THE TIMING OF THE CONTEMPLATED UPSTREAM CYBER-GRAB

There's an aspect missing thus far from the discussion of NSA's possible bid for a cyber certification under Section 702 for primary use in the collection of attack signatures that could not be attributed to a foreign government.

The timing.

The discussion of creating a new Section 702 certificate came in the aftermath of the 6-month back and forth between DOJ and the FISA Court over NSA having collected US person data as part of its upstream collection (for more detail than appears in the timeline below, see this post). During that process, John Bates ruled parts of the program — what he deemed the *intentional* collection of US person data within the US — to be unconstitutional. That part of his opinion is worth citing at length, because of the way Bates argues that the inability to detach entirely domestic communications that are part of a transaction does not mean that those domestic communications were "incidentally" collected. Rather, they were "intentionally" collected.

> Specifically, **the government argues that NSA is not "intentionally" acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic** and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. **This argument fails for several reasons**.
>
> NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore,

> to the extent NSA's upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA's acquisition is "unintentional." In fact, the government has argued, that the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [redacted]
>
> [snip]
>
> The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional."
>
> [snip]
>
> [T]here is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server.
>
> [snip]
>
> By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. (44-45, 48)

There are a number of ways to imagine that victim-related data and communications obtained with an attack signature might be considered "intentional" rather than "incidental," especially given the Snowden document acknowledging that so much victim data gets collected it should be segregated from regular collection. Add to that the far greater likelihood that the NSA will unknowingly target domestic hackers — because so much of hacking involves obscuring attribution — and the likelihood upstream collection targeting hackers would "intentionally" collect domestic data is quite high.

Plus, there's nothing in the 2011 documents released indicating the FISC knew upstream collection included cyber signatures — and related victim data — in spite of the fact that "current Certifications already allow for the tasking of these cyber signatures." No unredacted section discussed the collection of US person data tied to the pursuit of cyberattackers that appears to have been ongoing by that point.

Similarly, the white paper officially informing Congress about 702 didn't mention cyber signatures either. There's nothing public to suggest it did so after the Senate rejected a Cybersecurity bill in August, 2012, either. That bill would have authorized less involvement of NSA in cybersecurity than appears to have already been going on.

With all that in mind, consider the discussions reflected in the documents released last week. The entire discussion to use FBI's stated needs to apply as backup to apply for a cyber certificate came at the same time as NSA is trying to decide what to do with the data it illegally collected. Before getting that certificate, DOJ approved the collection of cyber signatures under other certificates. It seems likely that this collection would violate the spirit of the ruling from just the prior year.

And NSA's assistance to FBI may have violated the prior year's orders in another way. SSO contemplated delivering all this data directly to FBI.

> (S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

Yet one of the restrictions imposed on upstream collection — voluntarily offered up by DOJ — was that no raw data from NSA's upstream collection go to FBI (or CIA). If there was uncertainty where FBI's targeting ended and NSA's began, this would create a violation of prior orders.

Meanwhile, the reauthorization process had already started, and as part of that (though curiously timed to coincide with the release of DOJ's white paper on 702 collection) Ron Wyden and Mark Udall were trying to force NSA to figure out how much US person data they were collecting. Not only did the various Inspectors General refuse to count that data (which would have, under the logic of Bates' opinions finding that illegally collected data was only illegal if the government knew it was US person data, made the data illegal), but the Senate Intelligence Committee refused to consider reconstituting their Technical Advisory Committee which might be better able to assess whether NSA claims were correct.

Sometime in that period, just as Wyden was trying to call attention to the fact that NSA was collecting US person data via its upstream collection, NSA alerted the Intelligence Committees to further "overcollection" under upstream collection.

> (1) ~~(TS//SI//NF)~~ [redacted] NSA/CSS notified the Congressional intelligence committees about an overcollection of FAA §702 upstream collection as well as collection under other authorities. [redacted] (b)(1) P.L. 8 50 US [redacted] NSA has deployed a short-term solution to address the problem and is continuing work on a long-term solution.

As I suggested here, the length of the redaction

and mention of “other authorities” may reflect the involvement of another agency like FBI. One possibility, given the description of FBI collecting on cyber signatures using both PRTT and (presumably) traditional FISA in the discussions of SSO helping the FBI conduct this surveillance (note, I find it interesting though not conclusive that there is no mention of Section 215 to collect cybersecurity data), is that the initial efforts to go after these signatures in some way resulted in overcollection. If FISC interpreted victim-related data to be overcollection — as would be unsurprising under Bates’ 2011 upstream opinion — then it would explain the notice to Congress.

