IN THOMAS DRAKE CASE, PROTECTED DOESN'T MEAN PROTECTED

Earlier today, we learned that (thanks to Antonin Scalia) the word "suspicion" no longer means what it used to mean.

Now we learn that "protected" doesn't mean what it used to mean.

As Josh Gerstein reports, the judge in the Thomas Drake case has agreed to let the government protect unclassified information using the Classified Information Procedures Act. But as Drake's lawyers make clear, the process of substitution is making unclassified information look classified.

> Defense lawyers contend the prosecutions proposed substitutions would be obvious to jurors, despite Bennett's ruling that they they should be "seamless." Prosecutors say some of the changes will be seamless but others cannot be because they pertain to handwritten notes that can't be modified without jurors noticing.
>
> Defense lawyers also say that if jurors are aware of the changes, they'll conclude that the information Drake is accused of mishandling is worthy of being treated as national secrets. "This will signal to the jury that the Court and the government believe information in the document was so potentially damaging to national security that it had to be withheld from the public — the very fact they must decide," defense attorney Deborah Boardman wrote in a filing Monday.

Most interesting, though, is the Defense observation that one of the documents the government will introduce at trial defines "protected" differently than the government is defining it to claim it must be substituted under CIPA.

> The defense has briefed its position on the Court's decision to impose substitutions for relevant, unclassified information that the government deems "protected," and we will not reiterate our arguments here. However, we thought the Court should be aware of the fact that NSA, in its employee Security Agreements, defines the term "protected information" in the following manner: "information obtained as a result of my relationship with NSA which is classified or in the process of a classification determination pursuant to the standards of the Executive Order 12958." **Thus, according to an NSA document, which will be a government exhibit in this case, "protected information" is "classified" information. However, the government has led the Court to believe that "protected information" is unclassified information that NSA claims deserves protection. NSA cannot have it both ways**. [my emphasis]

That might make sense if language worked the way it's supposed to. But it appears we've entered that stage of late Empire where words don't mean what they used to mean anymore.

SCALIA INVENTS A NEW

MEANING FOR "SUSPICION" WHILE LETTING ASHCROFT OFF THE HOOK

SCOTUS has just ruled unanimously that John Ashcroft can't be sued by Abdullah al-Kidd for using a material witness warrant to incarcerate him. The 8 justices (Elena Kagan recused herself) all agree there was no law explicitly prohibiting this kind of abuse of material witness warrants, so Ashcroft has immunity from suit.

Where the decision gets interesting is in the justices' various statements about whether material witness warrants are valid under the Fourth Amendment. The court's swing justice, Anthony Kennedy, basically invited a constitutional challenge of the material witness warrants themselves.

> The scope of the statute's lawful authorization is uncertain. For example, a law-abiding citizen might observe a crime during the days or weeks before a scheduled flight abroad. It is unclear whether those facts alone might allow police to obtain a material witness warrant on the ground that it "may become impracticable" to secure the person's presence by subpoena. Ibid. The question becomes more difficult if one further assumes the traveler would be willing to testify if asked; and more difficult still if one supposes that authorities delay obtaining or executing the warrant until the traveler has arrived at the airport. These possibilities resemble the facts in this case. See ante, at 2.
>
> In considering these issues, it is important to bear in mind that the

> Material Witness Statute might not provide for the issuance of warrants within the meaning of the Fourth Amendment's Warrant Clause. The typical arrest warrant is based on probable cause that the arrestee has committed a crime; but that is not the standard for the issuance of warrants under the Material Witness Statute. See ante, at 11 (reserving the possibility that probable cause for purposes of the Fourth Amendment's Warrant Clause means "only probable cause to suspect a violation of law"). If material witness warrants do not qualify as "Warrants" under the Fourth Amendment, then material witness arrests might still be governed by the Fourth Amendment's separate reasonableness requirement for seizures of the person. See United States v. Watson, 423 U. S. 411 (1976). Given the difficulty of these issues, the Court is correct to address only the legal theory put before it, without further exploring when material witness ar-rests might be consistent with statutory and constitutional requirements.

