# THE INTELLIGENCE COMMUNITY'S WIDE OPEN, UNPROTECTED BACK DOOR TO ALL YOUR CONTENT

PCLOB has posted the transcript from the first part of its hearing on Monday. So I want to return to the issue I raised here: both Director of National Intelligence General Counsel Robert Litt and NSA General Counsel Raj De admit that there are almost no limits on Intelligence Community searches of incidentally collection US person data (we know that FBI, NSA, and CIA have this authority, and I suspect National Counterterrorism Center does as well).

This discussion starts when PCLOB Chair David Medine asks whether the IC would consider getting a warrant before searching on incidentally collected data.

> MR. MEDINE: And so turning to the protections for U.S. persons, as I understand it under the 702 program when you may target a non-U.S. person overseas you may capture communications where a U.S. person in the United States is on the other end of the communication. **Would you be open to a warrant requirement for searching that data when your focus is on the U.S. person** on the theory that they would be entitled to Fourth Amendment rights for the search of information about that U.S. person?
>
> MR. DE: Do you want me to take this?
>
> MR. LITT: Thanks, Raj. Raj is always easy, he raises his hands for all the easy ones.
>
> MR. DE: I can speak for NSA but

> this obviously has implications beyond just NSA as well.
>
> MR. LITT: I think that's really an unusual and extraordinary step to take with respect to information that has been lawfully required.
>
> I mean I started out as a prosecutor. There were all sorts of circumstances in which information is lawfully acquired that relates to persons who are not the subject of investigations. You can be overheard on a Title III wiretap, you can overheard on a Title I FISA wiretap. Somebody's computer can be seized and there may be information about you on it.
>
> **The general rule and premise has been that information that's lawfully acquired can be used by the government in the proper exercise of authorities**.
>
> Now we do have rules that limit our ability to collect, retain and disseminate information about U.S. persons. Those rules, as know, are fairly detailed. But generally speaking, we can't do that **except for foreign intelligence purposes, or when there's evidence of a crime, or so on and so forth**. But what we can't do under Section 702 is go out and affirmatively use the collection authority for the purpose of getting information about U.S. persons. Once we have that information I don't think it makes sense to say, you know, a year later if something comes up we need to go back and get a warrant to search that information. [my emphasis]

Litt compares finding incidental information on a laptop, presumably seized using a warrant, with searching for incidental information on a digital collection that includes very few limits

on specificity. Remember, NSA can and has claimed a targeted "facility" may mean all the Internet traffic from a particular country or at least a region of a country. This is petabytes of data obtained with a directive, not gigabytes obtained with a specific warrant.

Much later in the hearing, Center for Democracy and Technology VP James Dempsey followed up, asking whether NSA (and other agencies) even use the standard required before they can access the phone metadata database, Reasonable Articulable Suspicion (RAS).

> MR. DEMPSEY: A couple of questions on 702, and then also related 12333. On 702 collection of the content program, some of the communications that are acquired are communications persons reasonably believed to be overseas are to and from people in the United States. And it's my understanding that those are lawfully collected. It's not inadvertent, it's intentional and lawful. But then once that data is in it can be searched looking for communications of a U.S. person. So you have very low, sort of front-end protections, then am I right to say, or let me put it this way, what protections occur then on the search side?
>
> And I understand Bob's point that if it's lawfully collected the rule is you can search it and use it for a legitimate purpose. But **even with the 215 data you've imposed this RAS standard** and it's lawfully collected. Zero constitutional protection but you've nevertheless surrounded it with a lot of limitations. What are the limitations surrounding the incidentally but advertently collected U.S. person communications?
>
> MR. DE: So maybe I can start just with the initial premise that you

raised. So you're correct that we must target non-U.S. persons reasonably located to be abroad. But one important protection is that we can't willfully target a non-U.S. person in order to reverse target a U.S. person, which I know the panel is familiar with, but just so other folks are familiar with that.

