“COLLECTIONS SITES” AND THE THOMAS DRAKE CASE

I wanted to look at the the three documents that the government is withdrawing in whole or in part in the Thomas Drake case. Ellen Nakashima implies that three of the documents are three of the five charged documents.

> According to people following the case, the government may have to drop two Espionage Act counts that relate to information that Drake submitted to the Defense Department inspector general between 2002 and 2004 to buttress colleagues’ complaints about waste, fraud and abuse of a bungled NSA data-sifting program, Trailblazer. He and his former NSA colleagues thought the complaints were confidential.
>
> The evidence for those two counts is contained in Exhibits 42 and 43, according to the sources. Prosecutor William M. Welch II, in a letter Sunday to Bennett, a U.S. District Court judge in Baltimore, said those exhibits will be withdrawn. The letter was first reported by Politico.
>
> Another exhibit, numbered 41, also consisting of information Drake submitted to the inspector general, is intended to support a third Espionage Act count that may also be dropped, the sources said. That exhibit will be redacted, the prosecution has said.

In filings, Drake’s lawyers make it clear that Counts 1 and 2 relate to emails Drake kept; Counts 3, 4, and 5 relate to documents he had in boxes in his basement in connection with the DOD Inspector General complaint.

> To negate evidence that Mr. Drake "willfully retained" the documents in Counts 3-5, and to show that any misstatements resulted from confusion, mistake, or faulty memory, the defense intends to present evidence of the sheer volume of documents that Mr. Drake possessed and shared with the DOD-IG. The volume of the documents will provide a contrast with the slight number of DOD-IG related documents recovered from the basement and, thus, will evidence the likelihood of negligence, inadvertence, mistake, or carelessness.

In other words, the documents in Counts 3, 4, and 5 appear to be the documents the government has chosen to withdraw rather than provide adequate substitutions for. Those documents are described as:

- A four-page document "bearing the features of an email" titled "Volume is our Friend"
- A three-page document "bearing the features of an email" titled "Trial and Testing"
- A five-page document "bearing the features of an email" titled "the Collections Sites"

Note, while there's no way to guarantee that the government has maintained the same chronology in numbering Counts as it has Exhibits, it is withdrawing Exhibits 42 and 43, while it is just redacting all mention to the technology in question in Exhibit 41, suggesting that if the order was maintained, it'd be the "Trial and Testing" and "Collections Sites" documents the government had withdrawn completely.

But in any case, it appears that the emails in question deal with the volume of telecommunications data collected, the trial and testing of the system (remember that the key IG complaint was that Michael Hayden had selected Trailblazer over ThinThread in spite of the fact that the latter did better in testing), and places where telecommunications data were collected.

With that in mind, take a look at the following passages of the key Siobhan Gorman story in question:

> ThinThread would have:
>
> * Used more sophisticated methods of sorting through massive phone and e-mail data to identify suspect communications.
>
> [snip]
>
> A number of independent studies, including a classified 2004 report from the Pentagon’s inspector-general, in addition to the successful pilot tests, found that the program provided “superior processing, filtering and protection of U.S. citizens, and discovery of important and previously unknown targets,” said an intelligence official familiar with the program who described the reports to The Sun. The Pentagon report concluded that ThinThread’s ability to sort through data in 2001 was far superior to that of another NSA system in place in 2004, and that the program should be launched and enhanced.
>
> [snip]
>
> With the explosion of digital communications, especially phone calls over the Internet and the use of devices such as BlackBerries, the NSA was struggling to sort key nuggets of information from the huge volume of data it took in.