Mind you, he remains coy about what he thinks about the material witness warrants, as his language makes clear: "uncertain," "might," "unclear," "more difficult," "more difficult," "possibilities," "might not," "might." Of note, though, he neither endorses a rather crazy argument Antonin Scalia makes (joined by the usual suspects)—that witnesses to a crime may now be considered suspects of a sort—nor Ruth Bader Ginsburg's trashing (joined by Sotomayor and Breyer but not Kennedy) of that claim.

Here's Scalia's assertion:

> Needless to say, warrantless, "suspicionless intrusions pursuant to a general scheme," id., at 47, are far removed from the facts of this case. A

> warrant issued by a neutral Magistrate Judge authorized al-Kidd's arrest. The affidavit accompanying the warrant application (as al-Kidd concedes) gave individualized reasons to believe that he was a material witness and that he would soon disappear.The existence of a judicial warrant based on individualized suspicion takes this case outside the domain of not only our special-needs and administrative-search cases, but of Edmond as well.
>
> A warrant based on individualized suspicion in fact grants more protection against the malevolent and the incompetent than existed in most of our cases eschewing inquiries into intent.

Here's Ginsburg's response:

> The Court thrice states that the material witness warrant for al-Kidd's arrest was "based on individualized suspicion." Ante, at 6, 8. The word "suspicion," however, ordinarily indicates that the person suspected has engaged in wrongdoing. See Black's Law Dictionary 1585 (9th ed. 2009) (defining "reasonable suspicion" to mean "[a] particularized and objective basis, supported by specific and articulable facts, for suspecting a person of criminal activity"). Material witness status does not "involv[e] suspicion, or lack of suspicion," of the individual so identified. See Illinois v. Lidster, 540 U. S. 419, 424–425 (2004).This Court's decisions, until today, have uniformly used the term "individualized suspicion" to mean "individualized suspicion of wrong-doing."
>
> [12 cases—many of them the ones used to authorized warrantless wiretaps—cited]
>
> The Court's suggestion that the term

> "individualized suspicion" is more commonly associated with "know[ing] something about [a] crime" or "throwing . . . a surprise birthday party" than with criminal suspects, ante, at 6, n. 2 (internal quotation marks omitted), is hardly credible. The import of the term in legal argot is not genuinely debatable. When the evening news reports that a murder "suspect" is on the loose, the viewer is meant to be on the lookout for the perpetrator, not the witness. Ashcroft understood the term as lawyers commonly do: He spoke of detaining material witnesses as a means to "tak[e] suspected terrorists off the street." App. 41 (internal quotation marks omitted).

And here's Scalia's retort to that:

> JUSTICE GINSBURG suggests that our use of the word "suspicion" is peculiar because that word "ordinarily" means "that the person suspected has engaged in wrongdoing." Post, at 3, n. 2 (opinion concurring in judgment). We disagree. No usage of the word is more common and idiomatic than a statement such as "I have a suspicion he knows something about the crime," or even "I have a suspicion she is throwing me a surprise birthday party." The many cases cited by JUSTICE GINSBURG, post, at 3, n. 2, which use the neutral word "suspicion" in connection with wrongdoing, prove nothing except that searches and seizures for reasons other than suspected wrongdoing are rare.

In other words, Scalia wants to broaden the Fourth Amendment to sanction searches (and arrests) of people suspected of knowing something or doing something (throwing a birthday party!), rather than just those suspected of doing something **illegal**.

Not only does Scalia's novel interpretation of the word "suspicion" pre-empt future challenge to material witness warrants' constitutionality, but it also lays a novel groundwork for sanctioning all the domestic surveillance the government has been conducting. After all, the government is wiretapping (or tracking the geolocation of) people who may or may not have committed a crime, but are suspected solely of talking to or hanging out in the vicinity of a suspected terrorist.

And because Kennedy didn't tip his hand in either direction, that's the kind of interpretation the government will use—no doubt in its secret interpretations of the laws—to claim it can surveill even those of us suspected of no crime.

Because suspicion doesn't mean what it used to mean.

ABOUT THE LOCKHEED MARTIN HACK

As first started leaking last week, Lockheed Martin seems to have been hacked.

