Senate Committee on the Judiciary

"Strengthening Privacy Rights and National Security:

Oversight of FISA Surveillance Programs"

July 31, 2013

Questions for the Record from Ranking Member Charles E. Grassley

Stewart Baker, Steptoe & Johnson

Question:

Would ending the collection of telephone metadata in bulk under Section 215 – and instead requiring the government to show a link to a foreign power or agent thereof with respect to every record collected -- affect the government's ability to protect national security by "connecting the dots" of terrorist plots? Why or why not?

Response:

This is really a question that the government is in the best position to answer. According to declassified documents, the government, as recently as in 2011, believed that bulk collection of metadata under Section 215 is necessary to locate terrorists in the United States. Apparently, this information would have helped the government find one of the 9/11 hijackers, who was making calls to Yemen from San Diego. There is no reason to believe that the conditions that caused the government to take this position in 2011 have changed. So unless we plan to repeat the errors of 9/11 – by imposing artificial barriers on the government's ability to use information to keep us safe – my view is that we should continue to allow bulk collection.

Question:

Some have suggested that phone companies could be required to retain the telephone metadata for later searching by the government. Is this a practical alternative to the current program? How, if at all, would the government's ability to protect national security and the privacy interests of the public be affected by this potential change?

Response:

This proposal simply isn't practical for a number of reasons. The first problem with it is that if phone carriers retain the data, the government will be required to tell companies the telephone numbers it is worried about in order to conduct searches. This in itself increases the risk that these programs will be compromised as more actors get in involved with them. Moreover, some telecom providers are foreign-owned. Sharing the searches that the government wishes to conduct with those companies will certainly be less secure.

A second problem with leaving the data in the hands of private companies is that it complicates the process of searching it. The government would no longer be able to conduct searches of data that spans carriers. It would likely need to conduct more searches across more databases in order to obtain the same results. And it would need to find a way to fold all of the data together. This would be a complex and expensive IT problem.

Concerns about cost also apply to the actual storage of the data. If the government is going to require telecom companies to retain their metadata and periodically search it, the government will have to pay for it. Paying for the data to be held and searched by multiple companies in separate storage databases will impose a far greater cost on the government than simply holding it in one place.

Of course, overcoming all of these problems may be worthwhile if having private companies retain the data offered some real benefits for privacy and civil liberties. But it's hard to say what the benefits of this proposal would be. True, under this proposal the government wouldn't actually possess the metadata in question, but it would still be able to search it.

Further, there is no reason to believe that leaving metadata in the hands of private companies will prevent abuse. One thing we can say for certain is that when the government holds the data there are numerous oversight mechanisms, including Congress, the FISA Court, and numerous executive offices

Question:

Has the one-year ban on challenging non-disclosure orders under Section 215 played a role in protecting national security? If so, how? How, if at all, would the government's ability to protect national security and the privacy interests of the public be affected if this ban were repealed? Would repealing this ban help strike the correct balance between privacy and national security? Why or why not?

Response:

I do not have sufficient information to address this question.

Question:

Would the government's annual disclosure to the public of the following information related to Section 215 and 702 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

(a) How many FISA court orders were issued;
(b) How many individuals' (foreign and U.S. persons) information was collected;

(c) How many U.S. persons' information was collected; and
(d) How many U.S. persons' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were both collected and queried.

Response:

This question is quite similar to the question of whether to declassify the annual intelligence budget. People who are already suspicious of the Intelligence Community want this information published. One suggested response is to just publish the topline numbers. But the Intelligence Community rightly points out that just issuing the topline numbers will only lead to more questions and more speculation.

At first blush, the argument that more transparency will make us more comfortable seems compelling. But for national security reasons, we're never ever going to be able to be fully transparent about our FISA activities. Moreover, simply providing numbers in isolation may not communicate meaningful information. It's hard for most of us to really know what constitutes a large or troubling number of FISA court orders. Is a hundred a lot? What about a thousand? Ten thousand? In the absence of complete information, additional data is more likely to be used by people that have already made up their mind to attack the Intelligence Community than it is to make people comfortable with the IC's actions.

Question:

Would the government's annual disclosure to the public of the following information related to Section 105, 703, and 704 authorities be possible as a practical matter, and would it affect the government's ability to protect national security? Why or why not? Would making such disclosures help strike the correct balance between privacy and national security? Why or why not?

