On the Outside Looking In

Remarks by

Steven Aftergood

Federation of American Scientists

at the

8th annual Intelligence Community Legal Conference

May 7, 2014

Thank you for the opportunity to address this conference. As someone who has often been a critic of, and sometimes a litigant against, U.S. intelligence agencies, I was somewhat surprised but even more impressed to be invited to come speak to you. Your invitation shows a kind of intellectual curiosity and openness to alternate points of view that aren't always easy to find in your Community or in mine.

I probably can't tell you anything about national security law that you don't already know. But I can tell you something about what it's like to be a member of the public who is interested in intelligence law and policy and who wants to engage with it from the outside. I can tell you what it's like to be me.

How did I get here?

As a policy advocate, I had two formative experiences over the years that strongly influenced my perspectives on government secrecy and how to deal with it.

1. TIMBER WIND and the abuse of classification authority

In the early 1990s, I was studying safety and environmental issues associated with the use of nuclear power supplies in space, whether for deep space exploration (like the NASA Voyager probes) or for military applications in Earth orbit.

One day, to my astonishment, I received a package in the mail with no return address containing a stack of classified documents that described a Department of Defense program called TIMBER WIND. It was an effort to develop a nuclear reactor-driven rocket engine for potential anti-ballistic missile applications. I thought I knew pretty much everything about what was going in space nuclear research and development, but I didn't know about this program, and I wasn't supposed to. TIMBER WIND was what DoD calls an "unacknowledged special access program." That is, even the fact of its existence was classified.

So it got my attention. Why was it set up as a highly classified program? A DoD official privately told me outright: The program managers' intent was to evade the anti-nuclear public controversy which they anticipated that the program would encounter, at least until the basic technical concept could be validated. While this was an understandable move, it was not a permissible use of the national security classification system. As you know, classification is not supposed to be a tool for managing public perceptions.

So my very first exposure to classified information was also my introduction to classification abuse.

Aside from that, the TIMBER WIND episode taught me that the unauthorized disclosure of secrets can be a powerful political gesture. It seems like there is a latent potential energy in a secret document that can generate powerful consequences when it is released outside of official channels.

My boss at the Federation of American Scientists, Jeremy Stone, told me that before I could publicly release any classified documents on TIMBER WIND, I had to give the government a chance to explain its position on the matter. So I contacted an Air Force officer whose name I recognized on the list of those who had been read-in to the program. (The list of participants had also been sent to me). He told me he could not authorize or approve of any disclosure of classified information. But he said that if I was going to go ahead anyway, I ought to withhold technical documentation of TIMBER WIND's innovative particle bed reactor fuel design, because it could only be of interest to someone who was trying to replicate the technology. That made sense to me, and I did withhold that information.

But I released the rest of the story to the press, and it was front-page news in the *New York Times*, the *Washington Post*, and other papers on April 3, 1991. I also filed a complaint with the DoD Inspector General, who issued a report in December 1992 concluding that the establishment of TIMBER WIND as a special access program was "not adequately justified." (The program managers disagreed and presented dissenting views in the IG report.) The program itself was formally terminated in 1994.

2. A FOIA lawsuit against the National Reconnaissance Office

A second formative experience that shaped my outlook on government secrecy involved the Freedom of Information Act. In 2005 I asked the National Reconnaissance Office to release unclassified portions of its latest Congressional Budget Justification Book (CBJB), and NRO officials said no. They said that the CBJB was exempt from FOIA under what's known as the operational files exemption. I appealed the denial, and then I filed suit under FOIA as a *pro se* litigant.

The operational files exemption was a legal backwater that had rarely been litigated before (NRO's own specific exemption had not been), and it got a workout in this case. Among the legal questions at issue were: Was the CBJB technically a "record" or was it a "file"? What form of document dissemination is sufficient to nullify the exemption? And so on. It was not a particularly simple case.

To everyone's surprise, including my own, I won. DC District Judge Reggie Walton, who heard the case, ruled against the multi-billion dollar intelligence agency (NRO), and in favor of the FOIA requester (me) who didn't even have his own attorney.

That doesn't happen very often, but it happened to me. And it was a tremendous antidote to cynicism.

If the TIMBER WIND nuclear rocket case led me to conclude that the classification system was prone to abuse, my FOIA lawsuit against NRO taught me that overcoming inappropriate government secrecy is an achievable goal. I may be wrong about that, but that was the lesson I came away with.

So where are we today?

What strikes me – in the aftermath of the unauthorized disclosure of the bulk telephony metadata collection program by Edward Snowden – is that the intelligence community had an unfamiliar realization: transparency or public disclosure of intelligence information is not necessarily a problem—it can serve the interests of the IC too.

Declassification, the intelligence agencies discovered, can be used to correct errors in the record, it can provide relevant context for public deliberation, and it can help to counteract cynicism about official activities and motivations.

And as you know, the government has actually acted on this newfound realization. More classified government records about ongoing intelligence surveillance programs – not just historical programs – have recently been declassified than ever before. The number of pages of Top Secret records about bulk collection programs in particular that have been officially declassified is roughly double the number of pages leaked by Snowden that have been published in the news media.