> Last weekend was bad for a very large U. S. defense contractor that uses SecureID tokens from RSA to provide two-factor authentication for remote VPN access to their corporate networks. Late on Sunday all remote access to the internal corporate network was disabled. All workers were told was that it would be down for at least a week. Folks who regularly telecommute were asked to come into nearby offices to work. Then earlier today (Wednesday) came word that everybody with RSA SecureID tokens would be getting new tokens over the next

> several weeks. Also, everybody on the network (over 100,000 people) would be asked to reset their passwords, which means admin files have probably been compromised.

What seems to have happened is hackers used information gotten in the RSA Data Security hack to try to break Lockheed's own security—basically, Lockheed noticed that hackers were trying to use the keys they stole in March to open a bunch of locks at Lockheed. Lockheed appears to have discovered the effort and in response, started shutting down remote access on parts of its network.

> Lockheed Martin, the Pentagon's No. 1 supplier, is experiencing a major disruption to its computer systems that could be related to a problem with network security, a defense official and two sources familiar with the issue said on Thursday.
>
> Lockheed, the biggest provider of information technology to the U.S. government, is grappling with "major internal computer network problems," said one of the sources who was not authorized to publicly discuss the matter.
>
> [snip]
>
> The slowdown began on Sunday after security experts for the company detected an intrusion to the network, according to technology blogger Robert Cringely. He said it involved the use of SecurID tokens that employees use to access Lockheed's internal network from outside its firewall,
>
> [snip]
>
> Loren Thompson, chief operating officer of the Lexington Institute, and a consultant to Lockheed, said the company

> monitored every node on its vast global computer network from a large operations center in a Maryland suburb near Washington, D.C.
>
> "If it sees signs that the network is being compromised by outsiders it will shut down whole sectors of the network to protect information," Thompson said.
>
> He said Lockheed had advanced networking monitoring tools that gave it a "much better understanding of their systems' status than most other organizations, including the Department of Defense."

In other words, Lockheed may have prevented a much bigger breach into their own systems. But the assumption of many is that other companies might not have noticed what Lockheed did. Stories on this hack all feature a list of other defense contractors—like Boeing and Raytheon and Northrup Grumman—who "decline to comment," which might mean they're scrambling to address the same problem Lockheed is, only trying to do so without all the bad PR.

Now, most observers of this hack have suggested that the hackers—who might work for a state actors or some other sophisticated crime group—were after Lockheed's war toy information (which partly explains why you'd ask Lockheed's aerospace competitors if they'd been hacked too). But remember that Lockheed does a lot for the government besides build planes. Of particular note, they're a huge NSA contractor. Maybe the hackers were after info on jet fighters, or maybe they were after the data and data collection programs our own government hides from its own citizens.

Which is all a reminder that, amidst the sound and fury directed at WikiLeaks (which after all shared important information with citizens who deserved to know it), there's a whole lot more hacking we don't learn the results of, hacking that either might result in others adopting our

lethal technologies, or in third parties stealing the data we're not even allowed to know.

Now, granted, Lockheed has far far better security than DOD's SIPRNet does. At least they're trying to protect their data. But it's not clear they—or their counterparts—are entirely successful.

THE UN-PATRIOT ACTS OF HARRY REID

When the government, through its executive and compliant Congress, wants to cut surveillance and privacy corners out of laziness and control greed, and otherwise crush the soul of the Constitution and the 4th Amendment, demagoguery and fake exigencies are the order of the day. And so they are again. Oh, and of course they want to get out of town on their vacation. And that is what has happened today.