(a) How many FISA court orders were issued;
(b) How many individuals' (foreign and U.S. persons) information was collected; and
(c) How many U.S. persons' information was collected.

Response:

See my response above.

Question:

Would disclosure by companies served with FISA orders under Sections 215 and 702 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

(a) How many FISA court orders the company received;
(b) The percentage of those orders the company complied with;
(c) How many of their users' information they produced; and
(d) How many of their users' electronic communication contents and metadata, wire communications contents and metadata, and subscriber records were produced.

Response:

Allowing companies to disclose this information poses a risk to our national security. The more detail you release regarding individual companies, the more information you provide to terrorists about which companies to avoid. There's no question that foreign intelligence organizations and terrorist groups are right now analyzing the data that has already been leaked to strengthen their own counterintelligence tactics. Providing company-specific data will only increase the problem.

Question:

Would disclosure by companies served with FISA orders under Sections 105, 703, and 704 of the following information to the public affect the government's ability to protect national security? Why or why not? Would permitting such disclosures help strike the correct balance between privacy and national security? Why or why not?

(a) How many FISA court orders the company received;
(b) The percentage of those orders the company complied with; and
(c) How many of their users' information they produced.

Response:

See my response above.

Question:

When the government makes an application to a court for a wiretap or a search warrant in a typical criminal case, the target is not represented before the court. In contrast, would the appointment of a permanent office of independent attorneys tasked with reviewing all of the government's applications before the FISC and advocating against the government help strike the correct balance between privacy and national security? What about providing FISC judges the ad-hoc ability to seek the advice of an independent attorney to address rare, novel questions of law? Why or why not?

Response:

Setting up an independent office to advocate against the government before the FISC is a bad idea, both for the FISC as an institution and for the cause of privacy. Putting in place a

permanent advocate for privacy would turn the FISC proceedings adversarial and force the government to take sides against privacy protection.

This is not how the process works now. Contrary to many of the criticisms that have been circulating, the government largely pulls its punches today. The Department of Justice already sees itself as responsible for balancing privacy and security. The Office of Intelligence at the DOJ plays a role closer to umpire than advocate.

Staff attorneys at the FISC also play a significant role in protecting privacy rights. They're responsible for reviewing FISA warrant applications before they reach the desk of FISC judges. This involves both working with the government to ensure that the requested warrant complies with FISA as well as the US Constitution and providing recommendations to the Court.

If we decide to make the FISC process adversarial, by setting up an independent office to advocate for privacy, then it will necessarily change the FISC process in other ways. The government should no longer be required to pull its punches. It would necessarily have to advocate for its right to catch terrorists, and this would likely weaken internal oversight by agencies like the Office of Intelligence.

I believe that it is a fundamentally bad idea to rely on the FISA court in the way we now do. And loading the court up with more judicial trappings will only heighten the contradiction between the quasi-managerial oversight role it has assumed and the job that judges ordinarily do. I see signs that the court is already allowing its legal judgment to be warped in ways unfavorable to intelligence gathering by the role it has been given. I covered this point in more detail in a recent article on Skating on Stilts concerning the claim by Judge Walton of the FISA court that NSA had engaged in misrepresentations to him. Stewart A. Baker, *FISA: The Uncanny Valley of Article III?*, Skating on Stilts (Sept. 11, 2013, 12:19 AM), http://www.skatingonstilts.com/. It is excerpted below:

> There's an old saying that megalomania is an occupational hazard for district court judges. While Chief Judge Walton's opinion doesn't quite succumb to megalomania, there is a distinct lack of perspective in his approach that makes me wonder whether the FISA job slowly distorts a judge's perspective in unhealthy ways.
>
> That was certainly true of Judge Lamberth, who spent most of 2001 persecuting a well-regarded FBI agent for not observing the "wall" between law enforcement and intelligence. That's the wall that the court of appeals found to be utterly without a basis in law but that Chief Judge Lamberth nonetheless enforced with an iron hand. Judge Lamberth forced FISA applicants to swear an oath that they were observing the wall, a tactic that allowed him to sanction the applicants for misrepresentation if they didn't live up to his expectations. He was so aggressive in this pursuit that he had sidelined the most effective FBI counterterrorism teams

in August of 2001. The bureau knew by then that al Qaeda had terrorists in the United States but it couldn't use its best assets to find them them because Judge Lamberth had made it clear that he was willing to wreck their careers if they breached the wall.

