LATEST STUXNET INCARNATION RESEMBLES ALLEGED PROJECT OF MURDERED GCHQ OFFICER

Kaspersky Labs has found a new incarnation of StuxNet malware, which they've called Gauss. As Wired summarizes, the malware is focused geographically on Lebanon and has targeted banks.

> A newly uncovered espionage tool, apparently designed by the same people behind the state-sponsored Flame malware that infiltrated machines in Iran, has been found infecting systems in other countries in the Middle East, according to researchers.
>
> The malware, which steals system information but also has a mysterious payload that could be destructive against critical infrastructure, has been found infecting at least 2,500 machines, most of them in Lebanon, according to Russia-based security firm Kaspersky Lab, which discovered the malware in June and published an extensive analysis of it on Thursday.
>
> The spyware, dubbed Gauss after a name found in one of its main files, also has a module that targets bank accounts in order to capture login credentials. The malware targets accounts at several banks in Lebanon, including the Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank and Credit Libanais. It also targets customers of Citibank and PayPal.

I find that interesting for a number of reasons.

First, every time banks have squawked about our government's access of SWIFT to track terrorist financing, the spooks have said if they don't use SWIFT they'll access the information via other means; it appears this malware may be just that. And the focus on Lebanon fits, too, given the increasing US claims about Hezbollah money laundering in the time since Gauss was launched. I'm even struck by the coincidence of Gauss' creation last summer around the same time that John Ashcroft was going through the Lebanese Canadian Bank to find any evidence of money laundering rather than—as happens with US and European banks—crafting a settlement. I would imagine how that kind of access to a bank would give you some hints about how to build malware.

But the other thing the malware made me think of, almost immediately, was the (I thought) bogus excuse some British spooks offered last summer to explain the murder of Gareth Williams, the GCHQ officer—who had worked closely with NSA—who was found dead in a gym bag in his flat in August 2010. Williams was murdered, the Daily Mail claimed, because he was working on a way to track the money laundering of the Russian mob.

> The MI6 agent found dead in a holdall at his London flat was working on secret technology to target Russian criminal gangs who launder stolen money through Britain.
>
> [snip]
>
> But now security sources say Williams, who was on secondment to MI6 from the Government's eavesdropping centre GCHQ, was working on equipment that tracked the flow of money from Russia to Europe.
>
> The technology enabled MI6 agents to follow the money trails from bank accounts in Russia to criminal European gangs via internet and wire transfers, said the source.
>
> 'He was involved in a very sensitive project with the highest security

> clearance. He was not an agent doing surveillance, but was very much part of the team, working on the technology side, devising stuff like software,' said the source.
>
> He added: 'A knock-on effect of this technology would be that a number of criminal groups in Russia would be disrupted.
>
> 'Some of these powerful criminal networks have links with, and employ, former KGB agents who can track down people like Williams.'

Frankly, I always thought that explanation was bogus—I suggested that the Brits could just partner with the US to access such data via SWIFT. And whatever it means, I haven't seen such an explanation since.

But I do find it rather interesting that one of the most prominent unsolved murders of a spook was blamed—at around the time the StuxNet people were working on Gauss—on a plan to track money laundering.

DICK DURBIN: THE TARGETED KILLING MEMO IS LIKE THE TORTURE AND ILLEGAL WIRETAP MEMOS

It took transcribing the debate in the July 19 Senate Judiciary Committee hearing for me to realize it, but Democrats are running very serious interference to keep the Anwar al-Awlaki targeted killing memo secret. Not only did

Dianne Feinstein basically roll John Cornyn, telling him she'd introduce language that would accomplish his goal of getting all the oversight committees the memo when, if hers passes, it will only, maybe, get the Intelligence Committee the memo. Not only did the Democrats vote on a party line vote to table John Cornyn's amendment to require the Administration to share it—in classified or unclassified form—with the Judiciary and Armed Services Committees. Not only did Pat Leahy get pretty snippy with Cornyn for offering—and asking to speak on—the Amendment.

Most stunning, though, is Dick Durbin's comment on it.

> Durbin: Thank you Mr. Chairman. My staff briefed me of this on the way in, and I asked the basic question, "would I ask this of a Republican President? Of course. And **I did ask it, in a different context, of the previous President, when it came to questions of interrogation, torture, and surveillance**. I might say to the Senator from Texas I had no support from the other side of the table when I made that request. But I do believe it is a valid inquiry and I would join the Senator from Texas and any who wish in sending a letter to the Attorney General asking for this specific information on a bipartisan basis. And certainly we can raise it the next time the Attorney General appears before us. I do have to say that I'm going to vote to table because I think that as flawed as this [the FAA extension] may be without the Lee Amendment which I think would help it, I do believe we need to pass this and bringing in these other matters are going to jeopardize it. But I think it is a legitimate question to be asked of Presidents of either party, and I will join you in a letter to this President and his Attorney General for that

> purpose. [my emphasis]

This partisan retort (one Leahy repeated) says, in part, that the Democrats aren't going to cooperate with Cornyn's effort to get the memo because Cornyn didn't cooperate with Durbin's efforts to get the torture and illegal wiretap memos. Durbin and Leahy are right: Cornyn and the rest of the Republican party did obstruct their efforts.

That doesn't make obstructing Cornyn's effort right, of course, particularly given that Durbin purports to support Cornyn's intent.