One more point. In this post, I noted that USA F-ReDux authorized FISC to let the government use data it had illegally collected but which FISC had authorized by imposing additional minimization procedures. It’s just a wildarseguess, but I find it plausible that this 2012 overcollection involved cyber signatures (because we know NSA was collecting it and there is reason to believe it violated Bates’ 2011 opinion), and that any victim data now gets treated under minimization procedures and therefore that any illegal data from 2012 may now, as of last week, be used.

All of which is to say that the revelation of NSA and FBI’s use of upstream collection to target hackers involves far more legal issues than commentary on the issue has made out. And these legal issues may well have been more appropriate for the government to reveal before passage of USA F-ReDux.

Update, 11/6: Some dates added from this opinion.

May 2, 2011: DOJ Clarification to FISC letter first admits MCT problem.

May 5, 2011: Government asks for extension until July 22, 2011.

Mid-2011: NSA's Special Source Operations becomes aware of FBI's intent to seek orders involving telecom infrastructure.

July 8, 2011: Court (John Bates) meets with senior DOJ people, tells them he has serious concerns.

July 14, 2011: Government files another extension; court grants extension to September 20, 2011.

September 13, 2011: In filing submitted in response to Bates request, government refuses to count entirely US person content collected under upstream collection.

September 14, 2011: Court extends deadline to October 10, 2011.

October 3, 2011: John Bates rules parts of upstream 702 unconstitutional.

Before October 6, 2011: Government considers appealing Bates ruling.

October 13, 2011: Bates issues briefing order on illegally collected upstream data. Government responds by arguing 1809(a)(2) doesn't apply to it.

October 31, 2011: Bates approves new minimization procedures accounting for MCT problem but apparently not cyber collection.

December 9, 2011: PRTT order expires without renewal, NSA discontinues PRTT Internet dragnet and destroys all data.

December 20, 2011: FBI requests access to NSA's "access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers" to carry out FISA cyber orders (both Pen Register and content) targeting IP addresses.

December 21, 2011: SSO prepares approval form for assistance to FBI.

Late 2011: Government decides to start mitigating upstream 702 data.

January 2012: Obama reconfirms Transit Program.

March 23, 2012: New Cyber Certificate in the works.

March 27, 2012: SID Director Theresa Shea signs off on staff processing form for assistance to FBI.

April 2012: Government orally informs Bates it will purge upstream 702 data collected prior to October 31, 2011.

May 2012: DOJ approves targeting certain signatures under FAA FG Certificate.

May 4, 2012: DOJ informs Congress about 702 (including notice of MCT problem) in anticipation of 702 reauthorization. DOJ does *not* tell Congress NSA is using upstream 702 to collect on anything but email and phone identifiers.

May 4, 2012: Ron Wyden and Mark Udall request Charles McCullough to investigate how many Americans have been caught in upstream collection.

May 22, 2012: SSCI marks up FAA Reauthorization, rules Wyden amendment to reconstitute SSCI Technical Advisory Group to examine FAA out of order.

June 6, 2012: George Ellard tells Wyden a request for number of Americans caught in upstream collection is not possible and would violate the privacy of Americans.

June 16, 2012: Wyden releases McCullough's public response.

July 2012: DOJ approves targeting certain IP addresses under FAA.

July 1 to September 30, 2012: NSA informs Congress about upstream Section 702 (and other authority) overcollection.

August 2, 2012: Cybersecurity Bill of 2012 fails cloture vote.

August 24, 2012: Government submits first document for reauthorization and amendment (without mention of new certificate): “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications.”

September 20, 2012: FISC first approves minimization procedures allowing FBI to share of information it believes may mitigate or prevent cyber intrusions with private entities. Note, it’s possible this change also applied to NSA, but that does not appear in the unredacted discussion. If it only applies to FBI, it should pertain to PRISM production, as FBI doesn’t (or didn’t) get unminimized upstream data.

December 2012: FAA extended until December 31, 2017.

August 30, 2013: FISC approves revised language permitting FBI (unclear whether this also includes NSA) sharing of cyber threat information with private entities.