I CON THE RECORD'S "GENERALLY" USEFUL SECTION 702 Q&A

As the next step in the effort to reauthorize FISA Section 702, I Con the Record has a released a "generally" useful Q&A document on the law. For those who haven't been following along, it includes links to many (though not all) of the public resources on Section 702. It provides a generally fair overview, with some new almost admissions, which should at least provide Congress with a road map for unanswered questions they should demand answers on.

Downplaying FBI back door searches

My biggest gripe with the report parallels a gripe I've had about public testimony on Section 702 since the first confirmations that the NSA, CIA, and FBI can conduct queries on raw data — back door searches. In public hearings, the intelligence community always sends NSA witnesses who can describe, as former NSA lawyer April Doss did in March, a back door search process that is fairly constrained.

> I'm most familiar with NSA's processes: NSA analysts must obtain prior approval to run U.S. person identifier queries in FAA 702 content; there must be a basis to believe the query is reasonably likely to return foreign intelligence information; all queries are logged and reviewed after the fact by NSA; and DoJ and ODNI review every U.S. person query run at NSA and CIA, along with the documented justifications for those queries.

Of course, even though this description is completely true (as far as we know), it is

completely useless when it comes to helping Congress understand the problems inherent to back door searches.

Here's what the Q&A document says about back door searches.

> The government's minimization procedures restrict the ability of analysts to query the databases that hold "raw" Section 702 information (i.e., where information identifying a U.S. person has not yet been minimized for permanent retention) using an identifier, such as a name or telephone number, that is associated with a U.S. person. Generally, queries of raw content are only permitted if they are reasonably designed to identify foreign intelligence information, although the FBI also may conduct such queries to identify evidence of a crime. As part of Section 702's extensive oversight, DOJ and ODNI review the agencies' U.S. person queries of content to ensure the query satisfies the legal standard. Any compliance incidents are reported to Congress and the FISC.
>
> 12 Queries of Section 702 data using U.S. person identifiers are sometimes mischaracterized in the public discourse as "backdoor searches."

While it's true that NSA and CIA minimization procedures impose limits on when an analyst can query raw data for content (but not for metadata at CIA), that's simply not true at FBI, where the primary rule is that if someone is not cleared for FISA themselves, they ask a buddy to access the information. As a result — and because FBI queries FISA data for any national security assessment and "with some frequency" in the course of criminal investigations. In other words, partly because FBI is a domestic agency and partly because it has broader querying authorities, it conduct a "substantial" number

of queries as opposed to the thousands done by CIA. Here's how PCLOB describes it:

> In 2013, the NSA approved 198 U.S. person identifiers to be used as content query terms.
>
> [snip]
>
> In 2013, the CIA conducted approximately 1,900 content queries using U.S. person identifiers. Approximately forty percent of these content queries were at the request of other U.S. intelligence agencies. Some identifiers were queried more than once; the CIA has advised that approximately 1,400 unique identifiers were queried during this period.
>
> [snip]
>
> The CIA does not track how many metadata-only queries using U.S. person identities have been conducted.
>
> [snip]
>
> [T]he FBI's minimization procedures differ from the NSA and CIA's procedures insofar as they permit the FBI to conduct reasonably designed queries "to find and extract" both "foreign intelligence information" and "evidence of a crime."
>
> [snip]
>
> Because they are not identified as such in FBI systems, the FBI does not track the number of queries using U.S. person identifiers. The number of such queries, however, is substantial for two reasons. First, the FBI stores electronic data obtained from traditional FISA electronic surveillance and physical searches, which often target U.S. persons, in the same repositories as the FBI stores Section 702–acquired data, which cannot be acquired through the intentional targeting of U.S. persons.

> As such, FBI agents and analysts who query data using the identifiers of their U.S. person traditional FISA targets will also simultaneously query Section 702–acquired data. Second, whenever 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.

So it's simply dishonest to say that, "Generally, queries of raw content are only permitted if they are reasonably designed to identify foreign intelligence information," because the most common queries involve national security and common criminal purposes as well. "Generally," the queries don't require such things, unless you're focusing primarily at CIA and NSA, where the threat to US person privacy at the least.

Then, one thing this Q&A doesn't say is that Judge Thomas Hogan required the FBI to tell FISC of any positive hits on searches for entirely criminal purposes. Congress should know that, because it's an easy data point that the IC should be able to share with Congress.

And while the document generally describes giving notice to defendants,

> Section 706 governs the use of Title VII-derived information in litigation; as with Traditional FISA, it requires the government to give notice to aggrieved persons when the government intends to use evidence obtained or derived from Title VII collection in

> legal proceedings.

It doesn't hint at how apparently inadequate this notice has been. Those are all details that Congress needs to know.

Hiding a cybersecurity certificate in the cheap seats?

I'm also interested in how the Q&A describes the purpose of 702. Here's the 5 bullet points describing 702 successes (I've changed ODNI's bullets to numbers for ease of reference):

> 1. *NSA has used collection authorized under FISA Section 702 to acquire extensive insight into the highest level decision-making of a Middle Eastern government. This reporting from Section 702 collection provided U.S. policymakers with the clearest picture of a regional conflict and, in many cases, directly informed U.S. engagement with the country. Section 702 collection provides NSA with sensitive internal policy discussions of foreign intelligence value.*
> 2. *NSA has used collection*

authorized under FISA Section 702 to develop a body of knowledge regarding the proliferation of military communications equipment and sanctions evasion activity by a sanctions-restricted country. Additionally, Section 702 collection provided foreign intelligence information that was key to interdicting shipments of prohibited goods by the target country.

