THE SOURCE OF THE SECTION 702 LIMITATIONS: SPECIAL NEEDS?

Way back in 2013, in Marty Lederman's review of the NSA Review Group's Report, he pointed to the Report's suggestion that Section 702 collection was limited to use with counterterrorism, counterproliferation, and cybersecurity.

> The Report contains an interesting clue about how the government is presently using Section 702 that I do not recall being previously disclosed—and raises a related question about legal authorities under that provision of the FAA:
>
> The Report explains (page 136) that in implementing Section 702, "NSA identifies specific 'identifiers' (for example, e-mail addresses or telephone numbers) that it reasonably believes are being used by non-United States persons located outside of the United States to communicate foreign intelligence information within the scope of the approved categories (e.g., international terrorism, nuclear proliferation, and hostile cyber activities).
>
> [snip]
>
> Later, on pages 152-53, the authors "emphasiz[e] that, contrary to some representations,**section 702 does *not* authorize NSA to acquire the content of the communications of masses of ordinary people**. To the contrary, section 702 authorizes NSA to intercept communications of non-United States persons who are outside the United States ***only* if it reasonably believes that a particular 'identifier' (for example, an e-mail address or a**

> **telephone number) is being used to communicate foreign intelligence information related to such matters as international terrorism, nuclear proliferation, or hostile cyber activities**." (Italics in original.)
>
> I may be mistaken, but I don't believe that there's anything in the statute itself that imposes the limitations in bold—neither that the NSA must use such "identifiers," nor that international terrorism, nuclear proliferation, and hostile cyber activities are the only topics of acceptable foreign intelligence information that can be sought. Perhaps the FISC Court has insisted upon such limits; but, as far as I know, the Section 702 authority as currently codified is not so circumscribed.

Of course, if you're a regular emptywheel reader, you likely know where this has been suggested in the past, since I've been pointing out this apparent limitation to Section 702 since June 10 and discussed some implications of it here, here, and here.

In a response to Lederman, Julian Sanchez provided some specific cautions about treating these category limits as true "limitations." He suggests it is unlikely that the Intelligence Community or the FISA Court would impose such limitations.

> The 702 language, codified at 50 U.S.C. §1881a, permits the NSA to acquire any type of "foreign intelligence information," which is defined extraordinarily broadly to encompass, inter alia, anything that relates to the "conduct of the foreign affairs of the United States." But here we have the Review Group suggesting repeatedly that 702 surveillance is only for acquiring certain specific types of

> foreign intelligence information, related to nuclear proliferation, international terrorism, or cybersecurity. Have the intelligence agencies or the FISC imposed a more restricted reading of "foreign intelligence information" than the FISA statute does? I doubt it.

While I agree with most of Sanchez' other cautions, I actually do think it likely that the FISC conducts a review that ends up in such limited certifications. They did it for application of Section 215 to the phone dragnet (which legally could have been used for counterintelligence purposes) and I think they may well have done so with Section 702.

FISCR only ruled bulk content collection legal for "national security" foreign intelligence purposes

We'll learn whether I'm right or not when the FISC releases more of the 2008 Yahoo challenge to Protect America Act directives. But there is enough detail in the unclassified August 22, 2008 FISA Court of Review opinion released in early 2009 to suggest where that limitation may have come from.

The FISCR opinion, written by Bruce Selya, describes the certifications before the Court as limited to "foreign intelligence for national security purposes," a limitation that already circumscribes PAA (and the FISA Amendments Act, as Sanchez has laid out), which allow their use for foreign intelligence generally.

> In essence, as implemented, the certifications permit surveillances conducted to obtain foreign intelligence for national security purposes when those surveillances are directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States. [my emphasis]

This limitation is important because of the way Selya deals with the affirmation, in the FISC ruling before the FISCR, that there is a foreign intelligence exception to the Fourth Amendment: by instead finding a special needs exception to the Fourth tied to national security.

