19 YEARS ON

Next year it will be twenty years on. A few minutes ago it was exactly 19 years to the minute. The first plane hit the North Tower at 8:46 am EST. We now suffer a 9/11 every couple of days in the US thanks to Trump’s bungling of the Coronavirus response.

Fires are decimating some of the most beautiful parts of the country on the west coast. Corona is almost certainly set to rage again with the great “re-opening”.

But let’s take a minute to remember what happened 19 years ago, and how the nation came together and responded then. Imperfectly, and sometimes tragically, from the Bush/Cheney regime. It has all been covered here on these pages. The moment could have created a lasting unity and, instead, was exploited to the opposite. But for a couple of days, it felt different. Let us remember why.

---

702 REAUTHORIZATION BILL: WHY A BACK DOOR FIX FOR CRIMINAL SEARCHES IS

MEANINGLESS

In this post, I explained how the House Judiciary Committee Section 702 reauthorization bill only closes the back door search loophole for "quer[ies] for evidence of a crime." In addition, they let the government define what a "query reasonably designed for the primary purpose of returning foreign intelligence information" is, which means they're basically punting on defining it themselves until 2023.

Given that treatment, the back door search fix is virtually useless, because for every search that might return the communications of an American, the government can always claim they're considering recruiting the American as an informant.

Any communication queryable by back door search by definition involves a person of interest for a foreign intelligence reason

To understand why, first remember why FBI would get this information in the first place. They can only get raw 702 data if they have an active full investigation — and by definition, the targets of that that active full investigation are going to be targeted for the same reasons the target would be targeted by NSA, because they are of national security interest, pertaining to counterterrorism, counterproliferation, and counterintelligence/nation-state hacking.

Thus, any American whose communications might come up in a back door search will — by definition — be someone talking to a target of interest. That doesn't mean they're talking to a "bad guy," as US national security professionals

insist on speaking of adversaries. They're just someone who has foreign intelligence information related to one of those three-plus topics.

Since 2002, the government has insisted that any crime — including rape — can be foreign intelligence information

The precedent that determined the limits of the government's use of FISA-obtained information in criminal proceedings came in the 2002 *In Re Sealed case* challenge where the FISA Court of Review deemed the PATRIOT Act's adoption of "significant purpose" language in FISA targeting to permit the sharing of information for criminal purposes.

As part of that case, the government claimed it could use criminal information to recruit a foreign spy.

> Thus, for example, where information is relevant or necessary to recruit a foreign spy or terrorist as a double agent, that information is "foreign intelligence information" if the recruitment effort will "protect against" espionage or terrorism.
>
> [snip]
>
> Whether the government intends to prosecute a foreign spy or recruit him as a double agent (or use the threat of the former to accomplish the latter), the investigation will often be long range, involve the interrelation of various sources and types of information, and present unusual difficulties because of the special training and support available to

> foreign enemies of this country. [my emphasis]

During the hearing, FISCR judge Laurence Silberman tried to get Solicitor General Ted Olson to envision some kind of crime that couldn't be used for foreign intelligence purpose, suggesting rape. But even that, Olson argued, could be deemed foreign intelligence information, because the government could use evidence of rape to coerce someone to become an informant.

> OLSON: And it seems to me, if anything, it illustrates the position that we're taking about here. That, Judge Silberman, makes it clear that to the extent a FISA-approved surveillance uncovers information that's totally unrelated – let's say, that a person who is under surveillance has also engaged in some illegal conduct, cheating –
>
> JUDGE LEAVY: Income tax.
>
> SOLICITOR GENERAL OLSON: Income tax. What we keep going back to is practically all of this information might in some ways relate to the planning of a terrorist act or facilitation of it.
>
> JUDGE SILBERMAN: Try rape. That's unlikely to have a foreign intelligence component.
>
> SOLICITOR GENERAL OLSON: It's unlikely, but you could go to that individual and say we've got this information and we're prosecuting and you might be able to help us. I don't want to foreclose that.
>
> JUDGE SILBERMAN: It's a stretch.
>
> SOLICITOR GENERAL OLSON: It is a stretch but it's not impossible either. [my emphasis]

The previous year, in 2001, the government had used the threat of a rape prosecution against Abu Zubaydah's brother, Hesham Abu Zubaydah (who had had calls with his brother picked up on wiretaps), to convince him to become an informant. The FISCR decision certainly didn't endorse approving individual FISA warrants to find proof of crimes that could be used to flip people. But neither did it place meaningful limits (and why should it, given that in those halcyon days all FISA orders were individualized).

In years since then, the government has repeatedly told the FISC they're using programmatic spying to find informants. In both 2006 and 2009 it said it would use the phone dragnet "to discover individuals willing to become U.S. Government assets." (see PDF 22 for citations to two Keith Alexander statements) That's also one way the FBI measured the efficacy of Stellar Wind.