But remember, Republicans obstructed the release of the torture and illegal wiretap memos because, well, they showed the Executive had broken the law. When we all got to see the torture memos, they made it clear CIA had lied to DOJ to get authorization for torture, had exceeded the authorizations given to them, had engaged in previously unimagined amounts of torture, and had ignored legal precedent to justify it all.

And while we've only ever seen part of Jack Goldsmith's illegal wiretap memo (after the Bush Administration purportedly fixed the data mining and other illegal problems with it) and a teeny fragment of an earlier John Yoo memo, those showed that Yoo relied on gutting the Fourth Amendment, there is an additional secret memo on information sharing, they were hiding their flouting of the exclusivity provision, and—possibly—the illegal wiretap program violated an earlier decision from the FISA Court of Review. We also learned, through some Sheldon Whitehouse persistence, that these memos revealed the President had been pixie dusting Executive Orders and claiming the right to interpret the law for the Executive Branch.

The Republicans had good reason to want to help Bush bury these memos, because they showed breathtaking efforts on the part of the Bush Administration to evade the law.

And that’s the fight that Dick Durbin analogized this one to.

9TH CIRCUIT: NO WAY TO PUNISH THE GOVERNMENT IF THEY ILLEGALLY COLLECT (BUT DON’T USE) YOUR TELECOMMUNICATIONS

As Josh Gerstein just reported, the 9th Circuit has thrown out a decision against the government in the al-Haramain wiretapping suit. While they don’t comment on Judge Vaughn Walker’s judgement that al-Haramain had standing and had proven they had been spied on, the panel ultimately held that for the alleged actions—collecting al-Haramain’s telecommunications—the government has sovereign immunity. Al-Haramain can only sue individuals, not the government.

The ruling sucks for al-Haramain. But it has larger implications. Effectively, the 9th Circuit is saying there’s no way to hold the government accountable for simply collecting your telecommunications illegally; you can only hold them accountable if they use that information in a trial.

It distinguishes those two activities this way, pointing to language that specifically invokes the United States as a defendant in case of 1806 (use in an official proceeding) but not 1810 (collection).

> Contrasting § 1810 liability, for which sovereign immunity is not explicitly waived, with § 1806 liability, for which it is, also illuminates congressional

> purpose. Liability under the two sections, while similar in its reach, is not identical. Section 1806, combined with 18 U.S.C. § 2712, renders the United States liable only for the "use[ ] and disclos[ure]" of information "by Federal officers and employees" in an unlawful manner. Section 1810, by contrast, also creates liability for the actual collection of the information in the first place, targeting "electronic surveillance or . . . disclos[ure] or use[ ]" of that information. (emphasis added). **Under this scheme, Al-Haramain can bring a suit for damages against the United States for use of the collected information, but cannot bring suit against the government for collection of the information itself.** Cf. ACLU v. NSA, 493 F.3d 644, 671 (6th Cir. 2007) (Lead Opinion of Batchelder, J.) (noting that FISA potentially allows limitless information collection upon issuance of warrant, but limits use and dissemination of information under, inter alia, § 1806(a)). Although such a structure may seem anomalous and even unfair, the policy judgment is one for Congress, not the courts. Also, because governmental liability remains under § 1806, the district court's concern that FISA relief would become a dead letter is not valid. See In re Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d at 1125.
>
> [snip]
>
> Congress can and did waive sovereign immunity with respect to violations for which it wished to render the United States liable. It deliberately did not waive immunity with respect to § 1810, and the district court erred by imputing an implied waiver. Al Haramain's suit for damages against the United States may not proceed under § 1810.

Because al-Haramain, at a time when Vaughn Walker was using 1810 to get by the government's State Secrets invocation, said "it was not proceeding under other sections of FISA," its existing claim is limited to 1810. The government used the information collected—in a secret process that ended up declaring al-Haramain a terrorist supporter—but not in a trial, and therefore not in a way al-Haramain can easily hold the government liable for.

The implication, of course, is that all the rest of the collection the government engages in—of all of us, not just al-Haramain—also escapes all accountability. So long as the government never uses the information itself—even if the entire rest of their case is based on illegally collected information (as it was in, at a minimum, al-Haramain's terrorist designation)—a person cannot hold the government itself responsible.

The people who can be held accountable? The non-governmental or non law enforcement persons who conduct the surveillance.

But of course, they—the telecoms—have already been granted immunity.

IT'S NOT JUST WHETHER NIDAL HASAN'S EMAILS STUCK OUT, IT'S WHETHER ABDULMUTALLAB'S DID

I've been meaning to return to the Webster report on Nidal Hasan's conversations with Anwar al-Awlaki. This conversation between Gunpowder & Lead and Intelwire about how alarming those emails were will be a start provides a good

place to start.

Hasan's emails should have raised more concern—but probably didn't because of the sheer volume of Awlaki intercepts

G&L notes that certain details from the emails—such as his invocation of Hasan Akbar, a Muslim-American soldier who killed two officers in Kuwait—as an example that should have raised more concern than it did.

> But more significant, his question to Awlaki didn't actually deal with the valid question that he raised, the feeling of inner conflict between one's faith and serving in the U.S. military. Instead, he leaped right to a question that should rightly trigger alarm: *if Hasan Akbar died while attacking fellow soldiers, would he be a martyr*? Hasan skipped over questions about whether serving in the U.S. military is religiously acceptable; whether going to war against fellow Muslims is a violation of religious principles. Instead, in addressing "some" soldiers who felt conflicted about fighting fellow Muslims, Hasan right away asked whether it was permissible to kill other U.S. soldiers in the way Hasan Akbar.

