NSA SHOULD HAVE ADDRESSED ITS UPSTREAM PROBLEM IN 2013

I Con the Record has released a slew of documents pertaining to last year's problem with upstream searches, including the opinion ultimately approving new certifications. I'm doing a working thread and suspect I will have concerns about FISC oversight that I haven't had on past such reviews.

But for now, I'm aghast at this paragraph and accompanying footnote, describing how NSA's office of compliance and IG were trying to get a grasp on the problems.

> In anticipation of the January 31 deadline, the government updated the Court on these querying issues in the January 3, 2017 Notice. That Notice indicated that the IG's follow-on study (covering the first quarter of 2016) was still ongoing. A separate OCO review, limited in many of the same ways as the IG studies, and covering the periods of April through December 2015 and April through July of 2016, found that some redacted] [improper queries were conducted by [redacted] analysts during those periods.21 The January 3, 2017 Notice stated that "human error was the primary factor" in these incidents, but also suggested that system design issues contributed. *For example, some systems that are used to query multiple datasets simultaneously required analysts to "opt-out" of querying Section 702 upstream Internet data rather than requiring an affirmative "opt-in," which, in the Court's view, would have been more conducive to compliance*. See January 3, 2017 Notice at 5-6. It also

> appeared that NSA had not yet fully assessed the scope of the problem: the IG and OCO reviews "did not include systems through which queries are conducted of upstream data but that do not interface with NSA's query audit system." Id. at 3 n.6. Although NSD and ODNI undertook to work with NSA to identify other tools and systems in which NSA analysts were able to query upstream data, id., and the government proposed training and technical measures, it was clear to the Court that the issue was not yet fully scoped out.
>
> 21 NSA further reported that OCO reviewed queries involving a number of identifiers for known U.S. persons who were not targets under Sections 704 or 705(b) of the Act, and which were associated with "certain terrorism-related events that had occurred in the United States." January 3, 2017 Notice at 6. NSA OCO found [redacted] such queries, [redacted] of which improperly ran against Section 702 upstream Internet data. [redacted] of the improper queries were run in a system called [redacted] which NSA analysts use to of a current or prospective target of NSA collection, including under Section 702. Id. at 6-7. [my emphasis]

This passage seems to reveal several things: that NSA was querying upstream content before identifying whether something could be used as a target (which I suspect means it involved a triage process). It reveals that *not all queries are being audited!!!!*

And it also reveals that one reason NSA analysts were collecting upstream data is because over three years after DOJ and ODNI had figured out analysts were breaking the rules because they forgot to exclude upstream from their search, they were still doing so. Overseers noted this back in 2013!

> NSA [redacted] incidents of non-compliance with this subsection of its minimization procedures, many of which involved analysts inadvertently searching upstream collection. For example, [redacted], the NSA analyst conducted approved querying with United States persons identifiers ([long redaction]), but inadvertently forgot to exclude Section 702-acquired upstream data from his query.

This problem should have been fixed in the first full period when they were doing upstream searches. But for some reason … NSA never did.

Update: This language seems to say that this problem existed for the entire time they were conducting upstream in the 2011 fashion.

> In May and June 2016, NSA reported to oversight personnel in the ODNI and DOJ that, since approximately 2012, use of to query communications in had resulted in inadvertent violations of the above-described querying rules for Section 702 information. Id. The violations resulted from analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate queries to exclude such datasets. Id. at 1-2.