The Gartenlaub case shows FBI will use kiddie porn to (attempt to recruit) foreign intelligence informants

This is one reason the Keith Gartenlaub case is so important, in which the government used a criminal warrant, then a FISA warrant, then another criminal warrant to obtain evidence that Gartenlaub had nine-year old kiddie porn on his hard drives. The government justified all those warrants based on the claim that Gartenlaub was working with his Chinese in-laws — who always got described as influential in China — to steal Boeing information to share with China. Ultimately, they found no evidence of that.

I will eventually show evidence that the government *also* used Section 702 against Gartenlaub, probably (at a minimum) to obtain

the Skype conversations he had with his in-laws, who would be targetable as influential Chinese citizens.

In any case, in association with the Gartenlaub case, the government changed both the individual FISA and the Section 702 minimization procedures to permit the sharing of data collected under FISA with the National Center for Missing and Exploited Children, meaning they can use FISA to obtain information on kiddie porn in the name of foreign intelligence collection.

After they indicted Gartenlaub, the government offered to drop the charges for information on the spying with China.

> During his initial appearance in a federal courthouse in Santa Ana, Calif., the prosecutors indicated a willingness to reduce or drop the child pornography charges if he would tell them about the C-17, said Sara Naheedy, Gartenlaub's attorney at the time.

Even at that late date, after eighteen months, two criminal warrants, and a FISA warrant, the government was treating Gartenlaub's alleged kiddie porn possession as potential foreign intelligence information.

One purpose of assessments — and queries conducted under them — is to assess people to become informants

Every description of back door searches is clear: FBI can use them at the assessment level (that is, when they're trying to figure out whether to open a full investigation).

> [W]henever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment. With some frequency, FBI personnel will also query this data, including Section 702–acquired information, in the course of criminal investigations and assessments that are unrelated to national security efforts. In the case of an assessment, an assessment may be initiated "to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence information.

And FBI's Domestic Investigations and Operations Guide is equally clear: the FBI uses assessments to determine whether people would make good informants. For example, the DIOG describes this scenario — which sounds just like what happened to Professor Xiaoxiang Xi — among its scenarios for using assessments.

> A field office has a Full Investigation open on a group of individuals from country X believed to be targeting engineers and high-tech workers involved in the production of semiconductor chips. Evidence in the Full Investigation suggests that the individuals from country X are attempting to recruit the engineers and high tech workers to steal information regarding the semiconductor chips in exchange for money. During the investigation, an engineer who travels frequently to country X has been identified.
>
> Information developed during the Predicated Investigation may be used to determine whether the engineer should be

> viewed as a subject of the investigation or a potential [Confidential Human Source]. If the engineer is determined to be a subject of the Full Investigation, a Type 5 Assessment may not be opened and the engineer needs to be opened as the target of a Full Investigation. If the primary focus of the FBI's interest is to determine whether the individual may be a potential source, a Type 5 Assessment should be opened to collect information necessary to determine whether the FBI should attempt to recruit the engineer as a CHS. (PDF 117)

Remember: the FBI can obtain any 702 data related to a full investigation like the one described here. And Chinese scientists suspected of IP theft would be clear targets under the Foreign Government certificate. So it is solidly within the realm of possibility that the government would target Chinese scientists, obtain conversations (like the one that Xi got targeted for) about semiconductors, and then find that information at a later time when researching the American whose communication got collected incidentally.

That's the problem with trying to fix the back door loophole while still permitting back door searches for foreign intelligence assessments: because it's not until the government pulls up the information at the assessment stage — and it may well be years later, as was the case for Gartenlaub — that the government decides whether they're going to use it and its fruits as foreign intelligence or criminal information.

THE SECRETS THAT REMAIN ABOUT JOURNALIST NSLS

Someone has liberated to the Intercept a copy of the FBI's guidelines for using NSLs to obtain the call records of journalists. The entire appendix is For Official Use Only save one paragraph noting that foreigners serving as spooks or working for news outlets that are agents of a foreign power don't get any protection. Otherwise, this is only being protected under a claim of privilege, not classification. That's particularly troubling given that the US Attorney Guidelines on subpoenaing the press includes equivalent language about agents of a foreign power not getting the special treatment (though here it is more focused on terrorists).

> The protections of the policy do not extend to any individual or entity where there are reasonable grounds to believe that the individual or entity is a foreign power or an agent of a foreign power; a member or an affiliate of a foreign terrorist organization; designated a specially designated global terrorist; a specially designated terrorist; a terrorist organization; committing or attempting to commit a crime of terrorism; committing or attempting to commit the crime of providing material support or resources to a terrorist organization; or aiding, abetting, or conspiring in illegal activity with such individuals or entities. 28 C.F.R.50.10(b)(1)(ii).

The liberated passage (like the USA guidelines) does not, however, define who counts as a member of the news media.