WYDEN AND UDALL WANT OBAMA TO ADMIT TO SECRET COLLECTION PROGRAM

Ron Wyden and Mark Udall have an amendment to the PATRIOT Act that makes it clear the Obama Administration briefed the Intelligence Committees in February on an intelligence collection program, conducted under PATRIOT authority, that interprets the language of the law so broadly as to mean something it really

doesn’t say. The amendment reads, in part,

> (6) United States Government officials should not secretly reinterpret public laws and statutes in a manner that is inconsistent with the public’s understanding of these laws, and should not describe the execution of these laws in a way that misinforms or misleads the public;
>
> (7) On February 2, 2011, the congressional intelligence committees received a secret report from the Attorney General and the Director of National Intelligence that has been publicly described as pertaining to intelligence collection authorities that are subject to expiration under section 224 of the USA PATRIOT Act (Public Law 107–56; 115 Stat. 295); and
>
> (8) while it is entirely appropriate for particular intelligence collection techniques to be kept secret, the laws that authorize such techniques, and the United States Government’s official interpretation of these laws, should not be kept secret but should instead be transparent to the public, so that these laws can be the subject of informed public debate and consideration.
>
> (b) REPORT.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall publish in the Federal Register a report—
>
> (1) that details the legal basis for the intelligence collection activities described in the February 2, 2011, report to the congressional intelligence committees; and
>
> (2) that does not describe specific intelligence collection programs or activities, but that fully describes the legal interpretations and analysis necessary to understand the United

> States Government's official interpretation of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

In short, Eric Holder and James Clapper came to SSCI on February 2 and told the committee about a way the government was broadly interpreting FISA and the powers expiring next Monday.

This Amendment would require Holder to admit to what the government was doing, in broad terms, without revealing what kind of surveillance was going on.

This probably pertains to the Section 215 authorities; we know they're using it to construct databases of people who buy hydrogen peroxide and acetone. But I would bet there's a more generalized collection program that results in more databases they can mine. A very good guess would be using geolocation data from cell phones to collect information on the whereabouts of Americans.

Don't you think the time to press for such admissions is before this shit gets re-upped for another four years?

Update: Apparently this isn't even among the amendments Reid is pulling parliamentary maneuvers to avoid even discussing. So I guess this is just an effort to wave a flag saying, "PATRIOT isn't what it says it is?"

DID THOMAS DRAKE INCLUDE PRIVACY CONCERNS IN HIS

COMPLAINTS TO DOD'S INSPECTOR GENERAL?

I've been reviewing the docket on Thomas Drake's case to see whether it touches on the privacy concerns Drake had about NSA's post-9/11 activities.

It appears it doesn't, even while there was an ongoing dispute about whether or not Drake will have access to the materials he submitted to the DOD Inspector General in support of claims that the ThinThread program operated more effectively than the Trailblazer program that Michael Hayden chose to enrich SAIC with instead (the Judge ruled that material would be admissible, but not a formal whistleblower defense, which Drake wasn't trying to do anyway).

There are a couple of reasons why the silence, in the legal filings, about privacy concerns is interesting (aside from the fact that it's a focus of Jane Mayer's article.

First, because the two-sentence summary of the conclusion of the DOD IG Report on Trailblazer and ThinThread that the defense provides in a filing doesn't address privacy.

> In 2004, after more than a year of fact-finding, the Inspector General issued its initial audit findings. In a report entitled, "Requirements for the Trailblazer and Thinthread Systems," the auditors concluded that "the National Security Agency is inefficiently using resources to develop a digital network exploitation system that is not capable of fully exploiting the digital network intelligence available to analysts from the Global Information Network . . . (T)he NSA transformation effort may be developing a less capable long-term digital network exploitation solution that will take longer and cost significantly more to develop." The NSA

> continued to support the “less capable” program and its successor.

Which suggests the IG Report may not have addressed the claim that, in addition to being less efficient at “connecting the dots” than ThinThread, Trailblazer also offered none of the privacy protections ThinThread had.

That’s important because the government argued that Drake couldn’t claim to be a whistleblower because, by 2007, the issues at hand were resolved. They’re arguing both that any whistleblower claims would be mooted because Turbulence, Trailblazer’s successor, integrated “significant portions” of ThinThread, and that the debate was “over” by 2007, when Drake was (according to the indictment) serving as a source for Baltimore Sun reporter Siobhan Gorman.

