SURVEILLANCE WHACK-A-MOLE, SECTION 215 TO SECTION 702 EDITION

One thing that would be consistent with reporting on the NSA's termination of the Section 215 program is that it was improperly using it to collect encrypted app metadata.

INCIDENTAL COLLECTION UNDER SECTION 702 HAS PROBABLY CONTRIBUTED TO TRUMP'S DOWNFALL, TOO

Paul Ryan got Trump to revise his complaints about FISA yesterday by assuring him that Section 702 couldn't have hurt him. But there's a lot of circumstantial evidence to suggest Section 702 was important in getting Papadopoulos to flip as Title I was in getting Flynn to flip.

CONGRESS SHOULD REVERT TO SECTION 702

AS PASSED IN 2008, IF THAT'S WHAT THE SPOOKS WANT!

In an last ditch effort to spook Congress into passing a long-term 702 reauthorization, the spooks say that Congress had it right in 2008 when they authorized a Section 702 that didn't have many of the most invasive aspects.

HPSCI'S BIG REFORM TO SECTION 702: FIGURE OUT WHAT "DERIVED FROM" MEANS, SIX MONTHS TOO LATE

In its greatest act of reform, HPSCI would require the government to tell it why it isn't following notice requirements of FISA 6 months after it's too late to do anything about.

HOW FBI COULD USE REVERSE TARGETING TO USE SECTION 702 AGAINST KEITH GARTENLAUB

While the evidence is circumstantial, the case of Keith Gartenlaub shows why it is so

problematic that the government can reverse target under Section 702.

ELEVEN (OR THIRTEEN) SENATORS ARE COOL WITH USING SECTION 702 TO SPY ON AMERICANS

The Senate Intelligence Committee report on its version of Section 702 "reform" is out. It makes it clear that my concerns raised here and here are merited.

In this post, I'll examine what the report — particularly taken in conjunction with the Wyden-Paul reform — reveals about the use of Section 702 for domestic spying.

The first clue is Senator Wyden's effort to prohibit collection of domestic communications — the issue about which he and Director of National Intelligence Dan Coats have been fighting about since June.

> By a vote of four ayes to eleven noes, the Committee rejected an amendment by Senator Wyden that would have prohibited acquisition under Section 702 of communications known to be entirely domestic under authority to target certain persons outside of the United States. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Senator Cornyn—no; Vice Chairman Warner—no; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—

> aye; Senator King—no; Senator Manchin—no; and Senator Harris—aye.

It tells us that the government collects entirely domestic communications, a practice that Wyden tried to prohibit in his own bill, which added this language to Section 702.

> (F) may not acquire communications known to be entirely domestic;

This would effectively close the 2014 exception, which permitted the NSA to continue to collect on a facility even after it had identified that Americans also used it. As I have explained is used to collect Tor (and probably VPN) traffic to obtain foreigners' data. I suspect that detail is what Wyden had in mind when, in his comments in the report, he said the report itself "omit[s] key information about the scope of authorities granted the government" (though there are likely other things this report hides).

> I have concerns about this report. By omitting key information about the scope of authorities granted the government, the Committee is itself contributing to the continuing corrosive problem of secret law

As the bill report lays out, Senators Burr, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Warner, King, and Manchin are all cool using a foreign surveillance program to spy on their constituents, especially given that Burr has hidden precisely the impact of that spying in this report.

Any bets on whether they might have voted differently if we all got to know what kind of spying on us this bill authorized.

That, of course, is only eleven senators who are cool with treating their constituents (or at least those using location obscuring techniques)

like foreigners.

But I'm throwing Feinstein and Harris in with that group, because they voted against a Wyden amendment that would have limited how the government could use 702 collected data in investigations.

> By a vote of two ayes to thirteen noes, the Committee rejected an amendment by Senator Wyden that would have imposed further restrictions on use of Section 702-derived information in investigations and legal proceedings. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Senator Cornyn—no; Vice Chairman Warner—no; Senator Feinstein—no; Senator Wyden—aye; Senator Heinrich—aye; Senator King—no; Senator Manchin— no; and Senator Harris—no.

