DIANNE FEINSTEIN OPENS THE TECH BACK DOOR TO THE DRAGNET DATABASE EVEN WIDER

I've been writing for months about the great big loophole providing access to the phone dragnet database.

Basically, the NSA needs someone to massage the dragnet data before analysts do queries on it, to take out high frequency call numbers (telemarketers and pizza joints), and probably to take out certain protected numbers, like those of Members of Congress. (Note, that the NSA has to do this demonstrates not only that all their haystack claims are false, but also leaves the possibility they'll remove numbers that actually do have intelligence value.)

The problem of course, is that this means there is routine access to the database of all phone-based relationships in the United States that does not undergo normal oversight. We know this is a problem because we know NSA has found big chunks of this data in places where it doesn't belong, as it discovered on February 16, 2012 when it found over 3,000 call records that had been stashed and kept longer than the 5 years permitted by the FISA Court.

> As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed

> background analysis to document why certain contact chaining rules were created. In addition to the BR work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata.

The bill the Intelligence Committee passed out of committee yesterday not only codifies this practice, but exempts this practice from the explicit limits placed on other uses of this database.

Here's how it describes this access.

> (D) LIMITED ACCESS TO DATA.—Access to information retained in accordance with the procedures described in subparagraph (C) shall be prohibited, except for access—
>
> [snip]
>
> (iii) as may be necessary for technical assurance, data management or compliance purposes, or for the purpose of narrowing the results of queries, in which case no information produced pursuant to the order may be accessed, used, or disclosed for any other purpose, unless the information is

> responsive to a query authorized under paragraph (3).

Note, I've never seen this access described in a way that would include "narrowing the results of queries" before. I'm actually very curious why a tech would need to directly access the database, presumably after a query has already been run, to narrow it. Isn't that contrary to the entire haystack theory?

In any case, the rest of the bill relevant to the phone dragnet effectively exempts this access from almost all of the oversight it codifies.

The requirement for a written record of the Reasonable Articulable Suspicion and identity of the person making the query does not apply (see 2 A and B). Since no record is made, the FISA Court doesn't review these queries (6A) and these queries don't get included in the public reporting (b)(3)(C)(i). I don't see where the bill requires **any** record-keeping of this access.

The requirement that the data be kept secure specifically doesn't apply.

> SECURITY PROCEDURES FOR ACQUIRED DATA.—Information acquired pursuant to such an order **(other than information properly returned in response to a query under subparagraph (D)(iii))** shall be retained by the Government in accordance with security procedures approved by the court in a manner designed to ensure that only authorized personnel will have access to the information in the manner prescribed by this section and the court's order. [my emphasis]

And the requirement that personnel accessing the database for these purposes (4) be limited and specially trained doesn't apply.

> A court order issued pursuant to an application made under subsection (a),

> and subject to the requirements of this subsection, shall impose strict, reasonable limits, consistent with operational needs, on the number of Government personnel authorized to make a determination or perform a query pursuant to paragraph (1)(D)(i).

The only limit that appears to apply to the queries from this data management access of the database is the 5 year destruction.

Now, I think the FISA Court made tentative bids to limit some of the activities in 2009. But this language seems to undermine some of the controls the Court has placed on this access (including audits).

In short, in a purported bid to raise confidence about the NSA creating a database of every phone-based relationship in the United States, the Intelligence Committee has actually codified a loosening of access to the database outside the central purpose of it. It permits a range of people to access the database for vaguely defined purposes, it permits them to move that data onto less secure areas of the network, and it doesn't appear to require record-keeping of the practice.

But what could go wrong with permitting tech personnel — people like Edward Snowden — access to data with less oversight than that imposed on analysts?

Update: Added the language from the 2012 violation to show how clueless the NSA was about finding this data just lying around and its inability to determine where it came from.