



**Keynote Remarks as Prepared for Delivery:
Mr. Robert S. Litt, General Counsel, ODNI**

**American University Washington College of Law:
Freedom of Information Day Celebration**

**Location: Washington College of Law,
4801 Massachusetts Avenue, NW, Washington, D.C.
Room 603**

Date: March 18, 2014

Time: 12:30 p.m.

Thank you, Dan, for that generous introduction, and for inviting me to speak here today.

As you know, this is “Sunshine Week,” a national initiative to promote dialogue about the importance of open government and freedom of information. Public knowledge about the activities of government is essential to a free and democratic society, and so on his first full day in office President Obama, who has noted our “profound national commitment to ensuring an open government,” called upon the entire government to comply with both the letter and the spirit of the Freedom of Information Act. Today I would like to talk to you about the challenges of reconciling that commitment with the secrecy necessary to conduct effective intelligence operations in defense of our national interests.

You may have noticed that the issue of transparency of intelligence activities has been in the news a lot lately. I want to make very clear that Edward Snowden’s criminal leaks have seriously damaged our national security. The articles that have appeared have compromised specific and lawful intelligence collection capabilities, and we know that our enemies are taking

note of these disclosures. Only time will tell the extent of the damage, and even then, we may never know what information has escaped us because these articles have helped our adversaries evade our surveillance.

But these leaks have forced the Intelligence Community to rethink our approach to transparency and secrecy. We have had to reassess how we strike the balance between the need to keep secret the sensitive sources, methods and targets of our intelligence activities, and the goal of transparency with the American people about the rules and policies governing those activities, in an era where the half-life of a secret is not what it used to be, and where a 29-year-old systems administrator has the ability to compromise major collection activities. In the last 8 months, we have declassified thousands of pages of formerly classified documents, including significant opinions of the Foreign Intelligence Surveillance Court and some of the internal policies and procedures showing how we limit and oversee our intelligence collection activities. We have made speeches and testified publicly in Congress about intelligence activities, to an extent that would have been unthinkable a year ago. We've set up a tumblr website – not that I really understand what a tumblr is – on which we post for the public what we have released. The President has directed that this transparency continue, and it will. This is something that I am personally involved in and personally committed to.

One lesson that I have drawn from the recent events – and it is a lesson that others including the Director of National Intelligence have drawn as well – is that we would likely have suffered less damage from the leaks had we been more forthcoming about some of our activities, and particularly about the policies and decisions behind those activities. Going forward, I believe that the Intelligence Community is going to need to be much more forward-leaning in

what we tell the American people about what we do. We need to scrutinize more closely what truly needs to be classified in order to protect what needs to be protected. And we need to move beyond the mindset of merely reacting to formal requests that we make information public, to a mindset of proactively making available as much information as we can, consistent with the need to protect sources and methods.

This is, of course, a huge challenge for the Intelligence Community. Intelligence must by its very nature be conducted in secret in order to be effective. We simply cannot advertise what we are collecting, who we are collecting from and how we collect it without compromising our ability to protect the nation. Every intelligence officer understands the need for secrecy, and I think that that is part of the reason that we all have such a visceral, almost personal dismay that one of us decided to take it upon himself to violate his oath, break the law, and endanger our operations.

At the same time, the nature of the intelligence business, the need for secrecy, and the potential for abuse, all mean that there must be strong and credible oversight of intelligence activities. And in fact, contrary to the public impression, the Intelligence Community does not operate unchecked and unexamined. Since the 1970s, when the Church and Pike Committees exposed *genuine* abuses by intelligence agencies, our political system has chosen to reconcile the competing needs of secrecy and transparency primarily through the select committees on intelligence of the House and Senate. By law, we are required to keep these committees fully and currently informed of intelligence activities, and we do. We provide them dozens of written notifications each month, and dozens more briefings, covering the full range of activities from covert actions, to satellite construction, to the most recent information about the state of affairs in

Ukraine or Syria, and including our intelligence collection programs. And make no mistake – the Intelligence Committees knew about the collection programs that have been exposed. Much of this oversight necessarily takes place in a classified format, but the Intelligence Community takes its obligations to these committees very seriously.