After a close analysis of a number of the emails, G&L refutes the representation of these emails as "fairly benign."

I agree with that assessment (and would add that the suggestion, in a February 22, 2009 email, that Hasan was donating to entities that his mosque would not is another troubling detail). But I also agree with Intelwire. These emails, from an Army officer, surely merited more attention. But these emails, as they likely appeared among the stream of Anwar al-Awlaki communications, probably did not stick out.

> Based on who Hasan was (a military officer), who he was talking to (a

> suspected 9/11 accomplice), and the fact he repeatedly tried to get Awlaki's attention using a variety of stratagems, the case should have been escalated and Hasan's superiors should have been informed.
>
> But when you place the *content* of Hasan's messages alongside all the other raw intelligence that counterterrorism investigations generate, it's extremely hard to argue from a subjective, non-psychoanalytical reading that they represented a red flag.

Which is why this report has seemed poorly scoped to me. Because not only did Nidal Hasan's emails fail to trigger further attention, but Umar Farouk Abdulmutallab's contacts with Awlaki before Fort Hood did too.

In spite of the fact that the FBI had two people spending a significant chunk of each day (they claimed it took 40% or 3 hours of their work day; 88) reviewing communications tied to Awlaki, in spite of the fact that two men about to attack the US were in contact with Awlaki, "the FBI's full understanding of Aulaqi's operational ambitions developed only after the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009." (72)

The government also failed to respond to Abdulmutallab intercepts leading up to the Fort Hood attack

Consider: according to the report itself, Robert Mueller formally asked William Webster to conduct this inquiry on December 17, 2009 (though Webster's appointment was reported over a week before then). Just 8 days later, another terrorist who had been in contact with Awlaki struck the US. Just 5 days after that, sources started leaking details of NSA intercepts from 4 months earlier (so around August) that might have warned about the attack.

> Intelligence intercepts from Yemen beginning in early August, when Abdulmutallab arrived in that country, contained "bits and pieces about where he was, what his plans were, what he was telling people his plans were," as well as information about planning by the al-Qaeda branch in Yemen, a senior administration official said. "At first blush, not all these things appear to be related" to the 23-year-old Nigerian and the bombing attempt, he said, "but we believe they were."

It's unclear how many of these intercepts were directly between Abdulmutallab and Awlaki, and therefore presumably reviewed by the FBI team in San Diego. But at least according to the sentencing materials submitted in the Abdulmutallab case (there are reasons to treat this with a bit of skepticism), there were substantive communications between Awlaki and Abdulmutallab.

> Defendant provided this individual [who offered to connect him with Awlaki] with the number for his Yemeni cellular telephone. Thereafter, defendant received a text message from Awlaki telling defendant to call him, which defendant did. During their brief telephone conversation, it was agreed that defendant would send Awlaki a written message explaining why he wanted to become involved in jihad. Defendant took several days to write his message to Awlaki, telling him of his desire to become involved in jihad, and seeking Awlaki's guidance. After receiving defendant's message, Awlaki sent defendant a response, telling him that Awlaki would find a way for defendant to become involved in jihad.

Now, it's possible this communication didn't show up in the San Diego stream. Maybe the NSA

didn’t share all its Awlaki intercepts with the San Diego team. The report notes that Awlaki and his allies were using means to hide their contacts (127). The report notes some forms of VOIP are not included under CALEA, which may have affected Abdulmutallab’s call. (128) And the month after the Abdulmutallab attack and after Pete Hoekstra revealed the NSA intercepts on Awlaki, he allegedly implemented a sophisticated encryption system with Rajib Karim. But if the Awlaki collection, as it existed in 2009, failed both because of volume and because of technical reasons, shouldn’t those be part of the same inquiry?

By the end of December 2009, the FBI and NSA knew they had collected, reviewed, and failed to adequately respond to intercepts from two future terrorists. Why not include both in this study?

Hasan’s contacts (and presumably Abdulmutallab’s) were dissociated needles in an Awlaki haystack

The Webster report doesn’t provide exact details of how much intelligence was coming in on the Awlaki investigation. They redact the number of leads, investigations, and Information Intelligence Reports the intercepts produced—though they appear to be 3-digit numbers (see page 35). The report suggests that the San Diego team focused attention on Awlaki-related intercepts starting on March 16, 2008 (87; interestingly, in the extension period for PAA and before FAA imposed new protections for Americans overseas). Between March 2008 and November 2009, the JTTF team in San Diego reviewed over 29,000 intercepts. And the volume was growing: in earlier phases of the Hasan investigation, the San Diego team was averaging 1,420 intercepts a month; that number grew to 1,525 by the time of the Fort Hood attack. The daily average went from 65-70 intercepts a day to 70-75, though some days the team reviewed over 130 intercepts. And while he obviously had reasons to play up the volume involved, the Analyst on the San Diego team considered it a

"crushing volume" of intercepts to review. Discussions of the volume of intercepts appear on page 35, 36, 46, 61, 87, 88, 92.

In any case, the emails between Hasan and Awlaki made up just one quarter of one percent of the volume the FBI reviewers reviewed over this period. While we don't know how these emails compared to the rest of the traffic (a point the Webster report makes, (88) it is clear they made up just a tiny fraction of what the FBI reviewed.

There are two factors that must have made this review process more difficult.

