KEY DETAILS ABOUT THE MITCH MCCONNELL BID TO EXPAND FBI SURVEILLANCE

As I noted, one of the two poison pills that stalled (if not killed) ECPA reform in the Senate Judiciary Committee a few weeks back was a John Cornyn amendment that would give the FBI authority to obtain Electronic Communication Transaction Records — which have been billed as email records, but include far more, including URLs and IP records — with an NSL again.

In a move akin to what he did by attaching CISA to last year's Omnibus bill, Mitch McConnell has moved to shove that amendment through, this time on the Judiciary Appropriation.

Here are some key details about that effort:

Generally, the amendment would not have prevented the Orlando shooting

Republicans are spinning (and therefore some reporters are reporting) the amendment as "an effort … to respond to last week's mass shooting in an Orlando nightclub after a series of measures to restrict guns offered by both parties failed on Monday."

The reason why the ECTR change would not have prevented the Orlando shooting — as I noted when John Cornyn made the same bogus claim — is that, at least according to FBI Director Jim Comey (then what would *he* know?) FBI already obtained Omar Mateen's ECTRs. So it is false to say that this is a real response, except insofar as shifting the way FBI would have gotten ECTRs in this case would have had other implications.

The most obvious implication of obtaining ECTRs via a subpoena versus an NSL is the latter's gag, which the executive would retain significant prerogative over keeping in place years after obtaining the records. NSL gags have been used to hide records collection from their targets — and given that these use a "related to" standard, probably hides the number of innocent people collected for their role in someone else's suspicious behavior — but the record of the Nicholas Merrill NSL makes it clear the gag served even more prominently to hide the kinds of records the government obtained under a broad definition of ECTR.

FBI is doing this to bypass minimization the FISA Court fought for for years

For tactical reasons, privacy groups have been claiming that permitting FBI to obtain ECTRs with an NSL is an *expansion* of FBI authority. That's not technically correct: whether it should have been or not, FBI obtained ECTRs with an NSL from 2001 to 2009, until the publication of an OLC memo gave some tech companies the ability to refuse NSLs asking for ECTRs. Indeed, there's reason to believe some companies — notably including AT&T — still provide some records beyond those listed in the 2008 OLC memo with just an NSL.

But what happened next is critical for understanding why FBI wants this change now. When ECTR collection moved from NSLs to Section 215 orders starting in 2009, the number of 215 orders spiked from about 30 to about 200, and with that, court mandated minimization procedures spiked, and remained elevated, until FBI finally adopted minimization procedures mandated by the 2006 reauthorization of the authority after Edward Snowden's leaks (which makes me wonder whether they were

actually following FISC-ordered minimization in the interim). Given that we know the spike in 215 orders stemmed from ECTR requests, that has to mean that FISC believed this collection was sufficiently intrusive on innocent people that it needed to be minimized.

Side note: it's possible that those 175 ECTR records a year were bulky records: more systematic collection on orders issued four times a year, just like the phone dragnet orders, in lieu of tens of thousands of orders obtained via an NSL prior to that. If that's the case, it's possible that USA Freedom Act's limits on bulk have posed a problem for some, though not all, of this bulky collection. In most cases with a designated suspect, as with Mateen, the FBI could still get the records with a subpoena.

This would push through the more expansive of two ECTR efforts

There are actually two efforts to let the FBI obtain ECTRs via NSL. This amendment, which is largely similar to Cornyn's amendment to ECPA reform, and language already approved in the Intelligence Authorization (see section 803 at pp 64-65) for next year. The Intel Authorization version basically just adds "ECTRs" to the records available under 18 USC 2709.

