DAVID MEDINE'S PCLOB DEFENSE

Today, David Medine attempts to answer (most) of the questions Jennifer Granick argues weren't answered in the Privacy and Civil Liberties Oversight Board's report on Section 702. Here's my summary of how he does so:

Granick	Medine
1: How many collected communications are US persons?	Agrees PCLOB didn't answer, agrees NSA should.
2: Do US agencies have direct access to providers' systems?	That's classified, though suggests there are interim steps in both types of 702 collection.
3: Can PRISM operate at greater degrees of assurance on foreignness?	Foreignness designations are rigorous.
4: What is national security value of targeting people who aren't agents of a foreign power	They have information about people who are.
5: What kind of selectors does NSA use in "about" collection?	That's classified, though they don't use names and it's not (what the intelligence community considers) bulk collection.
6: Are things like buddy lists minimized?	Yes, because even things that are not communications are treated as communications.
7: How many times and about how many different people has NSA disclosed information to other agencies?	"NSA's dissemination of intelligence reports based on Section 702 collection is substantial, and a 'significant number of such reports ... (albeit a small percentage of the total) ... include reference to U.S. persons.;" NSA unmasked 10,000 US identities last year.
7: What are the legal basis and guidelines for back door searches?	See page 55-59 of this brief in the Mohamed Mohamud case. Patricia Wald and I said they need more controls.

Even while Medine "challenges" Granick's assessment that her questions weren't answered, he admits "Professor Granick may not find that all of her questions have been fully answered."

And that's clear from my summary: for classification reasons, PCLOB didn't answer the questions about volume of US person communications collected (question 1) or the kinds of selectors used (question 5), and only hinted at an answer to whether NSA had direct access to providers' networks (question 2). As I've suggested, even with the 100 new pieces of data PCLOB got declassified, their subjection to obviously bogus government classification claims discredits their report.

The most useful response Medine provides Granick — though not for what it says about the underlying question — is to inform us that buddy lists and a bunch of other things are treated as

communications.

> 6. *"Do intelligence agencies minimize address books, buddy lists, stored documents, system backups and/or other electronic transmissions where there is no human being on the received end of the transmission as "communications" under the minimization procedures? Or are those fair game?"*
>
> The report answers this question directly: "Everything that is collected under Section 702 is treated as a 'communication' and therefore is protected by the applicable minimization procedures." PCLOB report at p. 127 n. 524. As explained elsewhere in the report, the statute itself "requires that *all* acquired data be subject to minimization procedures." PCLOB report at p. 50 (emphasis added).

In a sense, Granick's original question was overtaken by events when it was confirmed — both in the WaPo's analysis of 702 collected data and in PCLOB — that minimization doesn't work as mandated by law (though PCLOB seems relatively untroubled by that). Sure, US person names in an address book will be masked, but they won't be destroyed because they have no foreign intelligence value. So even US person names in buddy lists will be available for analysis.

But Medine's answer — emphasizing that "everything .. is treated as 'communication'" — is important for his answer regarding what the government uses for upstream selectors.

> More specifically, every selector used for upstream collection (as for PRISM collection) must be "a specific communications identifier." PCLOB report at p. 123.

In my opinion, Medine's entire response to Granick on this question is straw manning. She admits PCLOB made it clear key words and names cannot be used for upstream selectors, yet he spends a paragraph explaining that they are not.

> The requirement that selectors be specific communications identifiers also means that selectors cannot be key words or terms. Critically, this ensures that "the government's collection devices are not searching for references to particular topics or ideas, but only for references to specific communications selectors used by people who have been targeted under Section 702." PCLOB report at p. 123.

Granick never asked — not even in her original questions — about bulk collection under upstream 702, but Medine spends most of his answer addressing that, including this truly bizarre paragraph.

> Nonetheless, under the targeting procedures approved by the FISA court, tasking selectors in any way that could fairly be characterized as "bulk" collection is prohibited, in no small part because it would result in the targeting of U.S. persons or people in the United States, which is barred by the statute. The scope of collection under Section 702 is large because the number of targets is large — roughly

> 89,000 as of last year — not because the program operates on the "collect it all, then sort it later" model that characterizes the NSA's Section 215 telephone records program.

He's of course using the intelligence community definition of bulk, not the common English one, something which discredits his report. If upstream collection sucks in 56,000 US persons it shouldn't — as John Bates has estimated — that's a bulk collection program to most people, no matter what Medine and the IC call it.

But his use of IC jargon is not consistent. After all, the IC claims that the "bulk" collection of the phone dragnet results in very limited "targeting" of US persons, but Medine's language here treats subsequent searches of the bulk collected data as targeting. The concern from both 215 and 702, however, comes from the access of vast amounts of US person data, and the standards for 702 back door searches are far lower than they are for the "bulk" collection under 215.

But back to Medine's emphasis that everything is treated as a communication under Section 702.

As I've noted, PCLOB pretended that Section 702 doesn't have a cyber function, the clarification that everything — including "electronic transmissions where there is no human being on the received end of the transmission" constitutes a communication just provides a broader potential application they know they have for cybersecurity.

Then there's Granick's question Medine doesn't answer at all.

> For example, is the URL where Al Qaeda publishes Insight Magazine a communications facility? Many people, including American scholars, read that magazine. Can NSA collect web traffic (including metadata) to, from and about that magazine under section 702? We

> still don't know the answer to that question.

For what it's worth, I think they search on the encryption codes or email located in that section of every Inspire magazine, but whichever theory you use for upstream collection of Inspire access, Medine simply blows off the question entirely.

But by making it clear that stored documents like the Inspire PDF are treated as communications, then it's clear it would be the communication of a foreign power, AQAP, and therefore fair game as an identifier under upstream 702. Yet another reason to be fairly certain they do use upstream 702 to identify Americans who access the magazine.

Medine seems to intend to reassure us with his upstream discussion, but given that "communication" has been broadly defined, we should be even more concerned!

There's one more aspect of Medine's response that undermines his defense of PCLOB. Medine's defense of the rigor of NSA's foreignness designation implicitly attacks press reports on the process.

> Despite press accounts suggesting that the NSA's "foreignness" determinations are superficial, we found the process to be rigorous.

Yet nowhere — neither in his discussion of how much US person data is collected nor in his discussion of foreignness — does he mention the WaPo analysis that shows, using hard data and a long description of their methodology, why PCLOB is overly optimistic about foreignness designators and what the probable range of US person communication data really is.

That's a problem, just like claiming the targeting procedures haven't been published when they have. Every time PCLOB makes claims that

ignore significant and substantive parts of the public debate (and at the same time engage in some straw man arguments), they adopt the method of NSA and the government more generally. If Medine wants to defend his report, he needs to at least acknowledge that WaPo's substantive work — the kind of work PCLOB itself recommends be done — in some ways undermines it.

I don't mean to knock the report. It is valuable and adds a bunch new stuff even I didn't know, and for less involved readers it offers a great primer on the program.

But PCLOB's mission — and particularly its partial adoption of the government's Kafkaesque secrecy charade — undermine its claims to legitimacy, particularly when it sounds too much like the government.

PCLOB's report answered a lot of questions. But it didn't answer some it easily could have.