First, the FBI's database of intercepts sucked. When the first Hasan intercepts came in, it allowed only keyword searches; tests the Webster team ran showed it would have taken some finesse even to return all the contacts between Hasan and Awlaki consistently. More importantly, it was not until February 2009 that the database provided some way to link related emails, so the Awlaki team in San Diego relied on spreadsheets, notes, or just their memory to link intercepts. (91) But even then, the database only linked formal emails; a number of Hasan's "emails" to Awlaki were actually web contacts, (100) which would not trigger the database's automatic linking function. In any case, it appears the Awlaki team never pulled all the emails between Hasan and Awlaki and read them together, which would have made Hasan seem much more worrisome (though when the San Diego agent set the alert for the second email, he searched and found the first one).

In addition, the Agent in charge of the investigation took on a supervisory role in mid-July 2009, just before Abdulmutallab came on the scene. (45) Given that the computer didn't allow for any institutional memory, losing an investigative team member would effectively lose the work on any given investigation.

One more factor would have made it harder to respond appropriately to early Abdulmutallab

intercepts. At least some of those reportedly needed to be translated (this also suggests that some of the most interesting intercepts involving Abdulmutallab weren't between Awlaki and the Nigerian, as English would be the natural language for the two to converse in).

Even tracking the communications of one terrorist radicalizer, we're drowning in data

All of which suggests we're still collecting more information than we can even analyze. Whatever else I've said about the government's evidence against Awlaki, I absolutely believe he was an obvious target for collection. But if we don't have the technical capabilities to exploit even that one stream, what does that say about our intelligence gathering?

The Webster report does say that many of the problems with FBI's intercepts database were fixed with a September 2011 update. And FBI changed training and access rules before that point to make sure key members of the JTTFs can use the database. But several of the recommendations made by the Webster team pertain to enhancing the database with both hardware and software improvements.

One of the big takeaways from the Webster report, it seems to me, is we were asking FBI officers to analyze a flood of data using the most archaic tools. Sure, there was reason enough they should have escalated the investigation into Nidal Hasan. But far more attention needs to be focused on our continued data failures, particularly among the belief more data is a cure-all.

USING PENSIONS TO

“PUNISH” “LEAKS” WILL SUBJECT CLEARANCE HOLDERS TO ARBITRARY POWER

The Senate Intelligence Committee’s new anti-leak laws are the part of the Intelligence Authorization that will generate the most attention. Greg Miller already got Dianne Feinstein to admit there’s no reason to think one of the new provisions—permitting only the most senior intelligence officials to do background briefings—will limit leaks.

> Feinstein acknowledged that she knew of no evidence tying those leaks or others to background sessions, which generally deal broadly with analysts’ interpretations of developments overseas and avoid discussions of the operations of the CIA or other spy services.

Another of the provisions—requiring intelligence committee heads to ensure that every sanctioned leak be recorded—ought to be named the Judy Miller and Bob Woodward Insta-Leak Recording Act.

> (a) RECORD REQUIREMENT.—The head of each element of the intelligence community shall ensure that such element creates and maintains a record of all authorized disclosures of classified information to media personnel, including any person or entity under contract or other binding agreement with the media to provide analysis or commentary, or to any person or entity if the disclosure is made with the intent or knowledge that such information will be made publicly available.

I’m sure someone can think of some downside to

this provision, but I can't think of it at the moment (which is why Obama will probably find some way to eliminate it). It will end some of the asymmetry and abuse of classification as it currently exists.

In addition, there are a bunch of provisions that are just dumb bureaucracy.

But it's this one that is deeply troubling. Among the other provisions making nondisclosure agreements more rigorous is a provision that would allow an intelligence community head to take away a person's pension if they "determine" that an individual violated her nondisclosure agreement.

> (3) specifies appropriate disciplinary actions, including the surrender of any current or future Federal Government pension benefit, to be taken against the individual if the Director of National Intelligence or the head of the appropriate element of the intelligence community determines that the individual has knowingly violated the prepublication review requirements contained in a nondisclosure agreement between the individual and an element of the intelligence community in a manner that disclosed classified information to an unauthorized person or entity;

Ron Wyden objects to this on the obvious due process grounds (and notes a big disparity between the treatment of intelligence agency employees and those in, say, the White House). He also describes a scenario in which a whistleblower might be targeted that gets awfully close to the plight of Thomas Drake, who was prosecuted for the documents he had—upon the instruction of the NSA Inspector General—kept in his basement to make a whistleblower complaint.

> It is unfortunately entirely plausible to me that a given intelligence agency could conclude that a written submission

> to the congressional intelligence committees or an agency Inspector General is an “unauthorized publication,” and that the whistleblower who submitted it is thereby subject to punishment under section 511, especially since there is no explicit language in the bill that contradicts this conclusion.

But there’s one thing Wyden left out: the proven arbitrariness of the existing prepublication review process. A slew of people have well-founded gripes with the prepublication review process: Valerie Plame, for CIA’s unwillingness to let her publish things that Dick Cheney already exposed; Peter Van Buren for State’s stupid policy on WikiLeaks; Glenn Carle for the delay and arbitrariness. That list alone ought to make it clear how a provision giving agencies even more power to use the prepublication review process as a means to exact revenge for critics would be abused.

Now consider the most egregious case: the disparate treatment of Jose Rodriguez and Ali Soufan’s books on torture. Rodriguez was able to make false claims, both about what intelligence torture produced and about legal facts of his destruction of the torture tapes. Yet Soufan was not permitted to publish the counterpart to those false claims. Thus, not only did prepublication review prevent Soufan from expressing legitimate criticism. But the process facilitated the production of propaganda about CIA actions.

