THE UPSTREAM "ABOUT" PROBLEM PROBABLY PERTAINS TO SCTS, NOT MCTS

Much of the reporting on the reason NSA is shutting down Section 702 authorized upstream "about" collection has assumed the problem pertains to multiple communication transactions, which is when emails get sent in batches, which can include targeted emails (meaning they include a selector tied to an approved foreign target) as well as untargeted, completely domestic ones. But we know that upstream collection also collects single communication transactions that constituted entirely domestic communications, which would happen if an email from one American to another included the selector (and remember, the selector can be things beyond email and phone numbers; it might include things like encryption keys or dark web forum addresses). Collection of a completely domestic SCT would happen for different technical reasons than an MCT: it would happen whenever an Internet communication between two Americans transited overseas and got caught in filters purportedly focused exclusively on international traffic. Here's how John Bates described SCTs in his October 3, 2011 opinion on the upstream problems.

> In addition to these MCTs, NSA likely acquires tends of thousands more wholly domestic communications every year, given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.

And I think the problem at issue probably pertains to the SCTs, not to MCTs.

The NSA statement on the issue says nothing that

would suggest this is a problem with MCTs. Indeed, its example of an "about" collection is an SCT — an email that itself contains the designated selector.

> An example of an "about" email communication is one that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets. The independent Privacy and Civil Liberties Oversight Board described these collection methods in an exhaustive report published in 2014.

More tellingly, Ron Wyden's statement about the risk of the practice also describes an SCT — an American's email that got collected because she mentioned the targeted selector.

> "This change ends a practice that could result in Americans' communications being collected without a warrant merely for mentioning a foreign target,"

The government hasn't liked to talk much about SCTs. It appears to have made no mention of them in the notice to Congress of upstream problems leading up to reauthorization in 2012. And when Bates asked NSA to count SCTs as part of upstream discussions in 2011, it basically refused to do so. Bates came up with his own estimate of 46,000 communications a year (which represented the majority of the domestic communications collected via upstream surveillance). Ron Wyden has been pushing for a real estimate since literally the same period Bates was making his own up.

But basically, the government has been permitted to collect entirely domestic communications of Americans using targeted selectors since 2007, even as Internet usage means more and more completely domestic communications will transit overseas.

And SCTs are the ones most likely to show up in a query of a US person communication.

That's because, when Bates was trying to sort through these issues in 2011, he viewed SCTs differently than he did MCTs, figuring that an SCT might itself have foreign intelligence value, whereas a completely unrelated email would not.

> NSA's upstream collection also likely results in the acquisition of tens of thousands of wholly SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [redacted] Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications that are neither to, from, nor about targeted selectors, to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition

> of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition.

Accordingly, most of the special minimization procedures pertaining to upstream collection — most importantly, that it be segregated in a special database — don't apply to SCTs.

Importantly, that destroy upon recognition is not absolute: if an analyst sees it and determines a communication has Foreign Intelligence value or is evidence of a crime (or two other things), then it can be retained, with DIRNSA approval. Of course, some kinds of selectors — such as certain dark web addresses and encryption keys — might by themselves be evidence of a crime, meaning a back door search could (hypothetically at least) lead directly to an American being implicated via 702 collection.

There are just two special limits that would protect these completely domestic SCTs: a two year — rather than five year — aging off process. And the rule that appears to have gotten broken: NSA can't do queries on US persons (that is, back door searches) on upstream collection.

> Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques.

That's the importance of this post — describing violations involving the use of US person selectors to search upstream communications. It

shows how it was possible, in 2013 and 2014, for analysts to "inadvertently" do back door searches on upstream collection. Those violations almost certainly occurred with SCTs, not MCTs, because SCTs would be the ones in general repositories that analysts who weren't specially trained would access.

We can see in those past violations how a US person search on upstream content might happen. In 2013, analysts would avoid searching on upstream data by formally excluding it as part of their search term (maybe by adding "NOT upstream" to their query). But on "many" occasions, analysts forget to exclude "upstream" in their back door searches on US person identifiers (and none of the unredacted discussion seems to have suggested requiring them to find a better approach to prevent searches on upstream data). Then, in 2014, ODNI and DOJ seemed to think that analysts were doing searches on identifiers they didn't know were US person identifiers and as a result doing US person searches on upstream data because they hadn't thought about excluding it (and, in fact, the wording of the minimization procedures permit searches using selectors that are not yet identifiable as US person selectors).

We'll find out soon enough what the current inadvertent method of searching upstream collected data using US person selectors is. But the point is, under the minimization procedures, MCTs would be segregated from general repositories but SCTs would not be, and so the mistakes are going to be easier to make (and the volume of entirely domestic communications will be greater) with SCTs. To fix the SCT problem you'd either have to move *all* upstream about content out of general repositories, find a better way to avoid collecting domestic communications that transited internationally, stop doing back door searches, or stop collecting on about. They're choosing the latter option. (Note, if this were an MCT problem, then you could just delete all about MCTs on intake.)

Here's the rub though. If the problem with upstream collection arises because so many entirely domestic US person communications now transit internationally, then shutting down upstream collection will not offer much further protection for US persons, because SCTs are — by definition! — communications that the NSA claims were transiting internationally, and so would be readily available under EO 12333 collection. And EO 12333 collection is now easier to share under Obama's EO 12333 sharing guidelines that were passed even as the debate about what to do about upstream collection was taking place. Those guidelines do prohibit the agencies from using "a query, identifier, or other selection term that is intended to select domestic communications," but if NSA couldn't prevent that with the heightened scrutiny that happens under FISA, how are they going to prevent it under EO 12333 analysis?

Now, to be fair, to do a content query of EO 12333 data, you'd need to get Attorney General (Jeff Sessions!) authorization or the head of the agency, the latter of which may be used for two entirely redacted reasons.

Still, if I'm right and the problem is SCTs, then ending upstream collection under Section 702 simply shifts the privacy problems under a new shell.