For those so lucky as to be considered a member

of the news media, when DOJ is obtaining their records to learn a confidential source, they need to get the Executive Assistant Director of National Security Branch (who must consult with the AAG for National Security) and General Counsel's approval to obtain an NSL. Note, the Public Affairs Director is not involved in this process, as he or she is supposed to be in the subpoena process (though even there, the policy states that DOJ's Policy and Statutory Enforcement Unit will make the call on who is or is not entitled to be a journalist). Which would say NSLs, on top of being secret and offering the journalist no opportunity to fight the subpoena, also receive only a national security review, not a press review.

Which brings me back to the other point about NSLs I keep harping on. The 2014 NSL IG report showed that the FBI was not reporting at least 6.8% of their NSLs, even to Congress, much less to the Inspector General. When asked about that, FBI said an accurate number was really not worth trying to do, even while it admitted that the uncounted NSLs were "sensitive" cases — a category that includes journalists (and politicians and faith leaders).

That means there's at least a decent possibility that some of the NSLs the FBI chooses not to report to either Congress or the Inspector General — in spite of the clear legal obligation to do so — are of journalists.

Given that they've been hiding this unclassified NSL policy under a dubious claim of privilege, that decent possibility seems all the more likely.

RON WYDEN: OBTAINING

ECTRS WITHOUT A WARRANT IS ALMOST LIKE SPYING ON SOMEONE'S THOUGHTS

As a number of outlets have reported, Ron Wyden has placed a hold on the Intelligence Authorization in an attempt to thwart FBI's quest to be able to obtain Electronic Communication Transaction Records with just a National Security Letter.

But Wyden's released statement on that hold differs in emphasis from what he said in his Senate address announcing the hold yesterday. The statement describes how all toll records — from emails, texts, or web browsing — can infringe on privacy.

> The fact of the matter is that 'electronic communication transaction records' can reveal a great deal of personal information about individual Americans. If government officials know that an individual routinely emails a mental health professional, or sends texts to a substance abuse support group, or visits a particular dating website, or the website of a particular political group, then the government knows a lot about that individual. Our Founding Fathers rightly argued that such intrusive searches should be approved by independent judges.

But in his floor statement, Wyden went on at length about the particular threat posed by obtaining web browsing history (this starts after 4:40).

> For example, the National Security Letters could be used to collect what are called Electronic Communication Transaction Records. This would be email and chat records and text message logs, and in particular, Mr. President, and I've had Senators come up to me to ask me about whether this could be true, folks at home this weekend, when I was out and responding to questions about this, people asked, "Does this really mean that the government can get the Internet browsing history of an individual without a warrant even when the government has the emergency authority if it's really necessary?"
>
> And the answer to that question, Mr. President, is yes, the government can. The government can get access to web browsing history under the Intelligence Authorization legislation, under the McCain amendment, and they can do it without getting a warrant, even when the government can go get it without a warrant when there is an emergency circumstance.
>
> Now the reality is web browsing history can reveal an awful lot of information about Americans. I know of little information, frankly Mr. President, that could be more intimate than that web browsing history. If you know that a person is visiting the website of a mental health professional, or a substance abuse support group, or a particular political organization, or – say – a particular dating site, you know a tremendous amount of private and personal and intimate information about that individual – that's what you get

> when you can get access to their web browsing history without a warrant, even when the government's interest is protected, as I've said, in an emergency.
>
> The reality is getting access to somebody's web browsing history is almost like spying on their thoughts. This level of surveillance absolutely ought to come with court oversight, and as I've spelled out tonight, that is possible in two separate ways — the traditional approach with getting a warrant, and then under Section 102, which I wrote as part of USA Freedom Act, the government can get the information when there's an emergency and come back later after the fact and settle up.

Wyden's statement makes a few other things clear. First, by focusing on the emergency provision of USA Freedom Act, Wyden illustrates that the FBI is trying to avoid court oversight, not so much obtain records quickly (though there would be more paperwork to a retroactive Section 215 order than an NSL).

That means two things. First, as I've noted, FBI is trying to avoid the minimization procedures the FISC spent three years imposing on FBI. Right now, we should assume that FISC would prohibit FBI from retaining all of the data it obtains from web searches, but if it moved (back) to NSL collection it would have no such restriction.

The other thing obtaining ECTRs with NSLs would do, though, is avoid a court First Amendment review, which should be of particular concern with web search history, since everything about web browsing involves First Amendment speech. Remember, a form of emergency provision (one limited to Section 215's phone chaining application) was approved in February 2014. But in the September 2014 order, the FISC

affirmatively required that such a review happen even with emergency orders. A 2015 IG Report on Section 215 (see page 176) explains why this is the case: because once FISC started approving seeds, NSA's Office of General Counsel stopped doing First Amendment reviews, leaving that for FISC. It's unclear whether it took FISC several cycles to figure that out, or whether they discovered an emergency approval that infringed on First Amendment issues. Under the expanded emergency provision under USAF, someone at FBI or DOJ's National Security Division would do the review. But FBI's interest in avoiding FISC's First Amendment review is of particular concern given that FBI has, in the past, used an NSL to obtain data the FISC refused on First Amendment grounds, and at least one of the NSL challenges appears to have significant First Amendment concerns.