What’s truly bizarre is that the same people who want to leverage the already arbitrary power prepublication review exacts over government employees have also expressed concern about how arbitrary the prepublication review process is.

> U.S. officials familiar with the inquiry, who spoke on condition of anonymity, said that it reflects growing concern in the intelligence community

> that the review process is biased toward agency loyalists, particularly those from the executive ranks.
>
> Members of the Senate Intelligence Committee expressed such concerns in a recent letter to CIA Director David H. Petraeus, a document that has not been publicly released.

As it is, intelligence community officials will be subject to unreliable polygraph questions focusing on unauthorized (but not authorized) leaks. Those expanded polygraphs come at a time when at least one agency has already been accused of using them for fishing expeditions.

And now the Senate Intelligence Community want to allow agency heads to use a prepublication review process **that they themselves** have worried is politicized to punish alleged leakers?

CONGRESS CAN'T LEGISLATE OVERSIGHT FOR FEAR OF LEGAL CHALLENGES THAT'D ACCOMPLISH OVERSIGHT CONGRESS CAN'T LEGISLATE

Julian Sanchez has his own rebuttal to former DOJ official Carrie Cordero's claims that FISA has plenty of oversight (see mine here). You should definitely read it, which is wonky and interesting. But I wanted to add my non-wonky answer to a question Sanchez poses.

> I'll grant Cordero this point: as absurd

> as it sounds to say “we can’t tell you how many Americans we’re spying on, because it would violate their privacy,” this might well be a concern if those of us who follow these issues from the outside are correct in our surmises about what NSA is doing under FAA authority. The only real restriction the law places on the *initial* interception of communications is that the NSA use “targeting procedures” designed to capture traffic to or from overseas groups and individuals. There’s an enormous amount of circumstantial evidence to suggest that initial acquisition is therefore *extremely* broad, with a large percentage of international communications traffic being fed into NSA databases for later querying. If that’s the case, then naturally the tiny subset of communications later reviewed by a human analyst—because they match far narrower criteria for suspicion—is going to be highly unrepresentative. To get even a rough statistical sample of what’s in the larger database, then, one would have to “inspect”—possibly using software—a whole lot of the innocent communications that wouldn’t otherwise ever be analyzed. And possibly the rules currently in place don’t make any allowance for querying the database—even to analyze metadata for the purpose of generating aggregate statistics—unless it’s directly related to an intelligence purpose.
>
> A few points about this. First: assuming, for the moment, that this is the case, why can’t NSA and DOJ say so clearly and publicly?

Sanchez dismisses a bunch of lame excuses that the government might provide. But he doesn’t consider another obvious answer.

The government can't tell us it can't tell us how many Americans get spied on after every foreign telecommunication gets sucked up because if it did, then it'd be a lot easier for the plaintiffs in Amnesty v. Clapper to get standing. And the government can't have that—particularly not before SCOTUS hears the case on October 29—because if so it would allow the plaintiffs to actually challenge the underlying surveillance, and possibly even to challenge what I've called the database exception.

So the government can't answer Ron Wyden's questions before the FISA Amendments Act gets extended because the government is not about to let this extension wait until after the election, which is, after all, just a week after SCOTUS hears Clapper. And since the House is planning to leave DC for the election on October 5, it means the public simply can't be told the underlying facts of this spying program, because it'd give Amnesty and the ACLU more than three weeks to figure out how to win their standing case at SCOTUS.

Which brings me to another piece of oversight we can't have. As I have noted, Dianne Feinstein, after suggesting her legislation requiring the government to turn over the Targeted Killing OLC memos would accomplish what John Cornyn wanted to accomplish, not only crafted the language such that the government could withhold the memo from Cornyn because he's not read into the assassination compartment.

DiFi's thorough rolling of Cornyn on this point was even worse, however. Cornyn wanted to put an amendment on the must-pass FISA Amendments Act. If his amendment hadn't been tabled, there'd be a very good chance it'd get passed, and therefore that it'd be passed by October 5, meaning (given Cornyn's one month deadline) the government would have to comply by November 5. Heck, it might even be passed by September 20, which is the next hearing for one of two FOIA hearings on drone and/or targeted killing the

ACLU has.

But the Intelligence Authorization is not a must-pass legislation, and certainly not something that has to pass by the election. So assuming it gets dumped into the lame duck period and given the six month deadline on DiFi's legislation, it would give the Administration until sometime next year to comply. Add in its covert operation loophole (the same way the government has been refusing the ACLU's FOIA), and its application solely to the Intelligence Committees, DiFi's amendment safely protects the government from having to admit publicly what it has already repeatedly admitted (albeit in a format the judges say doesn't count), that it has used drones to kill an American citizen.

DOJ can't tell the committees overseeing it about the authorization they gave the President to kill American citizens, you see, because if it did then the Administration could no longer claim the authorization to kill American citizens is too secret for oversight. Or something like that.

You see, I'm beginning to be convinced that the only kind of legislation Congress can accomplish ensures that it doesn't accidentally legislate something that accidentally allows NGOs using the courts to conduct the oversight that Congress won't exercise.

IF EVERYTHING NSA DOES IS "AUDITABLE," WHY CAN'T NSA TELL US HOW MANY AMERICANS

THEY'VE SPIED ON?