While we don't have the language of this amendment, I assume it does what this language in Wyden's bill does, which is to limit the use of Section 702 data for purposes laid out in the known certificates (foreign government including nation-state hacking, counterproliferation, and counterterrorism — though this language makes me wonder if there's a Critical Infrastructure certificate or whether it only depends on the permission to do so in the FBI minimization procedures, and the force protection language reminds me of the concerns raised by a recent HRW FOIA permitting the use of 12333 language to do so).

> (B) in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat of—
>
> (i) terrorism (as defined in clauses (i) through (iii) of section 2332(g)(5)(B)

> of title 18, United States Code);
>
> (ii) espionage (as used in chapter 37 of title 18, United States Code);
>
> (iii) proliferation or use of a weapon of mass destruction (as defined in section 2332a(c) of title 18, United States Code);
>
> (iv) a cybersecurity threat from a foreign country;
>
> (v) incapacitation or destruction of critical infrastructure (as defined in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e))); or
>
> (vi) a threat to the armed forces of the United States or an ally of the United States or to other personnel of the United States Government or a government of an ally of the United States.

Compare this list with the one included in the bill, which codifies the use of 702 data for issues that,

> "Affects, involves, or is related to" the national security of the United States (which will include proceedings used to flip informants on top of whatever terrorism, proliferation, or espionage and hacking crimes that would more directly fall under national security) or involves,
>
> - *Death*
> - *Kidnapping*
> - *Serious bodily injury*
> - *Specified offense against a minor*
> - *Incapacitation or destruction of critical*

> *infrastructure (critical infrastructure can include even campgrounds!)*
> - *Cybersecurity, including violations of CFAA*
> - *Transnational crime, including transnational narcotics trafficking*
> - *Human trafficking (which, especially dissociated from transnational crime, is often used as a ploy to prosecute prostitution; the government also includes assisting undocumented migration to be human trafficking)*
>
> [snip]
>
> Importantly, the bill *does not permit* judicial review on whether the determination that something "affects, involves, or is related to" national security. Meaning Attorney General Jeff Sessions could decide tomorrow that it can collect the Tor traffic of BLM or BDS activists, and no judge can rule that's an inappropriate use of a foreign intelligence program.

The bill report's description of this section makes it clear that — in spite of its use of the word "restriction," — this is really about providing affirmative "permission."

> Section 6 provides restrictions on the Federal Bureau of Investigation's (FBI's) use of Section 702-derived information, so that **the FBI can use** the information as evidence only in court proceedings [my emphasis]

That is, Wyden would restrict the use of 702 data to purposes the FISC has affirmatively approved, rather than the list of 702 purposes expanded to include the most problematic uses of Tor: all hacking, dark markets, and child porn.

So while Feinstein and Harris voted against the use of 702 to collect known domestic communications, they're still okay using domestic Tor commuincations they say they don't want to let NSA collect to prosecute Americans (which is actually not surprising given their past actions on sex workers).

Again, they're counting on the fact that the bill report is written such that their constituents won't know that this is going on. Unless they read me.

Look, I get the need to collect on Tor traffic to go after its worst uses. But if you're going to do that, stop pretending this is a foreign surveillance bill, and instead either call it a secret court bill (one that effectively evades warrant requirements for all Tor wiretapping in this country), or admit you're doing that collection and put review of it back into criminal courts where it belongs.

EVIDENCE THE US GOVERNMENT USED

SECTION 702 AGAINST KEITH GARTENLAUB[‘S PARENTS-IN-LAW]

Some early documents from the Keith Gartenlaub case suggest the government used Section 702 as part of it.

IN DISCUSSION OF UNMASKING ADMIRAL ROGERS GETS CLOSER TO ADMITTING TYPES OF SECTION 702 CYBERSECURITY USE

In a description of masking and unmasking, Admiral Rogers public admits more about how NSA uses Section 702 on cybersecurity.

