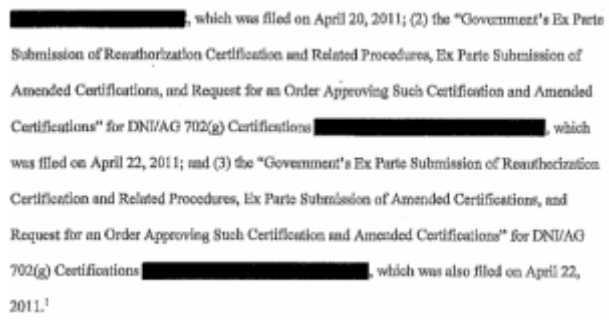
3 CERTIFICATIONS — TERROR, PROLIFERATION, AND CYBER — AND STEALING FROM GOOGLE

For months, I have been suggesting that


[redacted], which was filed on April 20, 2011; (2) the "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" for DNI/AG 702(g) Certifications [redacted], which was filed on April 22, 2011; and (3) the "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" for DNI/AG 702(g) Certifications [redacted], which was also filed on April 22, 2011.[1]

the government only uses Section 702 of FISA, under which it collects data directly from US Internet providers and conducts some upstream content from telecom providers, for three purposes:

- Counterterrorism
- Counterproliferation
- Cyber

I have said so based on two things: many points in documents — such as the second page from John Bates' October 3, 2011 opinion on 702, above — make it clear there are 3 sets of certifications for 702 collection. And other explainer documents released by the government talk about those three topics (though they always stop short of saying the government collects on only those 3 topics).

The NSA Review Group report released yesterday continues this pattern in perhaps more explicit form.

> [S]ection 702 authorized the FISC to approve annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that identify certain categories of foreign

> intelligence targets whose communications may be collected, subject to FISC-approved targeting and minimization procedures. The categories of targets specified by these certifications typically consist of, for example, international terrorists and individuals involved in the proliferation of weapons of mass destruction.

If I'm right, it explains one of the issues driving overseas collection and, almost certainly, rising tensions with the Internet companies.

I suggested, for example, that this might explain why NSA felt the need to steal data from Google's own fiber overseas.

> I wonder whether the types of targets they're pursuing have anything to do with this. For a variety of reasons, I've come to suspect NSA only uses Section 702 for three kinds of targets.
>
> - *Terrorists*
> - *Arms proliferators*
> - *Hackers and other cyber-attackers*
>
> According to the plain letter of Section 702 there shouldn't be this limitation; Section 702 should be available for any foreign intelligence purpose. But it's possible that some of the FISC rulings — perhaps even the 2007-8 one pertaining to Yahoo (which the government is in the process of declassifying as we speak) — rely on a special needs exception to the Fourth Amendment tied to these three types of threats (with the assumption being that other foreign intelligence targets don't infiltrate the US like these do).
>
> Which would make this passage one of the

> most revealing of the WaPo piece.
>
> > One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 “selectors,” or search terms. That is more than twice the number in use in the PRISM program, but even 100,000 cannot easily account for the millions of records that are said to be sent back to Fort Meade each day.
>
> Given that NSA is using twice as many selectors, it is likely the NSA is searching on content outside whatever parameters that FISC sets for it, perhaps on completely unrelated topics altogether. This may well be foreign intelligence, but it may not be content the FISC has deemed worthy of this kind of intrusive search.

That is, if NSA can only collect 3 topics domestically, but has other collection requirements it must fulfill — such as financial intelligence on whether the economy is going to crash, which FISC would have very good reasons not to approve as a special need for US collection — then they might collect it overseas (and in the Google case, they do it with the help of GCHQ). But as Google moved to encryption by default, NSA would have been forced to find new ways to collect it.

Which might explain why they found a way to steal data in motion (on Google’s cables, though).

Here’s the thing, though. As I’ll note in a piece coming out later today, the Review also emphasizes that EO 12333 should only be available for collection not covered by FISA. With Section 702, FISA covers all collection from US Internet providers. So FISC’s refusal to

approve (or DOJ's reluctance to ask for approval) to collect on other topics should foreclose that collection entirely. The government should not be able to collect some topics under 702 here, then steal on other topics overseas.

But it appears that's what it's doing.

All that said, the problem is one of NSA's own making, for other reasons. The reason FISC would need to use a special needs exception to the Fourth Amendment pertains to how 702 collection infringes on US persons' privacy. FISC would be nuts to say the government could conduct warrant-free collections of communications pertaining to (using my earlier example) financial discussions, because that'd be near the top of the list of things elites would object to collection on. So to get US collection of Internet data for other reasons, NSA would need to provide US persons more protection: no access to incidentally collected email, no back door searches.

As I'll show in more depth later, that's also what the Review Group recommends, providing this level of protection to US persons under 702 collection (and given how attentively the Review caters to the needs of the Internet companies, this dynamic may explain why).

> What the hell are you doing? Are you really hacking into the infrastructure of American companies overseas? The same American companies that cooperate with your lawful orders and spend a lot of money to comply with them to facilitate your intelligence collection?

… The tech companies reportedly complained to Obama when they met him the other day, before he decided to release the Review early.

This is the dilemma NSA (and Obama, as he reviews the report while in Hawaii) faces. The NSA has refused to provide US persons basic protections in its 702 collection, which

presumably is why FISC has limited its use to several specific topics. In response, NSA has broken the spirit of FISA by stealing from Google overseas, creating legal problems and a whole lot of pissed Internet CEOs.

For all it degrades our privacy elsewhere, on this issue Google (and Yahoo, which actually did fight this issue in real time and probably forced FISC to codify this special needs position) may well force the government to give us more of it.