NSA Director Keith Alexander just said this to the hackers at DefCon (while wearing an absolutely ridiculous hacker costume):

> "We get oversight by Congress, both intel committees and their congressional members and their staffs," he continued, "so everything we do is auditable by them, by the FISA court … and by the administration. And everything we do is accountable to them…. We are overseen by everybody. And I will tell you that those who would want to weave the story that we have millions or hundreds of millions of dossiers on people is absolutely false."

But a month ago, Alexander's Inspector General told Ron Wyden that an estimate of the number of people inside the United States who have had their communications collected or reviewed under the FISA Amendments Act "was beyond the capacity of his office." Of note, the IG and NSA leadership—that is, presumably Alexander himself—claimed such a review would "violate the privacy of U.S. persons."

I look forward to Ron Wyden's response to Alexander's seeming reversal on that earlier letter with claims of this unlimited auditability.

WHY ARE FAA BOOSTERS SATISFIED WITH INADEQUATE

OVERSIGHT?

Julian Sanchez hosted a Cato event yesterday that examined surveillance generally and the FISA Amendments Act specifically. At it, Ron Wyden presented his concerns about the FISA Amendments Act and other surveillance, and then ACLU's Michelle Richardson and NYT's Eric Lichtblau added their own views.

There was one question asked during the question period claiming that the program undergoes adequate reviews. The questioner was Georgetown's Director of National Security Studies, Carrie Cordero, who had a role on FISA implementation until 2010, who has now reprised and expanded her comments at Lawfare.

She starts by addressing Wyden's request that DNI to tell Congress how many Americans have had their communications "collected or reviewed."

> In particular, they have, in a series of letters, requested that the Executive Branch provide an estimate of the number of Americans **incidentally intercepted** during the course of FAA surveillance. According to the exchanges of letters, the Executive Branch has repeatedly denied the request, on the basis that: i) it would be an unreasonable burden on the workforce (and, presumably, would take intelligence professionals off their national security mission); and ii) gathering the data the senators are requesting would, in and of itself, violate privacy rights of Americans.
>
> The question of whether the data call itself would violate privacy rights is a more interesting one. Multiple oversight personnel independent of the operational and analytical wings of the Intelligence Community – including the Office of Management and Budget, the NSA Inspector General, and just last month, the Inspector General of the Intelligence

> Community, have all said that the data call requested by the senators is not feasible. The other members of the SSCI appear to accept this claim on its face. Meanwhile, Senator Wyden states he just finds the claim unbelievable. [my emphasis]

Note, first of all, that she mischaracterizes Wyden's request. He asked about US person communication that had been "collected or reviewed," whereas she claimed he was asking only about incidental interception. Those are different things, and what Wyden's interested in is far more invasive than simply having your communications sitting in a data warehouse in UT unread.

That's important because Cordero treats one aspect of the DNI IG's response—the privacy claim—as an "interesting question," but then she proceeds to not answer the question. She instead reverts back to what she had correctly portrayed as NSA's claim that NSA didn't have the capacity because it would be "unreasonable burden on the workforce," then asks why Wyden doesn't believe that claim.

Remember, the privacy claim was raised solely in terms of whether the NSA's Inspector General could conduct a review, not whether NSA analysts should be pulled off reviewing intercepts to find out how many of them are Americans. So if that claim is not credible—and ultimately, she doesn't say it is—then NSA IG's sole remaining rationale is a manpower one.

Frankly, if it would take that much manpower to come up with an answer, it says the program isn't being tracked adequately.

Cordero then gets to the jist of a comment she made at the hearing: that there are a bunch of reviews which provide adequate oversight.

> Meanwhile, the assertion of today's program's title that the FAA enables "mass spying without accountability," is

> debunked by the SSCI's own report issued on June 7. The intelligence committees have been on the receiving end of a mountain of reports describing FAA activities, the FISA Court's reviews, and the Executive Branch's own compliance reviews. **The SSCI report, and the additional written views of Senator Feinstein** (D-CA), the Committee's Chair, states that the statutorily-mandated reporting requirements "provide the Committee with extensive visibility into the application of…minimization procedures," and have enabled the Committee to conduct "extensive" and "robust" oversight. The report goes on to detail all of the different categories of reports and briefings that have been provided to the Committee to facilitate their oversight role, in accordance with the National Security Act of 1947, as amended. [my emphasis]

Cordero claims that the SSCI report **and** DiFi's additional reviews boast about reporting requirements. But only the word "extensive" appears in the report approved by SSCI as a whole, and it appears to simply repeat language from an appendix Eric Holder and James Clapper provided. The rest comes from this paragraph:

> Third, the numerous reporting requirements outlined above provide the Committee with extensive visibility into the application of these minimization procedures and enable the Committee to evaluate the extent to which these procedures are effective in protecting the privacy and civil liberties of U.S. persons. Notably, the FISA Court, which receives many of the same reports available to the Committee, has repeatedly held that collection carried out pursuant to the Section 702 minimization procedures used by the government is reasonable under the

> Fourth Amendment.

By now you're all familiar with the paragraph. It's the one—as Cordero's own rehearsal of the language Wyden got declassified makes clear—that the now-declassified revelation that the program has been found to violate the Fourth Amendment shows to be an incomplete representation. So to make her claim that the program has been adequately reviewed, she relies on language that has been discredited.

But that's not the only thing Cordero leaves out. She rather bizarrely doesn't mention that she raised this point at the panel. Which means she doesn't have to admit that Wyden responded to her question by saying the reason he had the language declassified was **because that statement wasn't accurate**. (This exchange comes about half way through the MP3.)

