# IN SPYING, "THINGS LIKE PHONE NUMBERS OR EMAILS" TURN OUT TO BE FAR MORE

According to Reuters, the Intelligence Community doesn't intend to share any details of the Yahoo scan revealed several weeks back with anyone outside of the FISA oversight committees — the House and Senate Intelligence and Judiciary Committees.

> Executive branch officials spoke to staff for members of the Senate and House of Representatives committees overseeing intelligence operations and the judiciary, according to people briefed on the events, which followed Reuters' disclosure of the massive search.
>
> But attempts by other members of Congress and civil society groups to learn more about the Yahoo order are unlikely to meet with success anytime soon, because its details remain a sensitive national security matter, U.S. officials told Reuters. Release of any declassified version of the order is unlikely in the foreseeable future, the officials said.

On its face, it's a stupid stance, as I think the scan probably fits within existing legal precedents that have already been made public, even if it stretches those precedents from "packet content as content" to "email content as content" (and it may not even do that).

In addition, given that the scan was approved by a judge (albeit one working within the secret FISA court and relying on prior decisions that were issued in secrecy), by releasing more details about the scan the government could at

least claim that a judge had determined the scan was necessary and proportionate to obtain details about the (as described to NYT) state-sponsored terrorist group targeted by the scan. This decision presumably relies on a long line of decisions finding warrantless surveillance justified by special needs precedents, which began to be laid out for FISC in In Re Sealed Case in 2002.

Nevertheless, even given the toll the government's secrecy is having on Yahoo (and presumably on other providers' willingness to cooperate with the IC), the government thus far has remained intransigent in its secrecy.

Which suggests that the IC believes it would risk more by releasing more data than by its continued, damaging silence.

I've already explained one of the risks they might face: that their quick anonymous description of this as a "state-sponsored terrorist group" might (this is admittedly a wildarsed guess) really mean they hacked all of Yahoo's users to get to Iranian targets, something that wouldn't have the same scare power as terrorists like ISIS, especially in Europe, which has a markedly different relationship with Iran than the US has.

But I also think ODNI risks losing credibility because it appears to conflict with what ODNI specifically and other spook officials generally have said in the past, both to the US public and to the international community. As I note here, the definition of "facility" has been evolving at FISC since at least 2004. But the privacy community just released a letter and a quote to Reuters that seems unaware of the change. The letter asserts,

> According to reports, the order was issued under Title I of FISA, which requires the government to demonstrate probable cause that its target is a foreign power or an agent of a foreign power (such as a spy or a terrorist),

> and probable cause that the "facility" at which the surveillance is conducted will carry the target's communications. If reports are true, this authority to conduct a particularized search has apparently been secretly construed to authorize a mass scan.

Traditional FISA orders haven't been limited to particularized targets since 2007, when an order targeting Al Qaeda was used to temporarily give Stellar Wind legal sanction. If one order requiring a scan of traffic at  telecom switches could target Al Qaeda in 2007, then surely one order can target Iran's Revolutionary Guard or a similar organization in 2016. The problem is in the execution of the order, requiring Yahoo to scan all its incoming email, but it's not clear the legal issues are much worse than in the 2007 execution.

A Reuters source goes even further, suggesting that all of Yahoo is the facility, rather than the specific code tied to the targeted group.

> The groups say that Title I of the Foreign Intelligence Surveillance Act, under which sources said the order was issued, requires a finding that the target of such a wiretap is probably an agent of a foreign power and that the facility to be tapped is probably going to be used for a transmission. An entire service, such as Yahoo, has never publicly been considered to be a "facility" in such a case: instead, the word usually refers to a phone number or an email account.

Never mind that under the phone dragnet, Verizon was counted as the targeted selector (which was used by terrorists and everyone else), though admittedly that was just for metadata. Had Yahoo been designed the "place" at which a physical search were conducted this usage might be correct (that said, we know very little about

how physical searches, including for stored communication, work in practice), but as Semiannual reports have made clear (admittedly in the Section 702 context), facility has come to be synonymous with selector.

> [T]argeting is effectuated by tasking communication facilities (also referred to as "selectors"), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers.

Facilities are selectors, and here FBI got a selector tied to a kind of usage of email — perhaps an encryption signature — approved as a selector/facility.