> In or about December 2004, the DOD IG completed its audit of [Trailblazer], including the allegations raised in the complaint letter. The NSA responded in August 2004 and February 2005, stating that based on the judgments of NSA’s experienced technical experts, the allegations were unfounded. Nonetheless, NSA agreed to incorporate significant portions of [ThinThread] into [Trailblazer] as a result of the DOD IG recommendations, thus largely mooting the issues raised in the complaint. In addition, starting in late 2005 and early 2006, the NSA transitioned away from [Trailblazer] to [Turbulence], another corporate architecture solution for Signals Intelligence collection.
>
> [snip]
>
> Just as importantly, by 2007, the timeframe of the charges in this case, there was no imminent harm faced by the defendant, because [Trailblazer] had incorporated elements of [ThinThread],

> and also because NSA had transitioned away from [Trailblazer] to [Turbulence].
>
> [snip]
>
> The defendant's actions had no impact in the debate regarding the efficacy of [Trailblazer and ThinThread], because NSA had begun transitioning to [Turbulence] by 2006. Put simply, the debate was over.

There's a lot going on in this passage. Obviously, the government is trying to claim that since Drake was allegedly collecting information for Gorman in 2007, he couldn't claim he was whistleblowing.

Mind you he was **not** claiming he was whistleblowing, in the legal sense. He was only trying to get the IG materials to prove that's why he collected three of the documents he's accused of willingly keeping; basically, he's arguing that if he overlooked three documents out of 5 boxes worth originally collected for the IG—and did not retain the really classified materials—that he basically just overlooked the three documents, rather than willfully retained them.

And the government is playing funny with dates. After all, they say Drake served as a source for Gorman from February 27, 2006, to November 28, 2007. The key story about ThinThread Drake served as a source for was dated May 18, 2006. And one of the charges accuses Drake of obstruction for shredding other documents. So not only is the 2007 date bogus because it igonores debates ongoing in 2006, but the government suggests that either Drake would be guilty for illegally retaining information, or obstructing an investigation. Moreover, Drake maintains he inadvertently included the three IG-related documents in the several boxes of unclassified materials, so the fact the debate was over is pointless.

Moreover, the successor to Trailblazer,

Turbulence, was suffering from the same management problems Trailblazer had, as the defense notes just after citing the IG Report. The government wants to pretend the shift from Trailblazer to Turbulence ended the complaints about management problems, but it didn't.

But then there's the way the government portrays the IG complaint: efficacy. As I laid out the other day, there are four ways, Gorman's sources claim, that ThinThread was better than Trailblazer:

> The program the NSA rejected, called ThinThread, was developed to handle greater volumes of information, partly in expectation of threats surrounding the millennium celebrations. Sources say it bundled together four cutting-edge surveillance tools. ThinThread would have:
>
> * Used more sophisticated methods of sorting through massive phone and e-mail data to identify suspect communications.
>
> * Identified U.S. phone numbers and other communications data and encrypted them to ensure caller privacy.
>
> * Employed an automated auditing system to monitor how analysts handled the information, in order to prevent misuse and improve efficiency.
>
> * Analyzed the data to identify relationships between callers and chronicle their contacts. Only when evidence of a potential threat had been developed would analysts be able to request decryption of the records.

In other words, privacy was just one of three ways ThinThread was better than Trailblazer, according to Gorman's sources.

But that's not the aspect the government seems to address. That is, the government seems to be saying that, because Turbulence adopted some of

the approaches of ThinThread that made it more efficient at analysis, Drake can't complain. The suggestion is (though we can't know because of the secrecy) privacy is not, like efficacy, an adequate reason to blow the whistle. Neither privacy, nor the Constitution.

And that's interesting for two more reasons. First, because the government references a notebook of documents Drake provided that had nothing to do with the IG Report.

> There was, for example, a notebook of documents provided by the defendant, many of which had nothing to do with the IG's audit, but this notebook was destroyed before the case began, and after the IG completed its audit.

Is it playing games with the scope of the audit? That is, did Drake provide materials on privacy, which the IG didn't include within the scope of its report? If so, the IG's destruction of the notebook, in violation of DOD's document retention policy, is all the more interesting.

Then, finally, the debates about privacy continued into 2007 and 2008. In August 2007, specifically, Mike McConnell nixed a Democratic version of the Protect America Act because it required the government to tell FISA judges what the plan for minimizing US person data is and allowed the judges to review for compliance. Debates on how to fix PAA continued throughout the fall and into the following year, with Russ Feingold and Sheldon Whitehouse both trying to make real improvements on the minimization requirements.