> The reason that I asked to have it declassified just last week is because I believe that a lot of those statements—and I don't cast malice or ill-intent on them—were inaccurate. That there had been violations of constitutionally protected rights under the Fourth Amendment and what Director Clapper said last Friday is he agreed with me. So that's why I did it and I'm not again casting any aspersions on people's intent, I'm just stating a fact. I asked that question because so many people stated exactly what you said. I didn't think it was accurate and Director Clapper agreed with me last Friday.

And Wyden's not the only one raising concerns about whether adequate oversight has been done. Pat Leahy—who backs passing the extension—said,

> My views about the implementation of these surveillance authorities are based on the information we have available now

> — but there is more that we need to know. For example, **important compliance reviews have not yet been completed by the Inspectors General of the Department of Justice or the NSA**. And there has never been a comprehensive, independent inspector general review of FISA Amendments Act implementation that cuts across the intelligence community, and that is not confined to one particular element or agency. Without the benefit of such independent reviews, I am concerned that a five-year extension is too long. [my emphasis]

So you've got two people who know what kind of reviews have been done, one who said to Cordero to her face that the statement she relied on was inaccurate, another (who backs the extension) who said very clearly that the DOJ and NSA IGs still haven't completed some compliance reviews.

Now maybe Cordero, from her experience with FISA up until two years ago, believes it has adequate oversight. Though for all we know, that was the period when the FISA Court found the program to be violating the Fourth Amendment.

But at least some of the people tasked with overseeing it right now dispute her claims about adequate review.

Update: After reviewing the exchange, I added Wyden's comment, corrected a misspelling of Cordero's last name, and made a few other fixes.

Also note—Scott Horton, formerly of Antiwar.com, who had me on a bunch of times—is trying to go out on his own. Please follow his radio program here and, if you can afford it, consider donating to support his reporting on civil liberties.

FAA EXTENSION: THE DATA GAPS ABOUT OUR DATA COLLECTION

As I noted the other day, part of the point of the language Ron Wyden got declassified the other day seemed to be to call out a misrepresentation in Dianne Feinstein's Additional Views in the Senate Intelligence Report on the extension of the FISA Amendments Act. DiFi had claimed that "the FISA Court … has repeatedly held that collection carried out pursuant to the Section 702 minimization procedures used by the government is reasonable under the Fourth Amendment." She neglected to mention that, "on at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment."

But since Wyden pointed back to that language, I wanted to note something else in the paragraph in which DiFi's misleading claim appears: She suggests there is substantial reporting on the program.

> This oversight has included **the receipt and examination of over eight assessments and reviews per year** concerning the implementation of FAA surveillance authorities, **which by law are required to be prepared by the Attorney General, the Director of National Intelligence, the heads of various elements of the intelligence community, and the Inspectors General associated with those elements**. In addition, the Committee has received and scrutinized un- redacted copies of every classified opinion of the Foreign Intelligence Surveillance Court (FISA Court) containing a significant construction or interpretation of the

> law, as well as the pleadings submitted by the Executive Branch to the FISA Court relating to such opinions.
>
> [snip]
>
> Third, the numerous reporting requirements outlined above provide the Committee with extensive visibility into the application of these minimization procedures and enable the Committee to evaluate the extent to which these procedures are effective in protecting the privacy and civil liberties of U.S. persons. [my emphasis]

But in her sentence claiming the FISA Court keeps approving the program, she reveals that the Court is not getting all those reports.

> Notably, the FISA Court, **which receives many of the same reports available to the Committee**, has repeatedly held that collection carried out pursuant to the Section 702 minimization procedures used by the government is reasonable under the Fourth Amendment.
>
> [my emphasis]

The Court receives "many" of the same reports. Which suggests it doesn't see all of them.

That comment is all the more interesting because of something Pat Leahy said at least week's Senate Judiciary Committee mark-up of the bill.

> Congress has been provided with information related to the implementation of the FISA Amendments Act, along with related documents from the FISA Court. Based on my review of this information, and after a series of classified briefings, I do not believe that there is any evidence that the law has been abused, or that the communications of U.S. persons are being intentionally targeted.

> [snip]
>
> My views about the implementation of these surveillance authorities are based on the information we have available now – but there is more that we need to know. For example, **important compliance reviews have not yet been completed by the Inspectors General of the Department of Justice or the NSA**. And there has never been a comprehensive, independent inspector general review of FISA Amendments Act implementation that cuts across the intelligence community, and that is not confined to one particular element or agency. Without the benefit of such independent reviews, I am concerned that a five-year extension is too long. [my emphasis]

Here's what the Inspectors General are supposed to report (basically, they're supposed to make sure the government is doing what it says it is, and track some–but not the most important–US collection):

> The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General–
>
> (A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);
>
> (B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person

> identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;
>
> (C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed;

Which is interesting because, in addition to adding a general review of the FAA collection and use by the Intelligence Inspector General, Leahy's substitute amendment tweaked the language on IG reviews, as well.

In addition to requiring the IGs to count the number of targets later found to be located in the US, Leahy also required them to count how many US persons had been targeted, such that (C) would read,

> (C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be **United States persons or** located in the United States and, to the extent possible, whether communications of such targets were reviewed; [my emphasis]

More interesting still, he changes the language describing which agencies will undertake such reviews (and it's a change in language he makes elsewhere in one or two places). Rather than requiring reviews from agencies that are "authorized to acquire foreign intelligence information," he requires it from agencies "with targeting or minimization procedures approved under this section." So the introductory paragraph in this section would read,

> The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community **with targeting or minimization procedures approved under this section**, with respect to the department or element of such Inspector General– [my emphasis]

Though note, the language in paragraph C still refers to acquisitions.