In spite of the fact that somewhere among 30 NGOs someone should have been able to make this argument (and ACLU's litigation side surely could do so), there is good reason for them to believe this.

That's because the IC has very deliberately avoided talking about how what are called "about" scans but really should be termed signature scans really work.

This is most striking in a March 19, 2014 Privacy and Civil Liberties Oversight Board hearing, which was one of the most extensive discussions of how Section 702 work. Shortly after this hearing, I contacted PCLOB to ask whether they were being fully briefed, including on the non-counterterrorism uses of 702, such as cyber, which use (or used) upstream selectors in a  different way.

Several different times in the hearing, IC witnesses described selectors as "selectors such as telephone numbers or email addresses" or "like telephone numbers or email addresses," obscuring the full extent of what might be included (Snowden tweeted a list that I included here). Bob Litt did so while insisting that Section 702 (he was referring both to PRISM and

upstream here) was not a bulk collection program:

> I want to make a couple of important overview points about Section 702. First, there is either a misconception or a mischaracterization commonly repeated that Section 702 is a form of bulk collection. It is not bulk collection. It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose.
>
> I just want to repeat that Section 702 is not a bulk collection program.

Then-Deputy Assistant Attorney General Brad Weigmann said selectors were "really phone numbers, email addresses, things like that" when he defined selector.

> A selector would typically be an email account or a phone number that you are targeting. So this is the, you get, you know, terrorists at Google.com, you know, whatever. That's the address that you have information about that if you have reason to believe that that person is a terrorist and you would like to collect foreign intelligence information, I might be focusing on that person's account.
>
> [snip]
>
> So that's when we say selector it's really an arcane term that people wouldn't understand, but it's really phone numbers, email addresses, things like that.

And when then-NSA General Counsel Raj De moved from describing Section 702 generally ("selectors are things like"), to discussing

upstream, he mistakenly said collection was based on "particularly phone numbers or emails" then immediately corrected himself to say, "things like phone numbers or emails."

> So there's two types of collection under Section 702. Both are targeted, as Bob was saying, which means they are both selector-based, and I'll get into some more detail about what that means. Selectors are things like phone numbers and email addresses.
>
> [snip]
>
> It is also however selector-based, i.e. based on particular phone numbers or emails, things like phone numbers or emails. This is collection to, from, or about selectors, the same selectors that are used in PRISM selection. This is not collection based on key words, for example.

That language would — and apparently did — create the false impression that about collection really did just use emails and phone numbers (which is why I called PCLOB, because I knew they were or had also targeted cyber signatures).

Here's how all that evasiveness appeared in the PCLOB 702 report:

> Although we cannot discuss the details in an unclassified public report, the moniker "about" collection describes a number of distinct scenarios, which the government has in the past characterized as different "categories" of "about" collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked

> selector but nevertheless are collected because they contain the selector somewhere within them.

That certainly goes beyond the linguistic game the IC witnesses were playing, but stops well short of explaining that this really isn't all about emails and phone numbers.

Plus, there's one exchange from that March 2014 hearing that might be taken to rule out about collection from a PRISM provider. In reply to specific prodding from Elisabeth Collins Cook, De said about collection cannot be made via PRISM.

> MS. COLLINS COOK: I wanted to ask one additional question about abouts. Can you do about collection through PRISM?
>
> MR. DE: No.
>
> MS. COLLINS COOK: So it is limited to upstream collection?
>
> MR. DE: Correct. PRISM is only collection to or from selectors.

Of course, De was referring to warrantless collection under Section 702. He wasn't talking at all about what is possible under Title I. But it may have left the impression that one couldn't order a PRISM provider to do an about scan, even though in 2007 FISA ordered telecoms to do about scans.

Ultimately, though, the IC is likely remaining mum about these details because revealing it would make clear what publicly released opinions do, but not in real detail: that these about scans have gotten far beyond a collection of content based off a scan of readily available metadata. These scans likely replicate the problem identified in 2004, in that the initial scan is not of things that count as metadata to the provider doing the scan.

The IC may have FISC approval for that argument. But they also had FISC approval for the Section 215 dragnet. And that didn’t live up to public scrutiny either.