The government seems to want to say that Drake's privacy concerns aren't a valid whistleblowing concern. Because, I guess, government officials aren't allowed to whistleblow about citizens' rights.

THOMAS DRAKE COMPLAINED ABOUT MICHAEL HAYDEN SPENDING $1B TO DO WHAT $3M COULD DO

Thomas Drake, the NSA whistleblower, was on 60 Minutes this evening. I'll have more to say about his appearance and case going forward, but I just wanted to highlight a critical detail revealed by 60 Minutes: the relative cost of Trailblazer—the SAIC implemented program Michael Hayden championed—and ThinThread—the program Drake and others claim was more effective and had privacy protections.

> One of them was Lieutenant General Michael Hayden, the head of the agency: he wanted to transform the agency and launched a massive modernization program, code named: "Trailblazer." It was supposed to do what Thin Thread did, and more.
>
> Trailblazer would be the NSA's biggest project. Hayden's philosophy was to let private industry do the job. Enormous deals were signed with defense contractors. [Bill] **Binney's Thin Thread program cost $3 million; Trailblazer would run more than $1 billion and take years to develop**.
>
> "Do you have any idea why General Hayden decided to go with Trailblazer as opposed to Thin Thread, which already existed?" Pelley asked.
>
> "I believe he was convinced by others that going with a large-scale,

> industrial strength solution was the approach that NSA needed to take. You can't really understand why they would make that kind of a decision without understanding the culture of NSA," Drake said.
>
> Asked to elaborate, Drake said, "Careers are built on projects and programs. The bigger, the better their career." [my emphasis]

So Drake was complaining about a program that cost 300 times as much as the one he championed (ultimately, Trailblazer cost $1.2 billion, so actually 400 times as much). It's not an apples-to-apples comparison. Trailblazer, according to a government filing, worked across more platforms. ThinThread, according to a Siobhan Gorman story, had additional functionality, including privacy protections.

But still, Drake complained about a program that did what ThinThread did—at 300 to 400 times the cost.

As one of the other NSA employees who whistleblew about Trailblazer, J. Kirk Wiebe, explains,

> "How does a man see 9/11 happened, know that some part of it is due to corruption and mismanagement and sleep at night. How does a man do that? He obviously couldn't," Wiebe told Pelley.

Yet the government wants to put Drake in jail for 35 years because he tried to make sure incompetence that led to 9/11 doesn't continue.

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?

PLEASE HELP SUPPORT

MY NEXT 525 POSTS ON TORTURE

Just over two years ago, right around the time I reported that Khalid Sheikh Mohammed was waterboarded 183 times in a month, many of you chipped into the "Marcy Wheeler fund" to support my work; that generosity paid my way until a short time ago. Here's what that support made possible.

Between May 1, 2009 and yesterday, by my rough count, I wrote 525 posts on torture. I unpacked the torture memos, the CIA IG Report, the OPR Report, and thousands of documents released through FOIA. I showed the bureaucratic games they used to set up our torture program, early efforts to place limits on things like mock

execution, followed by more bureaucratic and legal means to get away with violating even those limits. I showed how they hid documents and altered tapes to hide evidence of their torture. I showed how, after CIA and parts of DOJ tried to put limits on torture in 2004, they again used bureaucratic tricks and ridiculous legal documents to reauthorize it. I've tracked DOJ's kabuki claims to investigate torture (though bmaz gets credit for forcing DOJ to admit John Durham's torture tape investigation had run out the clock on Statutes of Limitation). And I've tracked the Obama Administration's successful efforts to suppress all evidence of torture. And all the while, I've relentlessly pushed back against the torture apologists' lies.

Of course, while writing about torture is a major part mapping out the decline of the rule of law, it's not the only part. Since May 2009, I've written almost 200 posts on wiretapping, almost as many on our Gitmo show trials, posts about state secrets, drones, fusion centers, the forever war metastisizing around the world. I've written about Wikileaks and Bradley Manning's treatment and the banksters and the auto companies.