In the Senate yesterday, Senator Wyden strongly suggested the FBI wants this ECTR provision so it can "spy[] on their thoughts" without a warrant. We know from other developments that doing so using an NSL — rather than an emergency Section 215 order — would bypass rigorous minimization and First Amendment review.

In other words, the FBI wants to spy on — and then archive — your thoughts.

SENATE NARROWLY AVOIDS VOTING THEMSELVES TO BECOME "TYPOS"

The McCain (Cornyn) amendment to the Judiciary Appropriations bill that would let them get Electronic Communication Transaction Records with a National Security Letter just narrowly

failed to get cloture, with Dan Sullivan flipping his vote to yes near the end but Mike Crapo, a likely no vote, not voting. The final vote was 59-37.

The floor debate leading up to the vote featured a few notable exchanges. Richard Burr was an absolutely douchebag, saying Ron "Wyden is consistently against providing LE the tools it needs to defend the American people." He did so in a speech admitting that, "My colleague says this wouldn't stop SB or Orlando. He's 100% correct."

Burr also insisted that we can't let the Lone Wolf provision, which allegedly has never been used, expire. It was extended just last year and doesn't expire until 2019.

More interesting though was the debate between Burr and Leahy over whether the FBI can't obtain ECTRs because of a typo in the law as passed in 1993. Leahy basically described that Congress had affirmatively decided not to include ECTRs in NSLs (implicit in this, Congress also did not decide to include it in the 2001 expansion). Burr claimed that Congress meant to include it but didn't in some kind of oversight.

Here's how Mazie Hirono and Martin Heinrich described the debate in the report on the Intelligence Authorization, which has a version of the ECTR change.

> The FBI has compared expanding these authorities to fixing a "typo" in the Electronic Communications Privacy Act (ECPA).
>
> However, during consideration of ECPA reform legislation in 1993, the House Judiciary Committee said in its committee report that "Exempt from the judicial scrutiny normally required for compulsory process, the national security letter is an extraordinary device. New applications are disfavored."

> The House Judiciary Committee report also makes clear that the bill's changes to Section 2709(b) of ECPA were a "modification of the language originally proposed by the FBI."
>
> This does not support claims that the removal of the ECTR language was a "typo."

Burr effectively argued that because law enforcement wanted ECTRs to be included back in 1993, they were meant to be included, and Congress' exclusion of them was just a typo.

In short, a member of the Senate just argued that if Congress affirmatively decides not to capitulate to every demand of law enforcement, it must be considered a "typo" and not legally binding law.

For the moment, the Senate voted down making itself a "typo," but Mitch McConnell filed a motion to reconsider, meaning he can bring the vote back up as soon as he arm twists one more vote.

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.

THE FBI IS USING NSLS TO TARGET "FACILITIES" NOW

The Freedom of the Press Foundation has been looking for more details about when the FBI can use NSLs to obtain records including the communication records of journalists, and they just obtained initial response to a FOIA on the subject. There is abundant reason to believe the government does this in leak cases, though as Trevor Timm noted in his piece on this, "a 'broad reading' of the media guidelines [was] allegedly hindering leak investigations" in the summer of 2015.

As part of DOJ's response to FPF's FOIA, the provided a section of the Domestic Investigations and Operations Guide for the FBI that covers NSLs generally. While I don't think the FOIA response provides the date of the DIOG (it was declassified on November 6, 2015), it appears to post-date last June's passage of USA Freedom Act, because it incorporates the language on disclosure from that bill (see the last section).

I was particularly interested in the discussion of reporting to Congress, as that's something DOJ's Inspector General found FBI to have serious problems with in the 2014 IG Report on NSLs.

There are two potentially significant changes in the passage on "notice and reporting requirements" in what FPF obtained (see page 9) from the 2011 version (see page 106) that was the last to be released on comprehensive fashion (see below for the text).

First, and probably most importantly, the 2015 version envisions targeting "facilities/accounts," whereas the 2011 version

envisioned targeting "phone numbers/e-mail accounts/financial accounts." The reason this is so concerning is that, in 2007, the government invented a new meaning for "facility" that could mean an entire data switch. The language is all the more concerning if, as I believe, this DIOG post-dates USAF, because that law limits bulk collection by requiring a selection term for NSLs and other collection. But if they're using that expansive definition of "facility," then selection terms may not be all that limiting.

That language is accompanied by a change I don't entirely understand (I can't figure out whether this alleviates or magnifies my concern about "facilities" being targeted). It appears the FBI has entirely reversed the meaning of the words "target" and "subject" here. Whereas they used to refer to the "target" of an investigation and then track individual "subjects" named in NSLs, they now refer to the "subject" of an investigation (which would more closely match how prosecutors would describe someone not yet charged and might cover enterprise investigations without one identified culprit) and the "target" of an NSL (which would allow all others collected to be treated as incidental collection). In both cases, they're surely accounting for the fact that the FBI may investigate a suspect by investigating other people known to have ties to the suspect. This pertains directly to tracking of US persons swept up, but I'm not entirely sure the net effect. Note, too, the language tying NSLs to "predicated" investigations is different in other parts of the DIOG fragment.