SECTION 702 REAUTHORIZATION BILL: THE VERY NARROWLY SCOPED BACK DOOR SEARCH FIX

This is my second post on the draft House Judiciary Committee version of the Section 702 reauthorization. In this post, I’ll look at how

the bill tries to fix the back door search loophole. In two followup posts I'll explain why this fix is inadequate legislatively, and why it is inadequate legally.

The back door fix:

- Requires a court order to access content "for evidence of a crime"
- Requires an AG relevance statement to access metadata-plus
- Creates exceptions that swallow the rule
- Prevents reverse targeting
- Mandates simultaneous access to FBI databases
- Permits broad delegation
- Creates auditable records with big loopholes
- Invites the government to define foreign intelligence information

Requires a court order to access content "for evidence of a crime"

Here's the language that requires the government to obtain a court order when accessing Section 702 data.

> (j) REQUIREMENTS FOR ACCESS AND DISSEMINATION OF COLLECTIONS OF COMMUNICATIONS.—
>
> (1) COURT ORDERS AND OTHER REQUIREMENTS.—
>
> (A) COURT ORDERS TO ACCESS CONTENTS.—Except as provided by

> subparagraph (C), in response to a query for evidence of a crime, the contents of queried communications acquired under subsection (a) may be accessed or disseminated only upon—
>
> (i) an application by the Attorney General to a judge of the Foreign Intelligence Surveillance Court that describes the determination of the Attorney General that—
>
> > (I) there is probable cause to believe that such contents may provide evidence of a crime specified in section 2516 of title 18, United States Code (including crimes covered by paragraph (2) of such section);
> >
> > (II) noncontents information accessed or disseminated pursuant to subparagraph (B) is not the sole basis for such probable cause;
> >
> > (III) such queried communications are relevant to an authorized investigation or assessment, provided that such investigation or assessment is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
> >
> > (IV) any use of such queried communications pursuant to section 706 will be carried out in accordance with such section;
>
> (ii) an order of the judge approving such application.

The requirement *only* applies to evidence of crime. It requires the crime to be one of the ones listed in the Wiretap Act, but includes state crimes, which in turn includes drug crimes (and child pornography, which of course is now

in Section 702's minimization procedures).

For some reason, it requires this application to go to FISC, rather than a regular magistrate, which is problematic both from a time management issue for FISC but also for reasons of standardization among magistrates. That's all the more concerning given that the bill doesn't explain what kind of review the FISC judge can do — whether the judge can actually review for probable cause, or whether she doesn't have that authority. This is a big concern, because DOJ has repeatedly told FISC judges in secret that they don't have authority specifically laid out in law, not even when they were asking judges to approve programmatic spying.

One good part of this language is that it requires something beyond metadata from a 702 search to support a probable cause review.

As I'll write in a follow-up, though, the limitation of this to criminal purposes makes it absolutely meaningless — it simply misunderstands how FBI conducts these queries (and obviously doesn't apply to how NSA and CIA do it).

Requires an AG relevance statement to access metadata-plus

In addition to the controls on content, this reauthorization *also* imposes new controls on access to metadata-plus.

> (B) RELEVANCE AND SUPERVISORY APPROVAL TO ACCESS NONCONTENTS INFORMATION.—Except as provided by subparagraph (C), in response to a query for evidence of a crime, the information of queried communications acquired under subsection (a) relating to the dialing, routing, addressing, signaling, or other similar noncontents information may be accessed or disseminated only upon a

> determination by the Attorney General that—
>
> (i) such queried communications are relevant to an authorized investigation or assessment, provided that such investigation or assessment is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> (ii) any use of such queried communications pursuant to section 706 will be carried out in accordance with such section.

This imposes an Attorney General certification of relevance for access to 702-derived "metadata-plus." I'm using that term to refer to the broadened definition of metadata that presumably invokes John Bates' definition adopted in a series of opinions, but which remains entirely redacted.

Consider the absurdity of the proposition that the government can search "just metadata" but metadata is so sensitive it can't be publicly defined. And Congress chooses not to define it here either.