Cataloging the decline of the rule of law has been exhausting and infuriating. The work has been challenging.

But most of all, it has been humbling. That's because you made this happen, as much as I did.

In addition to the absolutely brilliant observations you've made in comments, your support, two years ago, made this work possible. I'm profoundly grateful that many of you invested your faith and financial support in my work.

And now I'm asking for your faith and financial support again, to support the next 525 posts on torture. This time that support will come in the form of an ongoing Firedoglake membership. By becoming a member of Firedoglake, you will not

only give my work some stability over the long term, but support the superb work of Jane and DDay and Jon Walker, and just as importantly, the work of the people backstage who make this all technically possible. And you will become a closer part of our efforts to push our country in the right direction, to return to the rule of law.

Please join Firedoglake today.

I hope some day soon we'll begin to make headway against our expanding national security state. I hope some day, I won't feel the need to write a post on torture five days a week. But until then, I feel compelled to write about what is happening to our country. And I can only continue to do that with your help.

THE ISSUES THOMAS DRAKE AND OTHERS WHISTLEBLEW ON REMAIN URGENT

I've been looking at one of the Siobhan Gorman articles that accused whistleblower Thomas Drake served as a source for. I'll have more later, but I wanted to point out one main thrust of the story: the NSA had no way of measuring efficacy and controlling costs.

> At the NSA, and throughout the government, the Sept. 11 attacks created a crisis atmosphere. Congress responded by pouring money into anti-terrorism efforts, while intelligence agencies scrambled to put new programs in place — often without the planning and oversight needed to succeed, intelligence professionals said.

> At an agency-wide meeting at the NSA not long after the Sept. 11 attacks, Michael V. Hayden, then the NSA director, announced a $1 billion budget increase.
>
> But the top-secret agency, based at Fort Meade between Baltimore and Washington, has no mechanism to systematically assess whether it is spending its money effectively and getting what it has paid for, NSA veterans said. One former employee likened it to a neighborhood with no police to enforce the traffic laws.

While this is not necessarily the core of what—per Jane Mayer—the government is prosecuting Drake for, it's important for this reason. The NSA has been claiming—falsely—to have fixed its clusterfuck accounting system.

> In June 2009, the Director of NSA wrote to the Chairman and Vice Chairman, claiming that the NSA was now —fully compliant with the laws, regulations, and manuals referenced in the U.S. Army Finance Command report and the Federal Financial Managers Integrity Act. The NSA Director's letter also stated that the NSA had been able to reconcile its fiscal year 2008 financial records. In July 2009, the Chairman and Vice Chairman wrote to the Secretary of Defense concerning the NSA Director's letter. They stated that in light of the NSA's past difficulties in producing auditable financial statements, the Committee believed the progress claimed by the NSA should be independently confirmed by the DoD Inspector General. Specifically, the letter requested that the DoD IG conduct a form and content review of the NSA's fiscal year 2009 financial statements to determine whether they were supported by reliable and accounting data and supporting information.

> The Committee received the results of the DoD IG's review in November 2009, which was very critical of NSA's claims. Overall, the IG found that the **NSA's financial statements were not adequately supported by reliable accounting data and supporting information. An even more disturbing finding was that the NSA's —remediation plans do not fully address audit impediments**. Specific findings included an inability to reconcile critical general ledger balances, failure to perform required accounting processes, and inconsistencies between the information contained in the notes to the financial statements and the information provided to the IG. The IG's findings raised serious questions about the assertions made by the NSA Director in his June 2009 letter and the support he is receiving from the administrative staff involved. [my emphasis]

This is just one reason why the government's prosecution of Thomas Drake is so outrageous. While his charges pertain to the way in which contracts get picked (rather than to the accounting clusterfuck itself), the prosecution of him—effectively, if Mayer is right, because he refused to falsely claim close allies sourced the illegal wiretap story—serves primarily to intimidate whistleblowers.

It took intelligence oversight committees seven years to prove that NSA wasn't fixing problems first exposed eight years ago. Yet people were trying—in 2006—to expose the ongoing problems.

And yet the most transparent President seems to be doing everything he can to make sure no one makes similar efforts in the future.