23rd Annual Review of the Field of National Security Law

Executive Updates on Developments in National Security Law

Panel: Privacy, Technology and National Security: An Overview of Intelligence Collection

As Prepared Remarks of Robert S. Litt

General Counsel for the Office of the Director of National Intelligence

October 31, 2013

Not surprisingly, the two major issues that have been occupying my time recently have been budget issues and the fallout from the Snowden leaks.

I spent the first part of October working almost entirely alone in our office, supported just by my deputy, advising on who was allowed to work and what they were allowed to do.

And also responding to inquiries from people who did not seem to comprehend that when (a) Congress prohibits personnel from working when they aren't paid, and (b) the Intelligence Community isn't appropriated funds to pay personnel, then (c) most IC personnel won't be able to work.

But even before the shutdown, the Intelligence Community was feeling the pinch of sequestration.

We recognize that in the current budgetary environment, the IC, along with the rest of the government, will have to endure some cuts. The problem with sequestration is that, rather than allowing us to make cuts in a sensible manner, based on mission needs, it requires us to cut everything across the board.

We were able to deal with sequestration in the past year by delaying or deferring some activities and reprogramming funds to cover critical gaps.

But this fiscal year, sequestration will require another round of cuts, and we won't have the same flexibility to deal with them.

Instead of short-term delays or creative mitigation strategies, we will be forced to cut capabilities

Instead of determining what capabilities we need to keep the country safe, we will be forced to determine what capabilities we can afford to provide.

The impact of sequestration will likely open new intelligence gaps and prevent us from mitigating existing ones.

So we are hopeful that the Congress will find a way to avoid sequestration for this year, though we recognize that that is by no means a certain outcome.

Obviously, however, since June the bulk of my time has been spent dealing with leaks about our surveillance activities.

I want to address a couple of big picture issues about this topic.

For one thing, I'd like to provide a sort of "user's guide" for people who follow this in the press.

Begin with the proposition that you shouldn't believe everything you read or hear, and I mean that literally.

The media reports are often based on documents that are exceptionally complicated, dense and jargonized, and require a level of technical knowledge that most people, including me, don't have. And the documents often present only part of the story.

On top of that, even when reporters come to us for comment – and they don't always – we frequently cannot correct their mistakes without compromising sensitive sources and methods.

A good example of what I am talking about is the story last week that claimed that we had collected 70 million French telephone calls in a month.

That was simply untrue, because the reporter didn't understand what he was looking at. As has now been made public, these 70 million calls were in fact collected by the French intelligence service, outside of France, in furtherance of mutual counterterrorism and force protection concerns, and provided by the French intelligence service to us.

But until the truth was leaked to the Wall Street Journal, we couldn't correct this publicly, to avoid damaging sensitive intelligence relationships. That's the kind of problem we face.

Second, a lot of these stories have focused on the raw technical capabilities of the U.S. intelligence community. And yes, those capabilities are considerable. But it is important to differentiate between technical capability and actual practice – between what might be done and what is actually done – between what we can do technically and what we can do legally.

For example, there have been stories claiming that NSA is able to crack encryption or break into private networks, and charges that this compromises everyone's privacy.

I'm not going to comment on whether or not these stories were accurate.

But isn't cracking encryption, or breaking into private networks, exactly what we want an intelligence agency to be able to do?

How else are we going to collect the communications of people who want to harm us and our allies, and who use those tools to try to hide their communications, or to provide policy makers the intelligence they need to protect the nation?

But just because we try to develop the capability to intercept and decrypt communications of adversaries and terrorists does not mean that we can or do use those capabilities against ordinary U.S. citizens, or French citizens, or Belgians, etc.

Our intelligence agencies are the best in the world, but – and this is the key point – they only conduct surveillance to the extent they are allowed to by the law, and that includes that they do not target the communications of Americans except as specifically authorized by the law, and cannot target foreigners except for a valid foreign intelligence purpose.

And this leads to another big picture point. Everything that has been exposed so far has been done within the law.

We get court orders when we are required to, we minimize information about U.S. persons as we are required to, we collect intelligence for valid foreign intelligence purposes as we are required to.

And, unlike many other countries which engage in the same types of collection activities, our intelligence services are subject to multi-layered oversight, which includes oversight by Executive agencies, Congress and judicial authorities. As you have seen in FISA Court documents, that oversight is not pro forma. Errors are reported. Independent fact finding is conducted. Hearings are held and remedies are imposed. Congress is briefed.

We also have extensive technical systems that help us ensure that the rules are complied with.

Even though we aren't always perfect – even though technical and human failures can lead to compliance problems – nothing has come out that indicates that there has been any intentional abuse of our surveillance capabilities.

This is a far cry from, say, the illegal domestic surveillance of the 1960s and 1970s.

I recognize that there are people who believe that the law should be different, and they have advocated that position forcefully.

But – for example – the bulk telephony metadata program has been conducted pursuant to over 30 court orders by over a dozen separate judges.

The last two renewals were after the public controversy erupted, and in the face of all of the arguments that have been made against the program.

If the law changes, we'll follow the new law; but for now, we'll follow the law as Congress passed it and the courts interpret it.

Finally, I want to talk about the implications of the last few months for how we authorize and oversee classified intelligence activities.

These disclosures have started a public debate about the appropriate scope of surveillance.

But this debate comes with a cost, and the cost is that to the extent we are exposing what our intelligence agencies can do, we make it harder for them to do it. What the Washington Post reports, al Qaeda knows.

For over thirty years, we've had a consensus about how to balance the need for secrecy in intelligence programs with the need for oversight of those programs.

We did this through the congressional intelligence committees, which were set up precisely for this purpose. We are required by law to keep them fully and currently informed about all intelligence activities, and we do.

The committees have stood as proxies for the American people, to avoid the harm to our national security that would come from full public disclosure of our activities, while ensuring that elected representatives of the people oversee those activities.

The last few months have provided a different model of oversight – one in which private individuals, without visibility into or responsibility for protecting the nation, are making their own judgments about what should and should not be disclosed, and one in which the general public is debating what our intelligence agencies should and should not do.

Some might argue that there are benefits from this approach. It provides more transparency for the public and allows public debate about matters that typically have been kept secret.

But I want to end with two important issues that we need to think about.

One is – is oversight by the committee of the whole really the optimal way to conduct intelligence oversight? Or will the costs to our national security outweigh the benefits of disclosure?

And the second is that the intelligence community must acknowledge how difficult it is to keep secrets today. In determining what activities to undertake we need to give more consideration to what the impact of additional leaks would be. In each case we have to assess, to a greater extent than we have to date – is the game worth the candle?

The President has directed a review of our intelligence programs, in part with this issue in mind, and I think that that review, and any follow on actions, are certainly going to be occupying my time in the next year.

###