THE SECTION 215 RAP SHEET

Marco Rubio, who is running for President as an authoritarian, claims that "There is not a single documented case of abuse of this program."

He's not alone. One after another defender of the dragnet make such claims. FBI witnesses who were asked specifically about abuses in 2011 claimed FBI did not know of any abuses (even though FBI Director Robert Mueller had had to justify FBI's use of the program to get it turned back on after abuses discovered in 2009).

> Comment – Russ Feingold said that Section 215 authorities have been abused. How does the FBI respond to that accusation?
>
> A – To the FBI's knowledge, those authorities have not been abused.

Though Section 215 boosters tend to get sort of squishy on their vocabulary, changing language about whether this was illegal, unconstitutional, or abusive.

Here's what we actually know about the abuses, illegality, and unconstitutionality of Section 215, both the phone dragnet program and Section 215 more generally.

Judges

First, here's what judges have said about the program:

1) The phone dragnet has been reapproved around 41 times by at least 17 different FISC judges

The government points to this detail as justification for the program. It's worth noting, however, that FISC didn't get around to writing an opinion assessing the program legally until 10 judges and 34 orders in. Since Snowden

exposed the program, the FISC appears to have made a concerted effort to have new judges sign off on each new opinion.

2) Three Article III courts have upheld the program:

Judges William Pauley and Lynn Winmill upheld the constitutionality of the program (but did not asses the legality of it); though Pauley was reversed on statutory, not constitutional grounds. Judge Jeffrey Miller upheld the use of Section 215 evidence against Basaaly Moalin on constitutional grounds.

3) One Article III court — Judge Richard Leon in Klayman v. Obama — found the program unconstitutional.

4) The Second Circuit (along with PCLOB, including retired Circuit Court judge Patricia Wald, though they're not a court), found the program not authorized by statute.

The latter decision, of course, is thus far the binding one. And the 2nd Circuit has suggested that if it has to consider the program on constitution grounds, it might well find it unconstitutional as well.

Statutory abuses

1) As DOJ's IG confirmed yesterday, for most of the life of the phone dragnet (September 2006 through November 2013), the FBI flouted a mandate imposed by Congress in 2006 to adopt Section 215-specific minimization procedures that would give Americans additional protections under the provision (note—this affects all Section 215 programs, not just the phone dragnet). While, after a few years, FISC started imposing its own minimization procedures and reporting requirements (and rejected proposed minimization procedures in 2010), it nevertheless kept approving Section 215 orders.

In other words, in addition to being illegal (per the 2nd Circuit), the program also violated this part of the law for 7 years.

2) Along with all the violations of minimization procedures imposed by FISC discovered in 2009, the NSA admitted that it had been tracking roughly 3,000 presumed US persons against data collected under Section 215 without first certifying that they weren't targeted on the basis of First Amendment protected activities, as required by the statute.

> Between 24 May 2006 and 2 February 2009, NSA Homeland Mission Coordinators (HMCs) or their predecessors concluded that approximately 3,000 domestic telephone identifiers reported to Intelligence Community agencies satisfied the RAS standard and could be used as seed identifiers. However, at the time these domestic telephone identifiers were designated as RAS-approved, NSA's OGC had not reviewed and approved their use as "seeds" as required by the Court's Orders. NSA remedied this compliance incident by re-designating all such telephone identifiers as non RAS-approved for use as seed identifiers in early February 2009. NSA verified that although some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process discussed above, none of those alerts resulted in reports to Intelligence Community agencies.

NSA did not fix this problem by reviewing the basis for their targeting; instead, it simply moved these US person identifiers back onto the EO 12333 only list.

While we don't have the background explanation, in the last year, FISC reiterated that the government must give First Amendment review before targeting people under Emergency Provisions. If so, that would reflect the second time where close FISC review led the government to admit it wasn't doing proper First Amendment reviews, which may reflect a more systematic problem. That would not be surprising, since the

government has already been chipping away at that First Amendment review via specific orders.

Minimization procedure abuses

1) The best known abuses of minimization procedures imposed by the FISC were disclosed to the FISC in 2009. The main item disclosed involved the fact that NSA had been abusing the term "archive" to create a pre-archive search against identifiers not approved for search. While NSA claimed this problem arose because no one person knew what the requirements were, in point of fact, NSA's Inspector General warned that this alert function should be disclosed to FISC, and it was a function from the Stellar Wind program that NSA simply did not turn off when FISC set new requirements when it rubber-stamped the program.

But there were a slew of other violations of FISC-imposed minimization procedures disclosed at that time, almost all arising because NSA treated 215 data just like it treats EO 12333, in spite of FISC's clear requirements that such data be treated with additional protections. That includes making query results available to CIA and FBI, the use of automatic search functions, and including querying on any "correlated" identifiers. These violations, in sum, are very instructive for the USA F-ReDux debate because NSA has never managed to turn these automated processes back on since, and one thing they presumably hope to gain out of moving data to the providers is to better automate the process.

2) A potentially far more egregious abuse of minimization procedures was discovered (and disclosed) in 2012, when NSA discovered that raw data NSA's techs were using over 3,000 files of phone dragnet data on their technical server past the destruction date.

> As of 16 February 2012, NSA determined that approximately 3,032 files

> containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to document why certain contact chaining rules were created. In addition to the BR work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata.

But rather than investigate this violation — rather than clarify how much data this entailed, whether it had been mingled with Stellar Wind data, whether any other violations had occurred — NSA destroyed the data.

> In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the

> applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.

From everything we've seen the tech and research functions are not audited, not even when they're playing with raw data (which is, I guess, why SysAdmin Edward Snowden could walk away with so many records). So not only does this violation show that tech access to raw data falls outside of the compliance mechanisms laid out in minimization procedures (in part, with explicit permission), but that NSA doesn't try very hard to track down very significant violations that happen.

Overall sloppiness

Finally, while sloppiness on applications is not a legal violation, it does raise concerns about production under the statute. The IG Report reviewed just six case files which used Section 215 orders. Although the section is heavily redacted, there are reasons to be significantly concerned about four of those.

- An application made using expedited approval that made a material misstatement about where FBI obtained a tip *about the content of a phone call*. The FBI agent involved "is no longer with the FBI." The target was

prosecuted for unlawful disclosure of nuke information, but the Section 215 evidence was not introduced into trial and therefore he did not have an opportunity to challenge any illegal investigative methods.

- A 2009 application involving significant minimization concerns and for which FBI rolled out a "investigative value" exception for access limits on Section 215 databases. This also may involve FBI's secret definition of US person, which I suspect pertains to treating IP addresses as non-US persons until they know it is a US person (this is akin to what they do under 702 MPs). DOJ's minimization report to FISC included inaccuracies not fixed until June 13, 2013.
- A 2009 application for a preliminary investigation that obtained medical and education records from the target's employer. FBI ultimately determined the target "had no nexus to terrorism," though it appears FBI kept all information on the target

(meaning he will have records at FBI for 30 years). The FBI's minimization report included an error not fixed until June 13, 2013, after the IG pointed it out.
- A cyber-investigation for which the case agent could not locate the original production, which he claims was never placed in the case file.

And that's just what can be discerned from the unredacted bits.

Remember, too: the inaccuracies (as opposed to the material misstatement) were on minimization procedures. Which suggests FBI was either deceitful — or inattentive — to how it was complying with FISC-mandated minimization procedures designed to protect innocent Americans' privacy.

And remember — all this is *just* Section 215. The legal violations under PRTT were far more egregious, and there are other known violations and misstatements to FISC on other programs.

This is a troubling program, one that several judges have found either unconstitutional or illegal.