Of course, in addition to Congressional oversight, there is oversight within the Executive Branch and from the judiciary, by Inspectors General, General Counsels, Privacy and Civil Liberties Officers, the Department of Justice and the Foreign Intelligence Surveillance Court. But in effect, we as a society have determined that the Intelligence Committees will act as the people's primary authorized agents and representatives, and the Intelligence Community is transparent with them on the people's behalf. In my view, this accommodation between oversight and transparency is an appropriate one. Intelligence is a complicated business and one that must be kept isolated from partisan political pressures. The Intelligence Committees, with their tradition of nonpartisanship and their experienced and knowledgeable staff, have been pretty good at that.

In the wake of Snowden's leaks, however, this oversight structure has been called into question, with demands for much greater disclosure of information about collection programs directly to the public than has been the norm in the past. The entire political solution to oversight of intelligence activities – to the balance of transparency and secrecy – has been reopened.

I've spoken elsewhere about my views on changes in Congressional, judicial and executive branch oversight, so today, and because it is Freedom of Information Day, I will focus on disclosure to the public. And I want to emphasize that these are my own thoughts, and don't

necessarily represent the views of the DNI, the Intelligence Community or the Administration as a whole, but I hope that they will provoke some thought.

Over the past few months, as I said earlier, we have made significant strides in providing public insight into activities of the Intelligence Community. The process of reviewing documents for release was under way even before the leaks began, and appropriately so. But reviewing a classified document to determine what can be released consistent with national security is a complicated task, and I must admit that in this instance, the illegal disclosure of these programs affected the balance between transparency and national security. Even apart from the impact of these leaks, we are continuing to review additional documents for release, in the interest of providing as much transparency into intelligence activities as we can consistent with national security. Greater disclosure to the public is necessary to restore the American people's trust that intelligence activities are not only lawful and important to protecting our national security, but that they are appropriate and proportional in light of the privacy interests at stake. In the long run, our ability to protect the public requires that we have the public's support.

But lines must be drawn. First and foremost, we cannot allow transparency to compromise our sources and methods. We must continue to protect the specific targets of our intelligence collection, the specific methods by which we accomplish that collection, and the specifics of the intelligence we collect. Were we to announce to the world that we have the ability, for example, to intercept emails sent using particular email services, we would help terrorists, cyber criminals, foreign intelligence officers and other foreign intelligence targets communicate without fear of detection. We may never know what we are missing until it is too late. We can be, and we will be, more transparent about how we interpret certain laws to support

our activities, the procedures and oversight we have in place to ensure that our intelligence activities are appropriate, and the degree to which we have followed the law and our policies, but if intelligence is too transparent it is useless or worse.

In particular, I think that greater transparency about our processes could help us cope with one of the principal failings I see in the current public discussion, which is the failure to distinguish among what the Intelligence Community can do *technically*, what it can do *legally* and what it actually *does* do. Too much of the recent discussion has focused on technical capabilities – which are often fascinating and, quite frankly, amazing – while leaving a misleading impression of actual activities.

For example, there have been press reports that NSA has engaged in a concerted effort to break encryption. Without commenting on the accuracy of any particular story . . . isn't that exactly what intelligence agencies have historically done, and what they are supposed to do? We know that our enemies use encryption and other techniques precisely to avoid surveillance; NSA's job is to figure out how to break those techniques, and its capabilities are unmatched. But saying that NSA can break encryption is different from saying that they routinely spy on encrypted conversations of ordinary Americans or foreigners. They don't. All of NSA's technical expertise is brought to bear in furtherance of its authorized foreign intelligence mission and within the law. But we have learned how difficult it is to rebut these mischaracterizations when the basic procedural framework that makes clear what the limits are and how those limits are enforced is being wholly shielded from public view.