Again, I'm not entirely sure what all this means (aside from the fact that using "facility" instead of email or phone number is very concerning). But it is rather alarming, in any case.

2015 version

> i.e., delineate the number of targeted facilities/accounts in each NSL issued

> to an NSL recipient.
>
> NSLB also reports to Congress the USPER status of the target (as opposed to the subject of the investigation) of all NSLs, other than NSLs that seek only subscriber information. While the subject of the investigation is often the target of the NSL, that is not always the case. The EC must record the USPER status of the target of the NSL – the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must record the USPER status of each person.

2011 version

> The EC must delineate the number of targeted phone numbers/e-mail accounts/financial accounts that are addressed to each NSL recipient. For example, if there are three targets, ten accounts, and six recipients of an NSL, the EC must state how many accounts are the subject of the NSL as to Recipient 1, Recipient 2, etc. It is not sufficient to indicate only that there are ten accounts and six recipients.
>
> In addition, the FBI must report the USPER status of the subject of all NSLs (as opposed to the target of the investigation) other than NSLs that seek only subscriber information. While the subject is often the target of the investigation, that is not always the case. The EC must reflect the USPER status of the subject of the request–the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must reflect the USPER status of each person.

FBI REDACTED PASSAGES SHOWING JUDGE MOCKING ITS STUPID CLAIMS

As I noted earlier, today Nicholas Merrill was finally able to reveal the things he was requested to turn over to the FBI in response to a National Security Letter he received 11 years ago.

The expiration of his gag order also allowed him to publish an unredacted copy of the ruling ending the gag, which was released in redacted form in September. Comparing the two lets us see what the government believed had to be redacted in September. Not only does it show how ridiculous were FBI's claims of secrecy, but also makes it clear FBI used such claims to hide the fact that the judge in the case, Victor Marrero, was mocking the stupidity of its claims.

The most important new disclosure is that the FBI no longer uses NSLs to get location information and that it considered location information to be included among log files. (In all passages, I have underlined what the government originally redacted.)

> Additionally, the Government seeks to keep some information redacted despite publicly conceding that those types of records (i.e., "radius log" information, which is cell-tower based phone tracking information) are no longer sought through NSLs. Yet the Government still argues that this information should remain redacted because it would reveal techniques that might be used at some

> undetermined time under a hypothetical policy promulgated by a future administration.

More stunning is that the government wanted to hide that it can obtain daytime and evening phone numbers with one NSL.

> For example, the Government seeks to prevent Merrill from disclosing that the Attachment requested "Subscriber day/evening telephone numbers" even though the Government now concedes that the phrase "telephone number" can be disclosed. The Court is not persuaded that there is a "good reason" to believe that disclosure of the fact that the Government can use NSLs to seek both day and evening telephone numbers could result in an enumerated harm, especially if it is already publicly known that the Government can use NSLs to obtain a telephone number, more generally.

By golly if the terrorists realize the FBI knows some people have separate work numbers, they're sure to win!

Demands like this clearly tanked the government's credibility with Judge Marrero, because he kicked their ass about the absurdity of some claims, such as their attempt to redact the "s" indicating that the FBI would ask for telephone numbers, plural.

> As another example of the extreme and overly broad character of these redactions, the Government apparently believes that while the public can know that it seeks records of an "address" and a "telephone number," there is a "good reason" to prevent disclosure of the fact that the Government can seek "addresses" and "telephone numbers." (See Gov't Mem. Attach.) In any event, based on the Government's redactions

> alone, a potential target of an investigation, even a dim-witted one, would almost certainly be able to determine, simply by running through the alphabet, that "telephone numberll" could only be "telephone numbers." Redactions that defy common sense such as concealing a single letter at the end of a word diminish the force of the Government's claim to "good reason" to keep information under seal, and undermine its argument that disclosure of the currently-redacted information in the Attachment can be linked to a substantial risk of an enumerated harm.

Marrero then reminded the FBI that they had claimed they were chasing "sophisticated foreign adversaries," not dim-witted terrorists.

> Therefore, it strains credulity that future targets of other investigations would change their behavior in light of the currently-redacted information, when those targets (which, according to the Government, include "sophisticated foreign adversaries," see Perdue Deel. ~ 56) have access to much of this same information from other government divisions and agencies.

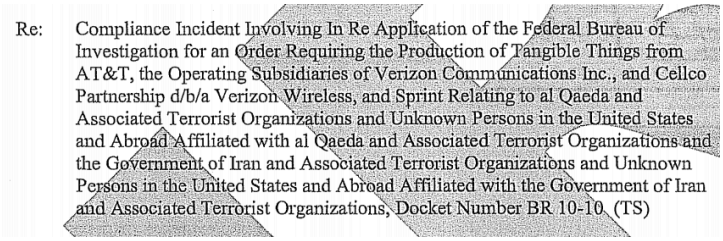
And he revealed that their declarant was demanding things they had already disclosed be kept secret.