> The recurrent theme permeating the petitioner's arguments is the notion that there is no foreign intelligence exception to the Fourth Amendment's Warrant Clause. 6 The FISC rejected this notion, positing that our decision in In re Sealed Case confirmed the existence of a foreign intelligence exception to the warrant requirement.
>
> While the Sealed Case court avoided an express holding that a foreign intelligence exception exists by assuming arguendo that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds, see 310 F.3d at 741-42, we believe that the FISC's reading of that decision is plausible.
>
> The petitioner argues correctly that the Supreme Court has not explicitly recognized such an exception; indeed, the Court reserved that question in United States v. United States District Court (Keith), 407 U.S . 297, 308-09 (1972). But the Court has recognized a comparable exception, outside the foreign intelligence context, in so-called "special needs cases. In those cases, the Court excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.
>
> [snip]
>
> The question, then, is whether the

> reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States. Applying principles derived from the special needs cases, we conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception.
>
> For one thing, the purpose behind the surveillances ordered pursuant to the directives goes well beyond any garden variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security. [my emphasis]

While Reggie Walton, who wrote the FISC ruling, seems to have found a general foreign intelligence exception to the Fourth Amendment, Selya's analysis limited it to foreign intelligence for national security purposes.

Then, when Selya conducts a reasonableness analysis, he returns to national security purposes.

> Here, the relevant governmental interest — the interest in national security — is of the highest order of magnitude. See Haig v. Agee, 453 U.S. 280, 307 (1981); In re Sealed Case, 310 F.3d at 746. Consequently, we must determine whether the protections afforded to the privacy rights of targeted persons are reasonable in light of this important interest.

Thus, while it appears Walton's analysis may have been broader, Selya — who rejected Yahoo's

effort to treat this as a facial challenge and relied on a number of specifics about the certifications before the Court to approve this application of it — only found PAA reasonable under the Fourth Amendment and therefore constitutional for the wiretapping of foreign agents for national security purposes.

The FISCR's ruling, which upon publication led other Internet companies to join PRISM under FAA, leaves open the possibility there might be certifications for which such bulk collection might not be reasonable, and it appears to distinguish those that have a clear national security application from more generalized foreign intelligence purposes.

Other details provide some hints about what "national security" foreign intelligence might include

There are three other details that suggest FISCR's ruling that PAA was constitutional may have been limited to things like terrorism which provide further clarity on how the FISC might interpret national security interests.

First, in an unconvincing effort to reject Yahoo's citation of FISCR's 2002 In re Sealed Case decision calling for functions analogous to warrants, Selya notes that NSA's application was based, in part, on a DOD statement of necessity.

> First, the petitioner notes that we found relevant six factors contributing to the protection of individual privacy in the face of a governmental intrusion for national security purposes. See In re Sealed Case, 310 F.3d at 737-41 (contemplating prior judicial review, presence or absence of probable cause, particularity, necessity, duration, and minimization) . On that exiguous basis, it reasons that our decision there requires a more rigorous standard for gauging reasonableness.
>
> This is a mistaken judgment.

> [snip]
>
> The AG's decision was informed by the contents of an application made pursuant to Department of Defense (DOD) regulations. See DOD, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DOD 5240.1-R, Proc. 5, Pt. 2.C (Dec. 1982) . Those regulations required that the application include a statement of facts demonstrating both probable cause and necessity.

Second and almost certainly very closely related, the language of Jack Goldsmith's May 6, 2004 OLC opinion authorizing the illegal wiretap program, on which the logic of the PAA must be significantly based, ties the purpose of the illegal wiretapping program to the need to find terrorists within the US (note, while I'm not arguing Goldsmith wrote them originally, a number of other paragraphs from his opinion showed up in recent state secrets invocations in Jewell, showing that much of this language is still operative boilerplate to explain the balancing analysis behind bulk content collection in the US).

> The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, it happens that the enemy may use public communications networks and some of the enemy may already be in the United States.
>
> [snip]
>
> As noted above [redacted—the Presidential Surveillance Program] is limited to communications suspected to be those of al Qaeda, al Qaeda-

> affiliated organizations and other international terrorist groups that the President determines both (i) are in armed conflict with the United States and (ii) pose a threat of hostile action within the United States.
>
> [snip]
>
> Finally, as part of the balancing of interests to evaluate the Fourth Amendment reasonableness, we think it is significant that [PSP] is limited solely to those international communications for which "there are reasonable grounds to believe … [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group." March 11, 2004 Authorization [redacted] The interception is thus targeted precisely at communications for which there is already a reasonable basis to think there is a terrorism connection. This is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem."