If we need to revisit the definition of metadata, then Congress should do it here, not just nod blindly to redacted opinions at FISC.

And, again, this applies only to crimes.

Creates exceptions that swallow the rule

As I keep saying, the back door search fix only applies to criminal searches. Here's what is not included.

> (C) EXCEPTIONS.—The requirement for an order of a judge pursuant to subparagraph (A) and the requirement for

> a determination by the Attorney General under subparagraph (B), respectively, shall not apply to accessing or disseminating queried communications acquired under subsection (a) if one or more of the following conditions are met:
>
> (i) Such query is reasonably designed for the primary purpose of returning foreign intelligence information.
>
> (ii) The Attorney General makes the determination described in subparagraph (A)(i) and
>
> > (I) the person related to the queried term is the subject of an order or emergency authorization that authorizes electronic surveillance or physical search under this Act or title 18 United States Code; or
> >
> > (II) the Attorney General has a reasonable belief that the life or safety of a person is threatened and such contents are sought for the purpose of assisting that person.
>
> (iii) Pursuant to paragraph (5), the person related to the queried term consents to such access or dissemination.

First, the bill exempts emergency or threat to life queries.

But before it does that, it exempts all requests "designed for the primary purpose of returning foreign intelligence information." In a different section, HJC punts on the issue of defining what "foreign intelligence information" means, directing the government to do that in minimization procedures.

It punts on more than that. How can you have one category for "primary purpose" FI information, but then not treat criminal searches as primary?

Where does that line end? Especially given that this is permitted, for both criminal and intelligence purposes, at the assessment level, which is before the government has any evidence.

In short, even where it is writing exceptions, the bill does it in such a way as to let the split swallow the rule.

Prevents reverse targeting

I think this language prohibits reverse targeting.

> (D) LIMITATION ON ELECTRONIC SURVEILLANCE OF UNITED STATES PERSONS.—If the Attorney General determines that it is necessary to conduct electronic surveillance on a known United States person who is related to a term used in a query of communications acquired under subsection (a), the Attorney General may only conduct such electronic surveillance using authority provided under other provisions of law.

As I read it, if the FBI queries 702 data and finds evidence of a crime, they cannot then develop that evidence using already collected (or newly targeted) 702 data. They have to get a criminal warrant to do it.

Mind you, this is the kind of authorities laundering they do anyway, but this prohibition is worthwhile.

Mandates simultaneous access to FBI databases

The most interesting — and potentially dangerous — language in this section mandates that when the FBI does queries, all the data they have be accessible.

> (E) SIMULTANEOUS ACCESS OF FBI DATABASES.—The Director of the Federal Bureau of Investigation shall ensure that all available investigative or intelligence databases of the Federal Bureau of Investigation are simultaneously accessed when the Bureau properly uses an information system of the Bureau to determine whether information exists in such a database. Regardless of any positive result that may be returned pursuant to such access, the requirements of this subsection shall apply.

I say it's dangerous, because it might require very compartmented data to be more broadly accessible.

But the other thing that's interesting about it is it will ensure that if there's any multiplicitous data in the databases, FBI will have options to bypass the intent of the back door fix.

Consider: a great deal of individually targeted FISA data will replicate data obtained using 702 (which may in fact be the data the government used to obtain a targeted FISA order). A search on such data will return both the traditional FISA data and the 702 data. In cases where the FBI can use the former, they don't have to bother with a "warrant" from FISC. As FBI obtains more and more raw EO 12333 data, that will be even more true there.

So while there may be an interesting operational reason for this — perhaps FBI even missed information in some sensitive investigation because not all data was accessible? — there are also clear downsides and the likelihood this will turn into a workaround to make the back door search even less meaningful.

Permits broad delegation

Another thing HJC doesn't bother to specify is how broadly the Attorney General can delegate the authority for these various declarations.

> (F) DELEGATION.—The Attorney General shall delegate the authority under this paragraph to the fewest number of officials that the Attorney General determines practicable.
>
> (2) AUTHORIZED PURPOSES FOR QUERIES.—A collection of communications acquired under subsection (a) may only be queried for legitimate national security purposes or legitimate law enforcement purposes.