I fear that Chief Judge Walton is going down the same road -- that the FISA court is the only agency of government not humbled by its failures on the road to 9/11 and is therefore the only agency that will repeat those failures. My concerns are best illustrated by the court's opinion of March 2, 2009, about which I offer three thoughts:

1. In much covered language, the judge claims that the government engaged in "misrepresentations" to the court. This is one of the three alleged misrepresentations mentioned by Chief Judge Bates in an opinion released last month. Since that opinion was released, commentators have widely assumed that NSA has been lying to the court. Because, frankly, that's what "misrepresentation" usually means. But the other filings declassified today show pretty persuasively that there was no intentional misrepresentation. Here's what seems to have happened, in brief. Back in 2006, scrambling to write procedures for the metadata program, a lawyer in NSA's Office of General Counsel wrote in a draft filing that a certain dataset of phone numbers always met the "reasonable articulable suspicion" standard. Turns out that that wasn't true; only some of the numbers did. The lawyer circulated his draft for comment, suggesting that he wasn't absolutely sure of his facts, but no one flagged the error, which turned out to be surprisingly difficult to verify. From then on, NSA and Justice simply copied the original error, over and over, all of their submissions. A mistake for sure. But a "material misrepresentation"? Only to a judge with a very warped view of the world, and the NSA.

2. How about the other headline-grabbing statement in the opinion, that the government's position "strained credulity"? Here, I think the court is on even shakier ground. The debate is about the court's minimization order, which declared that "any search or analysis of the [phone metadata] archive" must adhere to certain procedures. NSA dutifully imposed those procedures on analysts' ability to search or analyze the archive. The problem arose not from giving analysts access to the archive but from some pre-processing NSA performed as the data was flowing into the archive.

If I'm reading the filings properly (and I confess to some uncertainty on this point), NSA keeps an "alert" list of terror-related phone numbers of interest to individual analysts. Since new data shows up at NSA every day, the agency has automated the job of scanning to find those numbers as they show up in the

agency's daily take. The numbers on the alert list are compared to the day's incoming intercept data, and each analyst gets a report telling him how many times "his" numbers appear in which databases.

This alert list was run against data bound for the telephone metadata along with all the other incoming data. The difference was that an analyst who got a "hit" on that database couldn't access it without jumping through the hoops already set up by the FISA court -- reasonable articulable suspicion, special procedures, etc. This must have seemed quite reasonable to the techies at NSA. They knew what it meant for an analyst to "access" the database, and an automated scanning system that yielded only pointers was not the same as giving an analyst access. In the end NSA's office of general counsel came to the same conclusion: the court's orders regulated actual archive access, not scanning against a list for statistics and pointers.

But that's not how Chief Judge Walton saw it. He held that it "strained credulity" to say that alert list scanning was different from "accessing" the archive. Maybe he just didn't understand the technology (the opinion offers some reason to think that). Or maybe he just thought about the question like a judge, always alert to slippery slopes and unintended consequences: "If you can lawfully search this data without limit before the data gets into the archive, you will make meaningless all the limits I've set. Why would you think I'd let you undermine my order in so transparent a way?"

Unfortunately, Judge Walton wasn't thinking like a techie. The techies who implemented the court's order thought they'd been told to restrict access to the database, and they did. They weren't told to restrict the use of statistical tools that scanned incoming data automatically, so they didn't. They certainly didn't believe they were undermining the court's order. Quite the contrary, they had designed the system to make sure that the alert list was just a starting point. Analysts who learned they had a hit in the database couldn't get any further information without meeting the FISA court's "reasonable articulable suspicion" requirement.

It's hard not to see this as a misunderstanding, perhaps exacerbated by the difference between legal and technical cultures. But that's not how Judge Walton sees it. His opinion dismisses the possibility that this could possibly be a good-faith misunderstanding. It's an outrage, he fumes, and efforts to explain it "strain credulity." Frankly, if anything strains credulity in this case, it's that line in the opinion.