> By 1999, as some NSA officials grew increasingly concerned about millennium-related security, ThinThread seemed in position to become an important tool with which the NSA could prevent terrorist attacks. But it was never launched. Neither was it put into effect after the attacks in 2001. Despite its success in tests, ThinThread's information-sorting system was viewed by some in the agency as a competitor to Trailblazer, a $1.2 billion program that was being developed with similar goals. The NSA was committed to Trailblazer, which later ran into trouble and has been essentially abandoned.
>
> Both programs aimed to better sort through the sea of data to find key tips to the next terrorist attack, but Trailblazer had more political support internally because it was initiated by Hayden when he first arrived at the NSA, sources said.
>
> NSA managers did not want to adopt the data-sifting component of ThinThread out of fear that the Trailblazer program would be outperformed and "humiliated," an intelligence official said.
>
> Without ThinThread's data-sifting assets, the warrantless surveillance program was left with a sub-par tool for sniffing out information, and that has diminished the quality of its analysis, according to intelligence officials.
>
> Sources say the the NSA's existing system for data-sorting has produced a database clogged with corrupted and useless information.
>
> The mass collection of relatively unsorted data, combined with system flaws that sources say erroneously flag people as suspect, has produced numerous false leads, draining analyst resources,

> according to two intelligence officials. FBI agents have complained in published reports in The New York Times that NSA leads have resulted in numerous dead ends. [my emphasis]

In other words, one of the key differences between ThinThread and Trailblazer was in the data-sorting technique used.

Jane Mayer's piece on Drake reveals some details about why ThinThread was better at sorting.

> As [ThinThread's inventor Bill] Binney imagined it, ThinThread would correlate data from financial transactions, travel records, Web searches, G.P.S. equipment, and any other "attributes" that an analyst might find useful in pinpointing "the bad guys." By 2000, Binney, using fibre optics, had set up a computer network that could chart relationships among people in real time. It also turned the N.S.A.'s data-collection paradigm upside down. Instead of vacuuming up information around the world and then sending it all back to headquarters for analysis, ThinThread processed information as it was collected—discarding useless information on the spot and avoiding the overload problem that plagued centralized systems. Binney says, "The beauty of it is that it was open-ended, so it could keep expanding."
>
> [snip]
>
> Working with N.S.A. counterterrorism experts, he had planned to set up his system at sites where foreign terrorism was prevalent, including Afghanistan and Pakistan. "Those bits of conversations they found too late?" Binney said. "That would have never happened. I had it managed in a way that would send out automatic alerts. It would have been,

> Bang!”
>
> [snip]
>
> An agency spokesman declined to comment on how the agency “performs its mission,” but said that its activities are constitutional and subject to “comprehensive and rigorous” oversight. But Susan Landau, a former engineer at Sun Microsystems, and the author of a new book, “Surveillance or Security?,” notes that, in 2003, the government placed equipment capable of copying electronic communications at locations across America. These installations were made, she says, at “switching offices” that not only connect foreign and domestic communications but also handle purely domestic traffic. As a result, she surmises, the U.S. now has the capability to monitor domestic traffic on a huge scale. “Why was it done this way?” she asks. “One can come up with all sorts of nefarious reasons, but one doesn’t want to think that way about our government.”Binney, for his part, believes that the agency now stores copies of all e-mails transmitted in America, in case the government wants to retrieve the details later. In the past few years, the N.S.A. has built enormous electronic-storage facilities in Texas and Utah. Binney says that an N.S.A. e-mail database can be searched with “dictionary selection,” in the manner of Google. After 9/11, he says, “General Hayden reassured everyone that the N.S.A. didn’t put out dragnets, and that was true. It had no need—it was getting every fish in the sea.” [my emphasis]

In other words, aside from the built-in privacy protections, ThinThread performed better than Trailblazer because it sorted data as it was collected at remote sites chosen because of some tie to terrorism. Trailblazer, on the other hand, actually copied all the data passing through switching offices, some of which carried entirely domestic traffic. Only after collecting all this data did Trailblazer start sorting through to find the terrorists.

It seems possible that these differences are made clear in the documents the government just withdrew (particularly the “Collections Sites” one).

An important part of the complaint Thomas Drake and others were making is that the government chose to collect and store everyone’s telecommunications data rather than collecting data in more logical places and eliminating all the unnecessary data. And they did so, the whistleblowers suggest, so the government could go back in and pull up your communications history at some time in the future.

And that revelation may well be what the government is trying to prosecute Drake for, while hiding the underlying truth.