This was a significant problem behind the early NSL abuses. Letting the AG decide how much authority he wants to delegate invites similar abuses and is not why we're paying Congress.

Creates auditable records with big loopholes

As always with transparency provisions, the loopholes are far more interesting than the provisions themselves, because they reveal where the interesting stuff is hiding. This requirement applies to all four agencies that get raw 702 traffic: NSA, CIA, NCTC, and FBI.

NSA is already doing this kind of record-keeping (sort of, though given the violations discovered last year, there's reason to doubt it). But once they set the requirement, they create big problematic loopholes.

> (3) RETENTION OF AUDITABLE RECORDS.— The Attorney General and each Director concerned shall retain records of

> queries that return a positive result from a collection of communications acquired under subsection (a). Such records shall—
>
> (A) include such queries for not less than 5 years after the date on which the query is made; and
>
> (B) be maintained in a manner that is auditable and available for congressional oversight.

With this language, HJC exempts Congressional queries (which I'm fine with), but also tech queries.

> (4) COMPLIANCE AND MAINTENANCE.—The requirements of this subsection do not apply with respect to queries made for the purpose of—
>
> (A) submitting to Congress information required by this Act or otherwise ensuring compliance with the requirements of this section; or
>
> (B) performing maintenance or testing of information systems.

Until at least 2010, NSA was using tech queries to do metadata searches that weren't authorized by the phone dragnet (which was facilitated by having tech people co-located with analysts, which made it easy for the analysts to as for help). If you exempt tech people, you will have abuses on any restriction.

In addition, the auditable record requirement doesn't count for those who've given consent, which includes informants.

> (5) CONSENT.—The requirements of this subsection do not apply with respect to—
>
> (A) queries made using a term relating to a person who consents to such queries; or

> (B) the accessing or the dissemination of the contents of queried communications of a person who consents to such access or dissemination.

From this I assume that a great many of these queries (especially those at CIA that aren't now being counted) are being done for Insider Threat detection, which tracks a bunch of people who, by obtaining a clearance, have given consent for this kind of searching. I assume there are a great many of them too, since they need to be hidden.

> (6) DIRECTOR CONCERNED.—In this subsection, the term 'Director concerned' means the following:
>
> (A) The Director of the National Security Agency, with respect to matters concerning the National Security Agency.
>
> (B) The Director of the Federal Bureau of Investigation, with respect to matters concerning the Federal Bureau of Investigation.
>
> (C) The Director of the Central Intelligence Agency, with respect to matters concerning the Central Intelligence Agency.
>
> (D) The Director of the National Counterterrorism Center, with respect to matters concerning the National Counterterrorism Center.

Invites the government to define foreign intelligence information

Finally, the bill requires the government to adopt a meaning for "query reasonably designed for the primary purpose of returning foreign

intelligence information" in yearly certifications, rather than doing it themselves.

> (b) PROCEDURES.—Subsection (e) of such section 6 (50 U.S.C. 1881a(e)) is amended by adding at the end the following new paragraph:
>
> (3) CERTAIN PROCEDURES FOR QUERYING.—The minimization procedures adopted in accordance with paragraph (1) shall describe a query reasonably designed for the primary purpose of returning foreign intelligence information pursuant to subsection (j)(1)(C)(i).''.

Again, it is the job of Congress to do this. Once the IC defines this in such a way that will further swallow up the rule, what then? We wait until 2023 (which is when this law would next get reauthorized) to define the term meaningfully? At some point we need to have an explicit discussion about the foreign intelligence purposes that drive a lot of these queries, and talk about whether they're permissible under the Fourth Amendment. Now would be a good time, but this language just punts the question.

Other 702 posts

702 Reauthorization Bill: The "About" Fix (What Is A Person?)

DID NSA START USING SECTION 702 TO COLLECT FROM VPNS IN

2014?

It appears likely that a challenge to a new kind of 702 collection in late 2014 pertained to collection that would obtain, but not use, US person collection.