This seems to suggest there are agencies (the NSA) that are authorized to acquire all this telecom traffic. And then there are agencies (FBI, intelligence agencies at DOD, DEA) that have "minimization" procedures–that is, that actually access and use the information. And Leahy's trying to make sure we get reporting from both types of agencies.

All of which seems to pertain to something Julian Sanchez wrote about here. Not only doesn't "targeting" mean what you would think it means. But minimization doesn't either.

> Communications aren't "minimized" until they're reviewed by human analysts–and given the incredible volume of NSA collection, it's unlikely that more than a small fraction of what's intercepted ever is seen by human eyes. Yet in the statements above, we have two intriguing implications: First, that "collection" and "minimization" are in some sense happening contemporaneously (otherwise how could "collection" be "pursuant to" minimization rules?) and second, that these procedures are somehow fairly intimately connected to the question of "reasonableness" under the Fourth Amendment.
>
> To make sense of this, we need to turn to the Defense Department's somewhat counterintuitive definition of "collection" for intelligence purposes.

> As the Department's procedures manual explains:
>
> > Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties…. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.
>
> This dovetails with a great deal of what we know about recent NSA surveillance, in which enormous quantities of communications are stored in a vast database codenamed Pinwale for later analysis.
>
> [snip]
>
> The language of these statements, however, would be consistent with the clever "solution" former NSA employees and whistleblowers like Bill Binney have long been telling us the agency has adopted. Referring to a massive data storage facility being constructed by NSA in Utah, Binney writes:
>
> > The sheer size of that capacity indicates that the NSA is not filtering personal electronic communications such as email before storage but is, in fact, storing all that they are collecting. The capacity of NSA's planned infrastructure far exceeds the capacity necessary for the storage of discreet, targeted communications or even for the storage of the routing information from all electronic communications. The capacity of NSA's planned infrastructure is

> > consistent, as a mathematical matter, with seizing both the routing information and the contents o all electronic communications.
>
> Binney argues that when NSA officials have denied they are engaged in broad and indiscriminate "interception" of Americans' communications, they are using that term "in a very narrow way," analogous to the technical definition of "collection" above, not counting an e-mail or call as "intercepted" until it has been reviewed by human eyes. On this theory, the entire burden of satisfying the Fourth Amendment's requirement of "reasonableness" is borne by the "minimization procedures" governing the use of the massive Pinwale database. On this theory, the constitutional "search" does not occur when all these billions of calls and emails are actually intercepted (in the ordinary sense) and recorded by the NSA, but only when the database is queried.

So here's what I take away from all this.

First, there's no requirement that the agencies track when Americans get targeted (whether overseas or in the US), which, remember, is different than Americans having their communications read as part of "minimization."

Second, it seems possible that some agencies aren't doing this kind of reporting at all, because they technically can't "acquire" but they can "minimize" (that is, acquire) contacts.

Third, the two most important agencies—NSA and FBI—have not submitted some of the compliance reviews. So, for example, we don't know whether FBI has been minimizing (that is, acquiring) contacts from Americans willy nilly.

Fourth, the FISA Court may not even see all of

what Congress sees. And even without it, the Court found the government to be violating the Fourth Amendment at least once.

Fifth, no one has ever looked at how all this fits together, how what we would call acquisition fits together with minimization (which is when the government seems to claim "acquisition" happens). Which given that it appears the end users—the people who acquire under the name of minimization—seem to be the only ones who find out if the program is picking up Americans, means we don't know how often the collection process ends up collecting on US persons.

Finally, in spite of all of these data gaps, they're just going to extend the program for another three (or probably five, after it gets through Congress) anyway.

For a bunch of elected representatives purportedly trying to make sure we get the information we need, they seem to be in a rush to renew this program without the information we need.

RON WYDEN TO DIANNE FEINSTEIN: PANTS ON FIRE

While the language about the FISA Amendments Act that Ron Wyden just got James Clapper to clear for release (first reported by Spencer Ackerman) doesn't exactly call Dianne Feinstein a liar, it comes close.

Wyden got the following three statements cleared:

- A recent unclassified report noted that **the Foreign**

> **Intelligence Surveillance Court has repeatedly held that collection carried out pursuant to the FISA Section 702 minimization procedures used by the government is reasonable under the Fourth Amendment.**
>
> - It is also true that on at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment.
> - I believe that the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion, the FISA Court has reached this same conclusion. [my emphasis]

The unclassified report in question is the Senate Intelligence Committee's report from the FISA Amendments Act extension mark-up.

> Third, the numerous reporting requirements outlined above provide the Committee with extensive visibility into the application of these minimization procedures and enable the Committee to evaluate the extent to which these procedures are effective in protecting the privacy and civil liberties of U.S. persons. Notably, **the FISA Court,** which

> receives many of the same reports available to the Committee, **has repeatedly held that collection carried out pursuant to the Section 702 minimization procedures used by the government is reasonable under the Fourth Amendment**. [my emphasis]

The passage in question comes from DiFi's additional views.

With this declassified language, Wyden is making clear how incomplete DiFi's claims about the law are.

But don't worry, James Clapper's office says. They've rectified the problems. Of NSA violating minimization requirements, that is, not of the Senate Intelligence Committee Chair making grossly misleading comments to push for passage of the extension.