3. The chief judge is so sure there's evil afoot that he calls for briefing on "whether the Court should take action regarding persons responsible for any

misrepresentations to the Court or violations of its Orders, either through its contempt powers or by referral to appropriate investigative agencies." For anyone steeped in the disaster caused by Chief Judge Lamberth's witch-hunt for violators of the wall, this is tragically familiar ground. It's almost exactly how the FISA court drove the wall deep into the FBI.

I'm sure we'll be told by the press that this opinion brings to light another scandal and an agency out of control. But that's not how I see it. It looks to me as though NSA was doing its best to implement a set of legal concepts in a remarkably complex network. All complex systems have bugs, and sometimes you only find them when they fail. NSA found a bug and reported it, thinking that it was one more thing to fix. Then the roof fell in.

The interesting question is why it fell in. I think a fair-minded judge encountering the issue for the first time in the courtroom would not likely say that NSA's interpretations were disingenous or the result of bad faith or misrepresentation. Yet Judge Walton went there from the start.

I suspect that it's because we've unfairly given FISA judges a role akin to a school desegregation master -- more administrator than judge. Instead of resolving a setpiece dispute and moving on, FISA judges are dragged into a long series of linked encounters with the agency. In ordinary litigation, the judges misunderstand things all the time and reach decisions anyway, and they rarely discover all that they've misunderstood. The repetitive nature of the FISA court's contacts with the agency mean that they're always discovering that they only half understood things the last time around. It's only human to put the blame for that on somebody else. And so the judges' tempers get shorter and shorter, the presumption of agency good faith gets more and more frayed. Meanwhile, judges who are used to adulation, or at least respect, from the outside world, keep reading in the press that they are mere "rubber stamps" who should show some spine already. Sooner or later, it all comes together in a classic district judge meltdown, with sanctions, harsh words, and bad law all around.

If I'm right about the all too human frailties that beset the FISA court, building yet more quasijudicial, quasimanagerial oversight structures is precisely the wrong prescription. We'll be forcing judges to expand into a role they are utterly unsuited for and we'll put at risk our ability to actually collect intelligence. In fact, the more adversarial and court-like we make the system, the more weird and disorienting it will become for the judges, who will surely understand that at bottom they are being asked to be managers, not judges.

The further we go down the road, the more likely we are to turn FISA into the Uncanny Valley of Article III.

Question:

In your experience, are there institutional checks and safeguards in place that ensure that the FISC hears both sides of an issue, and not just the government's? If so, what are they and how do they work?

Response:

Yes. As explained above, the FISA warrant process contains a number of safeguards that I believe appropriately protect privacy interests.

Question:

In your experience, is there a difference in the way Republican-appointed judges on the FISC have discharged their duties, as compared with Democrat-appointed judges? If so, what is that difference?

Response:

In my experience, Democratic appointees to the FISC are indistinguishable from Republican appointees. The presiding judge of the FISC when I was dealing with it as the General Counsel of NSA was appointed by President Carter. The Court during that time was completely fair, and I did not find her or the rest of the court particularly hostile to the Intelligence Community.

The presiding judge that followed was a Republican appointee. During his tenure, the FISC imposed the wall between law enforcement and intelligence activities that I believe was largely responsible for the intelligence failures that led to 9/11 and that I discuss in more detail above. Thus, the most aggressive – and in my view improper -- use of FISA to limit the powers of the Intelligence Community occurred under a Republican appointee.

Question:

Are there any specific reforms to the current law and practice that you would suggest to help ensure that any data the government collects from the 215 and 702 programs is accessed and used only as the law or a court permits?

Response:

One possible area for reform is the obligation to report crimes identified as a result of intelligence programs. This is not an obligation that bears on national security. It is an additional requirement imposed by the DOJ based on the wishes of prosecutors. To the extent that intelligence efforts are being compromised by doubts that information obtained will be used

for prosecutions, additional safeguards are appropriate and unlikely to damage our national security.

Question:

To what extent, if any, can more information about FISA opinions be disclosed to the public without compromising the protection of national security?

Response:

It is hard to know with certainty, but there is little question that the FISA opinions that have been disclosed have promoted speculation and provided information about the functioning of programs that likely has compromised our national security. The recent decision by the Director of National Intelligence to declassify certain FISC opinions should not be read as indicating that there is no risk to declassification. It simply indicates that the damage being done by the current controversy was deemed to be greater than harm created by disclosure. I would therefore advise caution about further disclosures.