> 10 Also interestingly, the Perdue Declaration argues that the category of "[a] ny other information which [the recipient] consider [s] to be an electronic communication transactional record" should not be disclosed. (See Perdue Deel. , 70.) However, this category was not redacted by the Government in its submissions or even in the Perdue Declaration.

Here's the thing though: the last two of these redactions were not hiding secret information at all. Instead, they (plus the phone number comments, though technically those included top secret information about the FBI obtaining telephone numbers, plural) served to hide the fact that Marrero was making fun of the FBI's batshit claims.

Opinions may vary about whether the FBI's 11-year fight to hide the fact it knows some people have work phone numbers was an appropriate use of secrecy. But hiding that a judge is mocking your stupid claims doesn't fit under any legal use of classification. It's abuse, pure and simple.

DOJ THREATENS TO INVOKE STATE SECRETS OVER SOMETHING RELEASED IN FOIA


Re: Compliance Incident Involving In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications Inc., and Cellco Partnership d/b/a Verizon Wireless, and Sprint Relating to al Qaeda and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with al Qaeda and Associated Terrorist Organizations and the Government of Iran and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with the Government of Iran and Associated Terrorist Organizations, Docket Number BR 10-10 (TS)

In a hearing today, Judge Richard Leon said that Larry Klayman could pursue his dragnet challenge by adding a plaintiff who did business with Verizon Business Services. But as part of Klayman's effort, he noted — weakly — that evidence got released showing Verizon Wireless was included in the dragnet. Klayman cited just the Charlie Savage article, not the document released under FOIA showing VZ Wireless on a FISC caption (though I presume his underlying 49 page exhibit includes the actual report — just not necessarily with the passage in question

highlighted).

> It was disclosed on August 12, 2015 by Charlie Savage of The New York Times that Verizon Wireless, as this Court had already ruled in its Order of December 16, 2013, at all material times was conducting and continuing to conduct unconstitutional and illegal dragnet "almost Orwellian" surveillance on Plaintiffs and millions of other American citizens. See Exhibit 1, which is a Government document evidencing this, incorporated herein by reference, and see Exhibit 2, the New York Times article.

Moreover, Klayman surely overstated what the inclusion of VZ Wireless in a phone dragnet Primary Order caption from 2010 showed. Which probably explains why DOJ said "The government has not admitted in any way, shape, or form that Verizon Wireless participated" in the Section 215 phone dragnet, according to Devlin Barrett.

The point is, they should have to explain why it is that, according to a document they've released, VZ Wireless was targeted under the program. Perhaps we'll get that in Northern California, where EFF very competently pointed to what evidence there was.

Which is why the government's threat to invoke state secrets was so interesting.

> The Court should avoid discovery or other proceedings that would unnecessarily implicate classified national-security information, and the potential need to assert and resolve a claim of the state secrets privilege: Plaintiffs' proposed amendments, in particular their new allegations regarding the asserted participation of Verizon Wireless in the Section 215 program, implicate matters of a

> classified nature. The Government has acknowledged that the program involves collection of data from multiple telecommunications service providers, and that VBNS (allegedly the Little Plaintiffs' provider) was the recipient of a now-expired April 25, 2013, FISC Secondary Order. But otherwise the identities of the carriers participating in the program, now, or at any other time, remain classified for reasons of national security. See Klayman, 2015 WL 5058403, at *6 (Williams, S.J.).
>
> At this time the Government Defendants do not believe that it would be necessary to assert the state secrets privilege to respond to a motion by Plaintiffs for expedited injunctive relief that is based on the allegations of the Little Plaintiffs, or even the proposed new allegations (and exhibit) regarding Verizon Wireless. Nor should it be necessary to permit discovery into matters that would risk or require the disclosure of classified national-security information and thus precipitate the need to assert the state secrets privilege. Nevertheless, if Plaintiffs were permitted to seek discovery on the question of whether Verizon Wireless is now or ever has been a participating provider in the Section 215 program, the discovery sought could call for the disclosure of classified national-security information, in which case the Government would have to consider whether to assert the state secrets privilege over that information.
>
> As the Supreme Court has advised, the state secrets privilege "is not to be lightly invoked." United States v. Reynolds, 345 U.S. 1, 7 (1953). "To invoke the . . . privilege, a formal claim of privilege must be lodged by the head of the department which has control

> over the matter after actual personal consideration by that officer." Id. at 7-8. To defend an assertion of the privilege in court also requires the personal approval of the Attorney General. Policies and Procedures Governing Invocation of the State Secrets Privilege at 1-3, http://www.justice.gov/opa/documents/state-secret-privileges.pdf. The Government should not be forced to make so important a decision as whether or not to assert the state secrets privilege in circumstances where the challenged program is winding down and will end in a matter of weeks. Moreover, discovery into national-security information should be unnecessary to the extent the standing of the newly added Little Plaintiffs, and the appropriateness of injunctive relief, may be litigated without resort to such information.
>
> If, however, discovery into national-security information is permitted, the Government must be allowed sufficient time to give the decision whether to assert the state secrets privilege the serious consideration it requires. And if a decision to assert the privilege is made, the Government must also be given adequate time to prepare the senior-level declarations and other materials needed to support the claim of privilege, to ensure that the national security interests at stake are appropriately protected. See, e.g., Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1077, 1090 (9th Cir. 2009).

