
>
> In addition to increasing the time it takes to obtain transactional records, Section 215 requests, unlike NSL requests, require the involvement of FBI Headquarters, NSD, and the FISA Court. Supervisors in the Operations Section of NSD, which submits Section 215 applications to the FISA Court, told us that *the majority of Section 215 applications submitted to the FISA Court [redacted] in 2010 and [redacted] in 2011 — concerned requests for electronic communication transaction records*.
>
> The NSD supervisors told us that at first they intended the [3.5 lines redacted] They told us that when a legislative change no longer appeared imminent and [3 lines redacted] and by taking steps to better streamline the application process.

The government is, according to the report, going through all sorts of hoop-jumping on these records rather than working with Congress to pass ECPA reform.

> Why?

The FISA Court imposed minimization procedures on this production, meaning it was fairly bulky. That led me to speculate — particularly given Claire McCaskill questions confirming Section 215 might be used for the purpose — the collection obtained URL search information. More recently, particularly when the FBI claimed (which, sadly, coming from the FBI can never be assumed to be true) it used Section 215 for cyber investigations, I became convinced it involved data flow records.

Meanwhile, in January 2014, Nicholas Merrill, the first person to fight an NSL order when he received one in 2004, started fighting to overturn the gag order that had been imposed on him a decade earlier (this came at the same time as President Obama claimed he would move FBI to end its forever gags on NSLs). And while the FBI agreed to let Merrill tell the target of the NSL about it, it ordered him to keep most of what he had been ordered to turn over secret. He is currently permitted to reveal the following:


"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

-- [redacted]
-- Subscriber name [redacted]
-- Account number [redacted]
-- Address [redacted]
-- [redacted] telephone number [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted] e-mail address [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

In other words, while FBI is okay with Merrill telling the target of a decade-old investigation he or she was targeted, he can't tell us what — as far back as 2004 — FBI claimed was included under ECPA's definition of electronic

communication transactional records.

In December, Merrill sued to be able to tell us that. And on March 20, a redacted version of his declaration in that suit was released. While the government redacted what they had asked of him (and bizarrely, redacted language in his lawyer's declaration that appeared unredacted in documents they included as exhibits; see this Cryptome document for the full packet), Merrill provided a pretty good sense of what might have been included in those 15 (of 16!) redacted or partly redacted orders from a decade ago. First, he described all the records he had:

> Calyx Internet Access, like most ISPs, collected a wide array of information about its clients. For a given client, we may have collected their [1] name, [2] address and [3] telephone number; [4] other addresses associated with the account; [5] email addresses associated with the account; [6] IP addresses associated with the account; [7] Uniform Resource Locator (URL) addresses assigned to the account; [8] activity logs for the account; [9] logs tracking visitors to the client's website; [10] the content of a client's electronic communications; [11] data files residing on Calyx's server; [12] the client's customer list; [13] the client's bank account and [14] credit card numbers; [15] records relating to merchandise bought and sold; and the [16] date the account was opened or closed. [numbers 1 through 16 added]

Of all those 16 things, the only thing that should have been impossible to be included among the 16 requests the FBI made in its NSL demand on Merrill 11 years ago is the actual content of the client's communication, item 10 (though see my caveat below, explaining that they may well have demanded *that* too).

In addition to describing the kinds of things he

had — which therefore might be among the 16 things FBI demanded of him — Merrill described the kinds of things ISPs might have that the FBI might want. He includes URL searches and IP-based identifiers.

> Electronic communication service providers can maintain records of the IP addresses assigned to particular individuals and of the electronic communications involving that IP address. These records can identify, among other things, the identity of an otherwise anonymous individual communicating on the Internet, the identities of individuals in communication with one another, and the web sites (or other Internet content) that an individual has accessed.
>
> Electronic communication service providers can also monitor and store information regarding web transactions by their users. These transaction logs can be very detailed, including the name of every web page accessed, information about the page's content, the names of accounts accessed, and sometimes username and password combinations. This monitoring can occur by routing all of a user's traffic through a proxy server or by using a network monitoring system.
>
> [snip]
>
> Web servers also often maintain logs of every request that they receive and every web page that is served. This could include a complete list of all web pages seen by an individual, all search terms, names of email accounts, passwords, purchases made, names of other individuals with whom the user has communicated, and so on.

And he described flow data — the kinds of things FBI might use in a hacking investigation.

> Electronic communication service providers can also record internet "NetFlow" data. This data consists of a set of packets that travel between two points. Routers can be set to automatically record a list of all the NetFlows that they see, or all the NetFlows to or from a specific IP ,address. This NetFlow data can essentially provide a complete history of each electronic communications service used by a particular Internet user.

In short, Merrill is strongly hinting that he was asked for *both* URL information and NetFlow information. Merrill is hinting that the FBI was using NSLs to obtain detailed descriptions of all of the Internet activities for targets of NSLs.

Merrill also suggests that email subject lines — now considered content — might be demanded. That's interesting because he got served his NSL before the hospital confrontation in 2004, and the government (specifically Michael Hayden) has claimed that subject lines were metadata, not content. So he may be indicating that back in 2004, the FBI was treating subject lines as an electronic communication transactional record (and given that FBI did not withdraw the substance of his NSL until 2006, perhaps continued to do so).

So back in 2004, at least, the FBI was making vast demands for records of all of a target's Internet activity.

There's good reason to believe that this is precisely the kind of production (at least some) Internet companies successfully moved to Section 215 orders in 2009. That's true, in part, because in the NSL IG Report describing all the crazy requests FBI had been making under ECPA, the most substantive ongoing crazy requests appeared to be connected to AT&T production. Seven types of records from a provider that is

almost certainly AT&T were redacted in that IG Report. So while it's likely the FISC now reviews and minimizes that same kind of requests to ISPs as part of Section 215 orders, it probably doesn't from telecoms.

That said, all that might change if the Cybersecurity Information Sharing Act passes. That bill would pre-empt existing laws, including ECPA, for sharing of cybersecurity, leak, or IP theft investigations (and can be used to investigate a broad array of serious crimes). So CISA would provide the legal cover for ISPs to share such information, at least for any ISPs who would "voluntarily" share such data. For that reason, we should look much more closely at the terms of that "voluntary" production.

That's the subject of another post, however.

For now, take Merrill's declaration as pretty strong confirmation that the FBI at least was obtaining both URL search information and data flow information using nothing more than an NSL. Its desire to get such expansive data again is likely at least as pressing an issue behind current surveillance legislation debates as its desire to continue a dragnet of all our phone records.