3. *Based on FISA Section 702 collection, CIA alerted a foreign partner to the presence within its borders of an al-Qaeda sympathizer. Our foreign partner investigated the individual and subsequently recruited him as a source. Since his recruitment, the individual has continued to work with the foreign partner against al-Qaeda and ISIS affiliates within the country.*

4. *CIA has used FISA Section 702 collection to uncover details, including a photograph, that enabled an African partner to arrest two ISIS-affiliated militants who had traveled from Turkey and were connected to planning a specific and immediate threat against U.S. personnel and interests. Data recovered from the arrest enabled CIA to learn additional information about ISIS and uncovered actionable intelligence on an ISIS facilitation network and ISIS attack planning.*
5. *NSA FISA Section 702 collection against an email address used by an al-Qaeda courier in Pakistan resulted in the acquisition of a communication sent to that address by an unknown individual located in the United States. The message indicated that the United States-based individual was urgently*

> *seeking advice regarding how to make explosives. The NSA passed this information to the FBI. Using a National Security Letter (NSL), the FBI was able to quickly identify the individual as Najibullah Zazi. Further investigation revealed that Zazi and a group of confederates had imminent plans to detonate explosives on subway lines in Manhattan. Zazi and his co-conspirators were arrested and pled guilty or were convicted of their roles in the planned attack. As the Privacy and Civil Liberties Oversight Board (PCLOB) found in its report, "[w]ithout the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway bombing plot might have succeeded."*

The list has two advantages over the lists the IC was releasing in 2013. First, it's more

modest about its claims, not, this time, listing every quasi-thwarted terrorist funding opportunity as a big success. In addition, it describes all three confirmed certificates (from the Snowden documents): counterterrorism (bullets 3 through 5), counterproliferation (2), and foreign government (1, though if this is Iran, it might also be counterproliferation). It also admits that one point of all this spying is to find informants (bullet 3), even if not as explicitly as some court filings and IG reports do. That purpose — and the associated sensitivities (including whether and how it is used by FBI) is one thing all members of Congress should be briefed on.

That said, the description of the foreign government certificate doesn't come close to describing the kinds of people who might be swept up in it, and as such provides what I believe to be a misleading understanding of who might be targeted under 702.

Note, too, the silence about the use of certificates for counterintelligence purposes, which the government surely does. Again, that would present different threats to Americans' privacy.

Then there's the last sentence of the document, in the upstream collection section.

> Furthermore, this collection has allowed the IC to acquire unique intelligence that informs cybersecurity efforts.

Oh, huh, what's that doing there in the last line of the document rather than in the successes section?

From the very first public discussions of 702 after Edward Snowden, ODNI included cybersecurity among the successes, even before it had a certificate. In fact, the document released June 8, 2013, just three days after the first Snowden release, echoed some of the same language:

> Communications collected under Section 702 have provided significant and unique intelligence regarding potential cyber threats to the United States including specific potential computer network attacks. This insight has led to successful efforts to mitigate these threats.

This is a problem! Whether or not upstream 702 could be used for cyber purposes has been an undercurrent since the first USA Freedom Act. There are conflicting reports on whether NSA did obtain a cyber certificate in 2012, as they hoped to, or whether that was denied or so limited that it didn't serve the function the NSA needed. I've even been told that CISA is supposed to serve the same purpose.That said, FBI's minimization procedures (but not, by my read, NSA's) include some language directed at cybersecurity.

Congress deserves to have a better sense of whether and how the government is using upstream 702 for cybersecurity, because there are unique issues associated with it. It's clearly a great application of upstream searches, but not one without some risks. So the government should be more clear about this, at least in classified briefings available to all members.

Admitting NSA uses Section 704 not Section 703

Finally, this language is as close as the IC has come to admitting that it uses Section 704, not Section 703, to target Americans overseas.

> In contrast to Section 702, which focuses on foreign targets, Section 704 provides additional protection for collection activities directed against U.S. persons located outside of the United States. Section 2.5 of Executive

> Order 12333 requires the AG to approve the use of "any technique for which a warrant would be required if undertaken for law enforcement purposes" against U.S. persons abroad for intelligence purposes. The AG's approval must be based on a determination that probable cause exists to believe the U.S. person is a foreign power or an agent of a foreign power. Section 704 builds upon these pre-FAA requirements and provides that, in addition to the AG's approval, the government must obtain an order from the FISC in situations where the U.S. person target has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." The FISC order must be based upon a finding that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and that the target is reasonably believed to be located outside the United States. By requiring the approval of the FISC in addition to the approval of the AG, Section 704 provides an additional layer of civil liberties and privacy protection for U.S. persons located abroad.
>
> In addition to Sections 702 and 704, the FAA added several other provisions to FISA. Section 701 provides definitions for Title VII. Section 703 allows the FISC to authorize an application targeting a U.S. person located outside the U.S. when the collection is conducted inside the United States. Like Section 704, Section 703 requires a finding by the FISC that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably

> believed to be located outside the United States.

I've written about the distinction here.

Now, in theory, the authority used may not make a difference. Moreover, it's possible that the NSA simply uses 705b for Americans overseas, meaning they can rely on domestic providers for stored Internet data, while using their more powerful spying for overseas content (in which case Congress should know that too).

But I also think the methods used *may* have an impact on US persons' privacy, both the target and others. I'll try to lay this out in a post in the coming days.

All of which is to say, this document is useful. But there are a few areas — particularly with FBI back door searches, which is the most important area — where the document gets noticeably silent.