And this leads to the other question I want to raise about transparency, which is, Who is responsible for deciding what should be secret and what should be public? Decisions about what

can be disclosed consistent with the national interest require an appreciation of both sides of the equation: both the value of transparency and the value of secrecy. In my opinion, we cannot survive as a nation if we let those decisions be made by individuals who do not have adequate insight into the implications of their actions. The compromise of intelligence capabilities can result in the waste of millions of dollars, in an inability to give our policymakers the warning that they need to deal appropriately with threats, or, in the worst case, to the loss of lives. That's why we go through a careful, thorough, deliberative process before we disclose classified information, to ensure that we do not endanger capabilities or lives.

But leakers disrupt this process by taking it upon themselves to decide what should and should not be withheld from public view. They do this without understanding the context for the information that they release, and in willful disregard for the sensitive sources and methods that they are placing in harm's way. In short, leakers believe that they know more than everyone else, including the legislative and judicial branches of government that have continually endorsed the principle of classification for national security reasons.

Individuals in the Intelligence Community who want to blow the whistle on genuine waste, fraud, and abuse or illegality should do so. We expect and require our people to report when they believe the law isn't being followed, or when activities violate our internal procedures and guidelines. We have also established procedures that ensure that members of the Intelligence Community can raise such concerns with the appropriate authorities, including Congress, without risking harm to our national security, and without facing reprisals for their disclosures.

But what's most striking to me about the leaks that have taken place over the past few months is that they've really not been about whistleblowing at all. None of the leaks has shown that the government was engaged in any willful violation of law; even those who disagree with some of the legal analysis supporting our activities must acknowledge that they were found legal and were authorized by numerous different judges of the FISA Court, the Department of Justice and the lawyers in the Intelligence Community. None of the leaks has shown that the Intelligence Community was doing things that were hidden from the Congress or the courts. Instead, the leakers' argument appears to be that the Intelligence Community was engaging in behavior that *they* disagreed with as a matter of policy.

But now I can circle back to today's topic – freedom of information – because I strongly believe that the best way to prevent the damage that leakers can cause is by increased transparency on our part. Transparency can both lessen the incentive for disaffected employees to disclose our activities improperly, and provide the public appropriate context to evaluate leaks when they occur. But even when we are fully committed to the idea of transparency, we still face significant challenges in implementing it, and I want to talk about two of them now: overclassification and resources.

As we all know, one exemption from disclosure under the Freedom of Information Act is for matters that are “specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy, and are in fact properly classified pursuant to such Executive order.” This exemption is critical to our ability to protect the nation and must be maintained. I think that the next panel is discussing it in detail.

At the same time, there is no question that overclassification of information is a genuine problem. But I think it is important to understand the reasons for overclassification. I have been in my job as General Counsel for over five years now. I am what we call an “original classification authority,” which means that I am authorized to make an initial determination that certain information is classified. I’ve never exercised that authority, but every week I derivatively classify dozens or hundreds of documents, emails or memos, based on other people’s determinations. And I’ve participated in lots of deliberations about classification and declassification, so I have some experience in this area.

I think it is completely incorrect to suggest that the problem of overclassification results primarily, or even in any substantial part, from a desire to prevent embarrassment or for political reasons. I have never seen that to be a factor. I think that the reasons why too much information gets classified are much more mundane.

First, and most important, is a culture that places a high premium on protecting information and stresses the negative consequences that can – and do – flow from the improper disclosure of information. We are trained to protect information, to guard against improper disclosures, and to recognize counterintelligence risks. It’s part of our culture. But classification is, in effect, a risk analysis. It’s often difficult to say that an identifiable adverse consequence WILL occur if a particular piece of information is disclosed; you are always worried about the possibility of what MIGHT occur. To make a somewhat unexpected analogy, not every drunk driver causes a fatal accident, but we ban drunk driving because it increases the risk of accidents. In the same way, we classify information because of the risk of harm, even if no harm actually can be shown in the end from any particular disclosure.

Related to this is the concept of a “mosaic” of information – that one bit of information that may seem innocuous in itself could be combined with other information to compromise important national security equities. This is a concept well understood by those in the Intelligence Community; indeed the ability to pull together information in this way is one of the hallmarks of a first-rate intelligence analyst. We are always concerned that if we release one bit of information, it will lead to other bits of information, and that pulling on a single thread will ultimately unravel the entire sweater.

