NSA HAS A DATABASE PROBLEM

Back in 2009 when the government released what we now know is a FISA Court of Review decision ordering Yahoo to cooperate in PRISM, I questioned a passage of the decision that relied on the government's claim that it doesn't keep a database of incidentally collected conversations involving US persons.

> In this post, I just want to point to a passage that deserves more scrutiny:
>
> > The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.(26)
>
> To translate, if the government collects information from a US citizen (here or abroad), a legal permanent US resident, a predominantly US organization, or a US corporation in the course of collecting information on someone it is specifically targeting, it it claims it does not keep that in a database (I'll come back and parse this in a second). In other words, if the government has a tap on your local falafel joint because suspected terrorists live off their falafels, and you happen to call in a take out order, it does not that have in a database.
>
> There are reasons to doubt this claim.

In the rest of the post, I showed how a response

from Michaels Mukasey and McConnell to Russ Feingold's efforts to protect US person incidental collection during the FISA Amendments Act had made it clear having access to this incidentally collected data was part of the point, meaning the government's reassurances to the FISCR must have been delicate dodges in one way or another. (Feingold's Amendments would have prevented 3 years of Fourth Amendment violative collection, by the way.)

> Did the court ask only about a database consisting entirely of incidentally collected information? Did they ask whether the government keeps incidentally collected information in its existing databases (that is, it doesn't have a database devoted solely to incidental data, but neither does it pull the incidental data out of its existing database)? Or, as bmaz reminds me below but that I originally omitted, is the government having one or more contractors maintain such a database? Or is the government, rather, using an expansive definition of targeting, suggesting that anyone who buys falafels from the same place that suspected terrorist does then, in turn, becomes targeted?
>
> McConnell and Mukasey's objections to Feingold's amendments make sense only in a situation in which all this information gets dumped into a database that is exposed to data mining. So it's hard to resolve their objections with this claim—as described by the FISA Appeals Court.

Which is part of the reason I'm so intrigued by this passage of John Bates' October 3, 2011 decision ruling some of NSA's collection and retention practices violated the Fourth Amendment. In a footnote amending a passage explaining why the retention of entirely US person communications with the permissive

minimization procedures the government had proposed is a problem, Bates points back to that earlier comment.

> The Court of Review plaining limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 ("On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment." (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA's upstream collection of Internet transactions. Accordingly, the Court of Review had occasion to consider NSA's acquisition of MCTs (or even "about" communications, for that matter). Furthermore, the Court of Review noted that "[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary." Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

Ultimately, Bates' approval for the government to query on US person identifiers on existing incidentally collected Section 702 material (see pages 22-23) show that he hasn't really thought through what happens to US person incidental collection; he actually has a shocking (arguably mis-) understanding of how permissive the existing minimization rules are, and therefore how invasive his authorization for searching on incidentally collected information will actually be.

But his complaint with the proposed minimization procedures shows what he believes they should be.

> The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target.

As Bates tells it, so long as he's paying close attention to an issue, the government should ideally **destroy** any US person data it collects that is not relevant to the authorized purpose of the acquisition. (His suggestion to segregate it actually endorses Russ Feingold's fix from 2008.)

But the minimization rules clearly allow the government to keep such data (after this opinion, they made an exception only for the multiple communication transactions in question, but not even for the other search identifiers involving entirely domestic communication so long as that's the only communication in the packet).

All the government has to do, for the vast majority of the data it collects, is say it might have a foreign intelligence or crime or encryption or technical data or threat to property purpose, and it keeps it for 5 years.

In a database.

Back when the FISCR used this language, it allowed the government the dodge that, so long as it didn't have a database dedicated to solely US person communications incidentally, it was all good. But the language Bates used should make all the US person information sitting in databases for 5 year periods (which Bates seems

not to understand) problematic.

Not least, the phone dragnet database, which — after all — includes the records of 310 million people even while only 12 people's data has proved useful in thwarting terrorist plots.

Update: Fixed the last sentence to describe what the Section 215 dragnet has yielded so far.