I think it's quite possible that VZW was not turning over phone records under the Section 215 program in 2010 (which is quite another matter than suggesting NSA was not obtaining a great deal, if not most, of VZW phone records generally). I believe it quite likely NSA

obtained some VZW records under Section 215 during the 2010 period.

But I also believe explaining the distinctions between those issues would be very illuminating.

Meanwhile, the threat of stalling, with all the attendant rigamarole, served to scare Leon — he wants this to move quickly as badly as Klayman does. After all, Leon will have much less ability to issue a ruling that will stand after November 28, when the current dragnet dies.

We shall see what happens in CA when DOJ attempts to make a similar argument.

JOHN DOE UNGAGGED: NICHOLAS MERRILL WINS THE RIGHT TO REVEAL CONTENTS OF 11-YEAR OLD NATIONAL SECURITY LETTER

Nicholas Merrill, who first challenged a National Security Letter 11 years ago, has won the right to talk about what he was ordered to turn over to the FBI in 2004. A key holding from the decision is that private citizens — as distinct from government officials who have signed non-disclosure agreements — cannot be prevented from talking about stuff that the government, as a whole, has already released.

> A private citizen should be able to disclose information that has already been publicly disclosed by any government agency — at least once the underlying investigation has concluded and there is no reason for the

> identities of the recipient and target to remain secret. Otherwise, it would lead to the result that citizens who have not received such an NSL request can speak about information that is publicly known (and acknowledged by other agencies), but the very individuals who have received such NSL requests and are thus best suited to inform public discussion on the topic could not. Such a result would lead to "unending secrecy of actions taken by government officials" if private citizens actually affected by publicly known law enforcement techniques could not discuss them.

The judge in the case, Victor Marrero, gave the government 90 days to appeal. If they don't (?!?!), Merrill will finally be ungagged after 11 years of fighting.

As noted, the FBI served the NSL back in 2004, when Merrill ran a small Internet Service Provider. Merrill sued under the name John Doe. He twice won court rulings that the gag orders were unconstitutional. But it wasn't until 2010 that he was allowed to ID himself as Doe, and it wasn't until 2014 — a decade after receiving the NSL — that he was able to tell the person whose records the FBI wanted. Even then, even after Edward Snowden revealed the need for more transparency about these things, the government fought Merrill's demand to disclose what he had been asked to turn over, which was included in an attachment to the NSL itself.

See this post and this post for background on Merrill's renewed fight to disclose how much FBI has demanded under an NSL.

Marrero found that the government just didn't have really good reasons to gag this information, especially given that substantially similar information had been given out by other government agencies, and especially since the government admits it is only trying to hide the

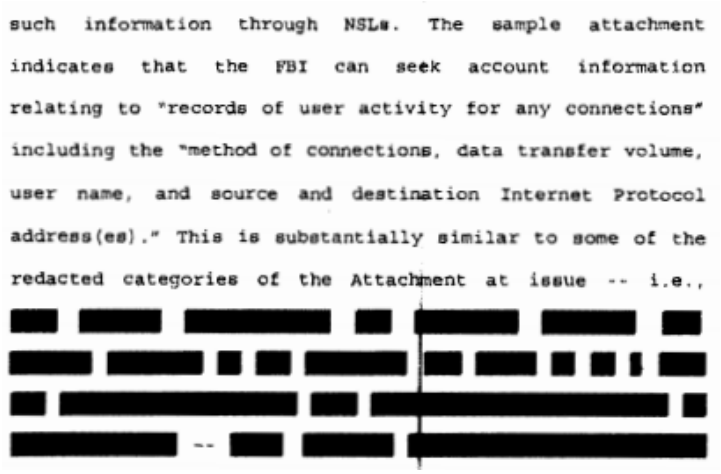
information from future targets, not anyone tied to the investigation that precipitated the NSL over a decade ago.