Our minimization procedures, including how we handle data, whether that's collection, analysis, dissemination, querying are all approved by the Foreign Intelligence Surveillance Court. There are protections on the dissemination of information, whether as a result of a query or analysis. So in other words, U.S. person information can only be disseminated if it's either necessary to understand the foreign intelligence value of the information, **evidence of a crime and so forth**. So I think those are the types of protections that are in place with this lawfully collected data.

MR. DEMPSEY: But am I right, there's no, on the query itself, **other than it be for a foreign intelligence purpose, is there any other limitation? We don't even have a RAS for that data**.

MR. DE: **There's certainly no other program for which the RAS standard is applicable**. That's limited to the 215 program, that's correct. But as to whether there is, and I think this was getting to the probable cause standard,

should there be a higher standard for querying lawfully collected data. I think that would be a novel approach in this context, not to suggest reasonable people can't disagree, discuss that. But I'm not aware of another context in which there is lawfully collected, minimized information in this capacity

> in which you would need a particular standard.
>
> MR. DEMPSEY: Minimized here just means you're keeping it.
>
> MR. DE: I'm sorry?
>
> MR. DEMPSEY: Minimized here means *you're keeping it, doesn't it?*
>
> MR. DE: It means – there are minimization requirements, both in terms of how it's collected, how it's processed internally. I mean we can go into more detail in a classified setting. How it's analyzed and how it's disseminated. So the statute requires minimization to apply in every stage of the analytic process.

De hides behind minimization procedures – falsely implying that the data is minimized before they search on it. But Dempsey persists and asks again whether they require even the very low standard of RAS before conducting these back door searches. And De confirms, by admitting there are no other uses of RAS outside of the phone metadata program, that no, they don't even require RAS before searching for US person data via a back door search.

For five months, the IC has (misleadingly) been suggesting that content is far more revealing than metadata. But the standard they use to access huge databases including US person content is actually far lower than the one they use to access a huge database including US person metadata.

One more point: Dempsey inaccurately suggests the IC can only search on US person data for foreign intelligence purposes (which is unbelievably broad anyway, given how they've blown up the meaning of that term; and remember the IC can only search on the metadata dragnet for counterterrorism purposes).

Litt admits they can search on US person data

"when there's evidence of a crime, or so on and so forth." De admits they can search on US person data for "evidence of a crime and so forth."

And DiFi's bill — as well as the minimization procedures — make it clear that in addition to searching for foreign intelligence or evidence of a crime, some of those "so on and and so forths" include.

- Technical assurance, which surely includes both algorithm development and testing, but also (per the Section 702 minimization procedures) cracking encryption and assessing data security (AKA hunting for malware).
- Data that do not constitute evidence of a crime but show threats to life or of bodily harm, which we know the NSA has secretly translated to mean threats to property.

After having established that the back door for Section 702 collected data is open wide open, Dempsey then turns to data collected using EO 12333, data that doesn't involve any court order or oversight whatsoever.

> MR. DEMPSEY: Okay. Am I right, **the same situation basically applies to information collected outside of FISA**? So FISA collection inside the United States, 12333 collection outside the United States, but those communications collected outside the United States might include collections to or from U.S. citizens, U.S. persons, and again, those can then be searched without even a RAS type

> determination, is that right?
>
> MR. DE: **I think, yeah**, I don't know if we've declassified sort of minimization procedures outside of the FISA context, but there are different rules that apply. [my emphasis]

De offers the same non-answer, pointing to the much weaker minimization procedures for EO 12333 data than exist for Section 702 data.

Remember: we've seen that NSA is collecting contact lists (including content) and stealing data as it moves around Google and Yahoo's data centers overseas — all data that includes some amount of US person that the NSA refuses to count. And these collections not only include upstream collection targeting whole countries or regions, but also the foreign servers of US based companies we all use to communicate.

And according to the DNI and NSA's own lawyers, there are almost no requirements imposed before an analyst can search that data, and there are broad categories under which analysts can distribute such data.