> request the name, address, length of service, local and long distance toll billing records, and electronic communication transactional records of a person or entity, but not the contents of an electronic communication,

The amendment that will get a vote tomorrow, however, lays out what can be obtained in much greater detail with this list:

> (A) Name, physical address, e-mail

> address, telephone number, instrument number, and other similar account identifying information.
>
> (B) Account number, login history, length of service (including start date), types of service, and means and sources of payment for service (including any card or bank account information).
>
> (C) Local and long distance toll billing records.
>
> (D) Internet Protocol (commonly known as 'IP') address or other network address, including any temporarily assigned IP or network address, communication addressing, routing, or transmission information, including any network address translation information (but excluding cell tower information), and session times and durations for an electronic communication.

There are three big differences in the Cornyn version. The Cornyn amendment affirmatively permits FBI to obtain payment information. The Cornyn amendment affirmatively permits a lot more information, in addition to that financial information, that is used to correlate identities (things like all types of service used, all possible types of "address" or instrument number, and IP generally; see this post for more on correlations). Finally, Cornyn lays out that ECTRs include IP address information.

Nicholas Merrill described the significance of IP address information in a declaration he submitted, with the explanation, "I believe that the public would be alarmed if they knew what kinds of records the FBI apparently believes constitute ECTR," in his bid to unseal the NSL he received.

> 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.
>
> 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.
>
> [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.
>
> Content Delivery Networks, such as Akamai and Limelight Networks, are availability networks that popular websites use to increase the speed at which their content is delivered to users. For example, many of the country's top media, entertainment, and electronic commerce companies use Akamai's services to store images and other rich content so that users can download their pages more quickly. These Content Delivery Networks record every image, webpage, video clip, or other "object" downloaded by every user of their client websites. Content Delivery Networks can therefore serve as independent sources of a user's web browsing history through the records that they store.

In 2004, when Merrill got his NSL, the FBI included Cell Site Location Information in its definition of ECTR. That is excluded here, but there are ways FBI can obtain general location information from IP address and other data included in ECTRs.

FBI likely would (and will, if and when the Intel Authorization passes) argue that ECTRs include the items identified by Merrill even if passed without the specifying language that appears in the Cornyn amendment. But with the language specifying login history and IP metadata, Cornyn's gets much closer to admitting that this kind of information is what FBI is really after.

And, as noted, we should assume the reason FBI wants the gags associated with NSLs is to hide what they're getting even more than from whom they're getting it.

Long live the allegedly never used Lone Wolf

I said above that the amendment that will get a vote tomorrow is almost the same as the Cornyn amendment was. With regards to the NSL language, they're virtually identical. But tomorrow's amendment extends the Lone Wolf provision of the PATRIOT Act — which FBI keeps telling Congress they have never ever used — forever.

I suspect FBI is being disingenuous when they say the Lone Wolf has never been used. I suspect that it, like the roaming wiretap provision, was used by the FISA Court as a concept to justify approving something else. For example, a number of Americans have had FISA warrants deeming them agents of a foreign power even without ever speaking to a member of an actual terrorist group. I suspect — and this is just a wildarsed guess — that FISC will treat a foreign extremist and/or a non-Al Qaeda/ISIS jihadist forum as a lone wolf in concept (the law itself only applies here in the US), thereby finding the ties between the American and that non-formal Islamic extremist entity to reach the bar of agent of a foreign power via foreign-located lone wolf.

If I'm right, the lone wolf provision exists not so much because it has proven necessary as Congress understands it, but as a gimmick to get more Americans treated as foreign agents by FISC. Again, if I'm right, someday this will be disclosed in court (or understood by enough trial judges that it starts being a problem). But if this amendment passes, there will not be an easy time to review the use of lone wolf.

Why didn't the GOP push this on USA Freedom Act?

There's one more point I find notable about

this. The USA Freedom Act affected both NSL and Section 215 orders last year, both of which are central to the question of how FBI obtains ECTRs. It also extended the Lone Wolf provision to December 15, 2019. In other words, Congress just legislated on precisely these issues, and USA Freedom Act would have been the appropriate time to make changes that might be necessary.

So why didn't FBI and Comey do that last year?

Update: With respect to this last question, I've been informed that there *was* a behind the scenes effort to add ECTRs to USAF, though not one that ever made a public draft of the bill.