

DID ANTHONY COPPOLINO FIB ABOUT NSA'S NEW ARCHITECTURE?

On Tuesday, EFF told the tale of yet another government freak-out over purportedly classified information. The DOJ lawyer litigating their multiple dragnet challenges, Anthony Coppolino, accidentally uttered classified information in a hearing in June. So the government tried to take the classified information out of the transcript without admitting they did so. After Judge Jeffrey White let EFF have a say about all this, the government ultimately decided the information wasn't classified after all. So the Court finally released the transcript.

My wildarseguess is that this is the passage in question:

Judge Bates never ultimately held that the acquisition violated the Constitution. The problem in that case was the minimization procedures were not sufficient to protect the Fourth Amendment interests of the people of the United States.

And so he ordered that they be changed, and they were changed. And he approved them. And in addition, in the process of not only approving the minimization procedures, *NSA implemented new system architecture that did a better job at assuring that those communications were minimized and ultimately destroyed*, which is the goal here. It's part of the statutory framework not to collect on U.S. citizens and when you've incidentally done it, destroy it. [my emphasis]

According to the John Bates opinions relating to

this incident, the NSA implemented a new system of ingesting this data, marking it, checking it before it gets moved into the general repository of data, and purging it if it includes entirely domestic communications. But does that count as new architecture? I'm not sure.

Meanwhile, the NSA has been upgrading their architecture. We learned that (among other places) in the most recent Theresa Shea declaration on NSA systems in EFF's Jewel case. It doesn't mention new architecture pertaining to upstream 702, though she does discuss a more general architecture upgrade and how it affects Section 215 specifically.

Then there's this language, addressing the NSA's inability to filter US person data reliably, from PCL0B.

The NSA's acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector."¹⁵⁵ While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided.¹⁵⁶ If time were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that

filter would be out-of-date as soon as time was restarted and a protocol changed, a new service or function was offered, or a user changed his or her settings to interact with the Internet in a different way. Conducting upstream Internet acquisition will therefore continue to result in the acquisition of some communications that are unrelated to the intended targets.

The fact that the NSA acquires Internet communications through the acquisition of Internet transactions, be they SCTs or MCTs, has implications for the technical measures, such as IP filters, that the NSA employs to prevent the intentional acquisition of wholly domestic communications. With respect to SCTs, wholly domestic communications that are routed via a foreign server for any reason are susceptible to Section 702 acquisition if the SCT contains a Section 702 tasked selector.¹⁵⁷ With respect to MCTs, wholly domestic communications also may be embedded within Internet transactions that also contain foreign communications with a Section 702 target. The NSA's technical means for filtering domestic communications cannot currently discover and prevent the acquisition of such MCTs.¹⁵⁸

The footnotes in this section all cite to John Bates' 2011 opinion (including, probably, some language that remains redacted in the public copy, such as on page 47). So we might presume it is out of date. Except that PCLOB has done independent work on these issues and the end of the first paragraph includes language not sourced at all.

That is, PCLOB seems to think there remain technical problems with sorting out US person data, the filtering problem cannot be solved. (Which makes the ridiculous John Bates more

skeptical on this point than PCLOB.)

So do the data segregation techniques implemented in 2011 amount to new architecture? Does the larger architecture upgrade going on going to affect upstream collection in some more meaningful fashion?

I don't know. One other reason I think this might be the language is because Coppelino was – as he frequently does – running his mouth. Bates did rule the US person data collected before 2011 violated the Fourth Amendment, even if the task before him was solely to judge whether the minimization procedures before him did. More importantly, Bates was quite clear that this US person collection was intentional, not incidental.

So Coppelino was making claims about one of the practices (the PRTT collection is another) that is most likely to help EFF win their suit, upstream collection, which actually does entail domestic wiretapping of US person content. He made a claim that suggested – with the fancy word “architecture” – that NSA had made technical fixes. But PCLOB, at least, doesn't believe they've gotten to the real issue.

Who knows? It's just a guess. What's not a guess is that Coppelino seems to recognize upstream 702 presents a real problem in this suit.