> For the reasons discussed below, the court finds that the Government has not satisfied its burden of demonstrating a "good reason" to expect that disclosure of the NSL Attachment in its entirety will risk an enumerated harm, pursuant to Sections 2709 and 3511.
>
> [snip]
>
> The Government argues that disclosure of the Attachment would reveal law enforcement techniques that the FBI has not acknowledged in the context of NSLs, would indicate the types of information the FBI deems important for investigative purposes, and could lead to potential targets of investigations changing their behavior to evade law enforcement detection. {See Gov't Mem. at 6.) The Court agrees that such reasons could, in some circumstances, constitute "good" reasons for disclosure.
>
> [snip]
>
> The Government's justifications might constitute "good" reasons if the information contained in the Attachment that is still redacted were not, at least in substance even if not in the precise form, already disclosed by government divisions and agencies, and thus known to the public. Here, publicly-available government documents provide substantially similar information as that set forth in the Attactunent. For that reason, the Court is not persuaded that it matters that these other documents were not disclosed by the FBI itself rather than by other government agencies, and that they would hold significant weight for a potential

> target of a national security investigation in ascertaining whether the FBI would gather such information through an NSL. The documents referred to were prepared and published by various government divisions discussing the FBI's authority to issue NSLs, the types of materials the FBI seeks, and how to draft NSL requests.
>
> [snip]
>
> Now, unlike earlier iterations of this litigation, the asserted Government interest in keeping the Attachment confidential is based solely on protecting law enforcement sensitive information that is relevant to future or potential national security investigations.
>
> [snip]
>
> [I]t strains credulity that future targets of other investigations would change their behavior in light of the currently-redacted information, when those targets (which, according to the Government, [redacted] see Perdue Deel. ¶ 56) have access to much of this same information from other government divisions and agencies.

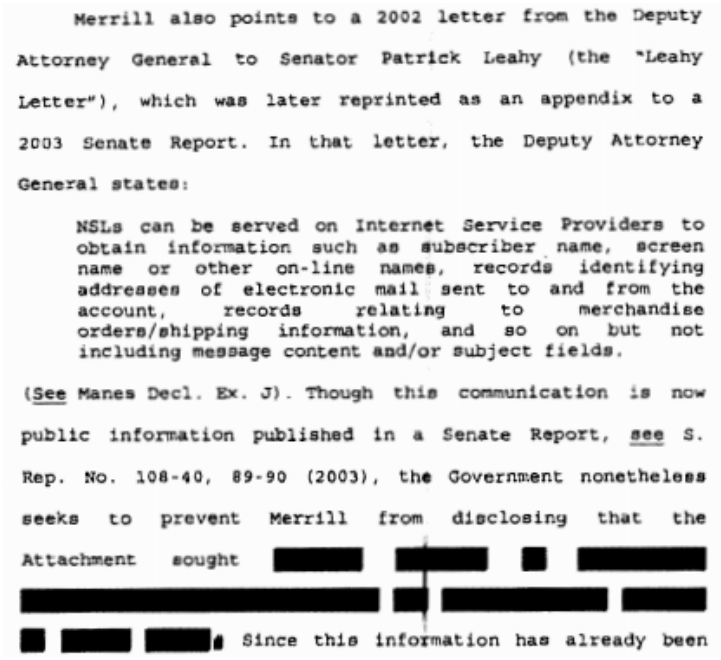
Effectively, Marrero is arguing that since the government has asserted potential national security targets are good at putting 2 plus 2 together, and 2 and 2 are already in the public domain, any targets can already access the information in the attachment.

Marrero's quotations from already released documents and the redactions from the attachment make it clear the government is trying to hide they were getting activity logs…



such information through NSLs. The sample attachment indicates that the FBI can seek account information relating to "records of user activity for any connections" including the "method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es)." This is substantially similar to some of the redacted categories of the Attachment at issue -- i.e., [redacted] --

And the various identities tied to an account (which we know the government matches to better be able to map activity across multiple identities).



Merrill also points to a 2002 letter from the Deputy Attorney General to Senator Patrick Leahy (the "Leahy Letter"), which was later reprinted as an appendix to a 2003 Senate Report. In that letter, the Deputy Attorney General states:

> NSLs can be served on Internet Service Providers to obtain information such as subscriber name, screen name or other on-line names, records identifying addresses of electronic mail sent to and from the account, records relating to merchandise orders/shipping information, and so on but not including message content and/or subject fields.

(See Manes Decl. Ex. J). Though this communication is now public information published in a Senate Report, see S. Rep. No. 108-40, 89-90 (2003), the Government nonetheless seeks to prevent Merrill from disclosing that the Attachment sought [redacted] Since this information has already been

I'll lay more of this out shortly — effectively, Marrero has already done the mosaic work for targets, even without the attachment (though I suspect what the government is really trying to prevent is release of a document defendants can point to to support discovery requests).

Ultimately, Marrero points to the absurd — and dangerous, for a democracy — position that would result if the government were able to suppress this already public information.

> If the Court were to find instead that the Government has met its burden of

> showing a good reason for nondisclosure here, could Merrillever overcome such a showing? Under the Government's reasoning, the Court sees only two such hypothetical circumstances in which Merrill could prevail: a world in which no threat of terrorism exists, or a world in which the FBI, acting on its own accord and its own time, decides to disclose the contents of the Attachment. Such a result implicates serious issues, both with respect to the First Amendment and accountability of the government to the people.

Especially at a time when the President claims to want to reverse the practice of forever gags on NSLs, Marrero finds such a stance untenable.

Let's see whether the government doubles down on secrecy.