NSA TWICE CHOSE TO FORGO PRIVACY PROTECTIONS IN DOMESTIC DATA MINING PROGRAMS

While Jane Mayer's profile on NSA whistleblower Thomas Drake has generated a lot of attention for the way Obama's DOJ is senselessly prosecuting him, there has been less focus on the key revelation that Drake and others went on the record to reveal in Mayer's story: that the NSA chose not to integrate the privacy protections from a program called ThinThread into its illegal domestic surveillance program.

> Pilot tests of ThinThread proved almost too successful, according to a former intelligence expert who analyzed it. "It was nearly perfect," the official says. "But it processed such a large amount of data that it picked up more Americans than the other systems." Though ThinThread was intended to intercept foreign communications, it continued documenting signals when a trail crossed into the U.S. This was a big problem: federal law forbade the monitoring of domestic communications without a court warrant. And a warrant couldn't be issued without probable cause and a known suspect. In order to comply with the law, [Bill Binney, a crypto-mathmetician who headed Signals Intelligence Automation Research Center (SARC) that developed ThinThread] installed privacy controls and added an "anonymizing feature," so that all American communications would be encrypted until a warrant was issued. The system would indicate when a pattern looked suspicious enough to justify a warrant.

> [snip]
>
> When Binney heard the rumors, he was convinced that the new domestic-surveillance program employed components of ThinThread: a bastardized version, stripped of privacy controls. “It was my brainchild,” he said. “**But they removed the protections, the anonymization process. When you remove that, you can target anyone.**” He said that although he was not “read in” to the new secret surveillance program, “my people were brought in, and they told me, ‘Can you believe they’re doing this? They’re getting billing records on U.S. citizens! They’re putting pen registers’ ”—logs of dialled phone numbers—“ ‘on everyone in the country!’ ”
>
> [snip]
>
> [Former HPSCI staffer Diane Roark] asked Hayden why the N.S.A. had chosen not to include privacy protections for Americans. She says that he “kept not answering. Finally, he mumbled, and looked down, and said, ‘We didn’t need them. We had the power.’ He didn’t even look me in the eye. I was flabbergasted.” She asked him directly if the government was getting warrants for domestic surveillance, and he admitted that it was not. [my emphasis]

Mayer’s actually not the first to report on the decision not to implement the privacy protections of ThinThread. It was the subject of one of Siobhan Gorman’s articles during the period when Drake, according to the indictment, served as a source for her. The article appeared on May 18, 2006, the morning of Michael Hayden’s confirmation hearing to be CIA Director. (Unlike most of Gorman’s articles from the period, this appears to be available only behind the Sun’s firewall. Update: I’ve found a link to the article at CommonDreams.) It describes that

since Bush's authorization for the program required no privacy protections, the NSA just didn't bother to implement that part of ThinThread.

> Once President Bush gave the go-ahead for the NSA to secretly gather and analyze domestic phone records — an authorization that carried no stipulations about identity protection — **agency officials regarded the encryption as an unnecessary step and rejected it**, according to two intelligence officials knowledgeable about ThinThread and the warrantless surveillance programs."**They basically just disabled the [privacy] safeguards,**" said one intelligence official.
>
> A former top intelligence official said that without a privacy requirement, "there was no reason to go back to something that was perhaps more difficult to implement."
>
> However two officials familiar with the program said the encryption feature would have been simple to implement. One said the time required would have involved minutes, not hours. [my emphasis; bracket original]

In other words, ThinThread came equipped with a measure—encryption—to achieve the same thing as minimization, but before the fact. But in implementing Dick Cheney's illegal wiretapping, NSA took that protection out of the program. And when asked why he had done that, Michael Hayden explained they didn't need the protection, not with the Presidential authorization they used to justify the program.

October 2001, as Michael Hayden was implementing Cheney's illegal program, was not the only time the government chose not to include privacy protections on a data mining program focused on Americans.

As Shane Harris reported in 2006 and in more detail in his book, The Watchers, when the government dismantled John Poindexter's Total Information Awareness program in August 2003 after Congress defunded it, they didn't actual dismantle most of it—they just moved it into the NSA. In his book, Harris described Poindexter's regret that the government had not salvaged the privacy protection research.

> But he regretted that the privacy research had been tossed into the dustbin. He'd never felt that the idea got traction, and what little research there'd been would wither without funding. It was a fateful decision, since the agency inheriting TIA would so on enough find itself accused of a massive and illegal incursion into Americans' private lives.

So in October 2001, NSA affirmatively chose to disable privacy protections in ThinThread, and then again in August to December 2003, the government chose to salvage the data mining aspects of Total Information Awareness, but not the privacy research.

In other words, the government, on at least two occasions, chose not to incorporate existing technology into its data mining program to protect the privacy of Americans. Sort of makes it clear that the Bush Administration wanted to make sure Americans' privacy **wasn't** protected, huh?