I believe that this risk aversion is the primary reason that people in the Intelligence Community lean towards classifying information rather than not classifying it. No one wants to risk being the person who is responsible for unmasking a clandestine human asset, or for compromising a collection capability.

The other major reason for overclassification, in my view, is bureaucratic inertia. I mentioned above the concept of derivative classification. That’s when you classify a document because it is based on material that someone else has already classified, and it is how the great majority of documents are classified. When we are talking about finished intelligence products, or legal memos that my office prepares, or similar formal documents, we go through the classification process pretty carefully, and make conscious decisions about classification on a line by line basis. But an awful lot of business today takes place via email – I send or receive several hundred emails each day – and I think it is fair to say that the classification process is not – and as a practical matter cannot be – followed as strictly in that context. People apply broad heuristics – for example, an email that relates to a top secret collection program is likely to be classified top secret, without assessing the specific damage that could be caused by disclosure of

the particular statements made in that email. There's nothing corrupt or wicked about that; it's simply a practical consequence of the amount of information we deal with on a daily basis, and by and large, in my experience, it works pretty well.

So how do we deal with the problem of overclassification? I think that there are three principal steps we can take. The first is to change the culture. We need high-level management emphasis on the problem of overclassification. We need to provide better training of both original and derivative classifiers that explains the importance of transparency as well as of secrecy. We should consider making proper attention to classification part of employees' performance evaluations. We must continue to ensure that secrets are protected, but we need equally to ensure that *only* secrets are protected.

Second, we need to continue our efforts at proactive transparency – at reviewing information that we have historically protected to see whether, in fact, the overall public interest would better be served by releasing the information.

Finally, I think that those in the agencies who are responsible for responding to FOIA requests, and who are representing the government in FOIA litigation, need to look critically at all potentially responsive documents that are classified. We must continue to vigorously defend the withholding of classified documents when it is justified, but we need also to look carefully at documents to see whether, in fact, they should be withheld. We should focus not on whether we can protect information, but whether we should.

But this brings up the other challenge we face with increased transparency, which is resources. Since last June, the Intelligence Community has been inundated with requests for

documents, both from individuals seeking records on themselves and from media and public interest group requesters seeking to leverage authorized and unauthorized disclosures to request additional records. Let me give you a few sobering statistics. In 2012, NSA received 1,809 FOIA requests; in 2013, it received 4,328.

Even more dramatically, during the first two months of 2013, before the leaks began, NSA received 157 FOIA requests; during the first two months of 2014, it received 682 requests, more than four times as many. All in all, since the leaks began last June, NSA has received nearly 5,000 FOIA requests, many of which are voluminous in nature. Other Intelligence Community agencies are also seeing an increase in FOIA requests. For example, our requests at the ODNI are up by 45%.

The task of responding to these FOIA requests is daunting. It involves not only those who are directly responsible for FOIA responses, but each of us in the community who has to search our files every time a request comes in, and those who have to conduct the careful review of documents that I described earlier, to determine whether they can be released. And that's just the FOIA workload. It doesn't take into account discovery demands in criminal or civil cases, or declassification requests, or our voluntary transparency efforts, or pre-publication review requests. Even before the recent explosion, budgetary constraints were hindering our ability to respond to FOIA requests timely and efficiently. The Intelligence Community FOIA staffs are committed to implementation of the statute, and are dedicated and hardworking, but we simply cannot process all requests within the statutory time limits, and as a result we get sued, increasing the workload still more. If we're going to process disclosures faster, someone is going to have to provide us the resources to do that, or tell us what other part of our mission they

want us to stop doing in order to free up the necessary resources. And you may have noticed that this is kind of a tough time to be seeking additional resources.

Despite these challenges, our commitment to increased transparency will continue. We understand that to a degree far beyond what we ever considered necessary, it's important for us to give the public a better and more complete understanding of the processes and procedures we use to guide and regulate our intelligence activities. Some information will have to remain secret – more information, I am sure, than some of the other panelists today would like – but public confidence in the way that we conduct our admittedly secret activities is essential if we are to continue to be able to anticipate and respond to the many threats to our nation.

Thank you.