Both Goldsmith's memo (see PDF 14) and the Draft NSA IG Report (PDF 10) make it clear that, in addition to temporarily shutting down the Internet dragnet, the March 19, 2004 modifications to the program narrowed the program's focus to exclude the Iraqi Intelligence figures who had previously been included, suggesting that Goldsmith only felt he could approve the program for terrorists.

That is, the legal stance of the program — at least as it existed before FISC first approved orders covering the program in 2007 — tied reasonableness and therefore arguably legality to the kind of target and the kind of task, identifying enemies within the US.

Finally, it's possible that by the time Yahoo's challenge got to FISCR, its scope had already been limited. The initial certifications were amended, presumably by Walton, though it's not clear in what way.

> The original certifications were amended, and we refer throughout to the amended certifications and the directives issued in pursuance thereof.

So it may be that Walton set certain outside boundaries for PAA/PRISM collection from the very start.

From terrorism to WMD to cybersecurity to … drug war?

Thus, the bulk content collection programs' predecessor – the illegal wiretap program – was sold as a legal special need explicitly tied solely to terrorism. With the 2008 passage of FISA Amendments Act, Congress affirmatively added WMD proliferators, so it is unsurprising that FISC has approved certifications for it.

Which leaves just cybersecurity as an expansion off the original (pre-FISC) scope, presumably the third certification John Bates authorized for 2012.

At one level, the cybersecurity case is harder to make. After all, there's no authorization to use military force against China's hackers. It's a lot harder to prove that hackers have any association with a foreign power (though here, the overly broad definition of foreign power may come into play).

That said, I can imagine the government might make a defense-contractor related case for military necessity. And according to Ron Wyden, the OLC memo that supports some kind of crazy definition of common commercial services agreements that might be used with cybersecurity dates to 2003 (I'll return to this later), meaning that as with the terror surveillance program, FISC may have been faced with an

illegal cyber surveillance program they needed to legalize with dubious legal opinions.

But it's easy to imagine how DOJ would justify including cybersecurity, because Jack Goldsmith has already made that case publicly.

> the cybersecurity threat is more pervasive and severe than the terrorism threat and is somewhat easier to see.
>
> [snip]
>
> As cyber-theft and cyber-attacks continue to spread (and they will), and especially when they result in a catastrophic disaster (like a banking compromise that destroys market confidence, or a successful attack on an electrical grid), the public will demand government action to remedy the problem and will adjust its tolerance for intrusive government measures.

And the rationale is the same: that you need to collect content to be able to identify who the enemies in the US are.

But remember: Congress may well specifically preclude the use of Section 702 with cybersecurity; Leahy-Sensenbrenner would limit the use of Section 702 to authorize upstream collection for anything but terrorism and proliferation after a 6 months grace period.

So it seems plausible, at least, that FISC has only approved (and perhaps the government has only asked to approve) bulk content collection for those applications that present a real threat of domestic attack and the rationale that the government must use surveillance to identify the enemy. Such a limit would parallel the similar limit placed on the phone dragnet, where the FISC has not permitted the NSA to query the phone dragnet for permissible counterintelligence purposes (unless that's the basis they used to authorize its use with Iranian targets).

All that said, Sanchez is right. So long as FISC keeps what certifications have been approved secret, they can change at any time, even off the yearly cycle the three other certifications would be approved. After all, the logic behind the terrorism argument and probably behind the cybersecurity one — that wiretapping content is the best way to find the enemy in the US — could easily be applied to drug cartels.

But this is why I think the upstream collection limitations on cybersecurity seems so significant. The more this program looks like domestic surveillance (and I can imagine that upstream collection on malware identifiers might well be largely domestic), the more likely Congress will limit Section 702 statutorialy.