Several new government websites have been established to publicize and disseminate declassified intelligence records, including records pertaining to the privacy interests of U.S. persons (e.g., *IC on the Record*, the website for the FISA Court, the NCTC site).

For the first time, a presidential directive on signals intelligence (PPD-28) was issued by President Obama in unclassified form. (It

forms a bookend in a way to the Top Secret PPD-20 on Cyber Operations that was released by Snowden.)

New policy debates have emerged on previously remote topics such as what consideration, if any, should be given by US intelligence to the privacy rights of foreigners abroad, or the reported role of U.S. intelligence agencies in weakening public encryption standards or stockpiling known software vulnerabilities.

*

On the other hand, secrecy has remained a source of friction and public consternation. And while the IC has been opening up on some fronts, it is shutting down and tightening control on others. The new dawn of transparency so far has been largely limited to issues of bulk collection of telephone metadata.

If you want to know how many civilian non-combatants have died as a result of US drone strikes, the government won't tell you, since those deaths occurred under the rubric of covert action and are not supposed to be acknowledged or discussed.

If you want to know under what circumstances the US government can target and kill a US citizen without any judicial process beforehand or public accountability after the fact, that too is a secret.

If you would like to read a Senate Intelligence Committee review of CIA interrogation activities that took place a decade ago, stand by and maybe, just maybe, portions of the executive summary will be declassified. Sometime.

For the first time in more than four decades, the public no longer has access to open source news reports collected and translated

by the ODNI Open Source Center (formerly the Foreign Broadcast Information Service). The channel by which the public could subscribe to those products (known as the World News Connection) was terminated by the CIA last December 31.

The cup of secrecy regularly overflows. Last month, ODNI released a redacted version of Intelligence Community Directive 304 on Human Intelligence, which blacked out all references to the fact that the Director of CIA is the National HUMINT Manager. We thought that was silly and inappropriate, and we made the unredacted directive available on our website.

Another new directive -- Intelligence Community Directive 119 on media contacts -- prohibits IC employees from having unauthorized contact with reporters or anyone who disseminates information to the public without prior approval. You're not only prohibited from disclosing classified information – that has always been true – but now you can't even discuss *unclassified* information that is "intelligence-related."

A newly updated ODNI Instruction – 80.04 on prepublication review – requires that all official and non-official information intended for public release must be approved in advance. Information that is to be released must be "consistent with the official ODNI position or message." So if you ever disagreed with the official ODNI position on anything, you had better keep it to yourself.

I think that kind of regimented approach to information management is a mistake. It's bad for me, it's bad for you, it's bad for the IC. It creates a wall between the public and government that doesn't need to be there. I think the DNI was not well served

by whoever advised him to adopt these policies -- especially the directive on media contacts -- and I hope that they will be reconsidered and rescinded.

*

But let's go back to something more positive.

In recent interviews and testimony, DNI Clapper has stated his conclusion that the need for greater transparency is one of the major lessons to be learned from the past year. In particular, he said it would have been prudent and proper to seek public consent for the bulk collection of call records from the start.

"Had we been transparent about this from the outset right after 9/11… we wouldn't have had the problem we had," he said in an interview with the *Daily Beast*.

This acknowledgment that greater transparency would have benefited the intelligence community all along creates an opening for a new conversation about what is wrong with current classification practices, and what can be done to rectify them.

After all, overclassification or unnecessary classification doesn't really help anyone. For the IC, it creates both financial and operational costs, it impedes information sharing inside and outside the government, and it contributes to a climate of public cynicism.

For those same reasons, reducing overclassification would positively serve government interests. It has the potential to lower costs, to foster information sharing, and to engender public confidence. Nobody criticizes the Internal Revenue Service for keeping people's income tax returns too secret or too secure;

everybody understands that that sort of secrecy is in their own interest. The IC should strive for an optimal level of secrecy that is justified in the same way, so that people have reason to believe it serves them, not that it threatens them.

That sounds good. But how to do it?

*

I think that the key to achieving significant reductions in official secrecy is to submit agency classification decisions to some form of external review and critique.

What makes me think that is that it is already being done, at least on a small scale, by an executive branch body called the Interagency Security Classification Appeals Panel, or ISCAP.

Between 1996 and 2012, the ISCAP completely overturned the classification judgments of executive branch agencies in 27% of the cases that it reviewed, and it partially overturned classification decisions in another 41% of such cases.

That is a much more dramatic record of secrecy reversals than you would ever find in Freedom of Information Act appeals or litigation.

I think it can be explained by considering the fact that the ISCAP as a body, though it is fully committed to protecting legitimate national security interests, does not share the specific bureaucratic interests of the member agencies whose classification judgments it rejected. By subjecting those individual agency classification decisions to an external evaluation (albeit still within the executive branch), the ISCAP process has consistently yielded a reduction in secrecy.

But whatever the explanation is, the process works. Having been validated in practice year after year, this basic principle could now be applied more broadly.

One conceivable way to apply it would be to submit relevant IC classification guides – the official guidance on exactly what types of information are to be classified and at what level – for independent review and critique to an external entity. This could be an ad hoc review body, an expanded ISCAP, or an existing entity such as the Public Interest Declassification Board (PIDB) or the Privacy and Civil Liberties Oversight Board.

The PIDB, an official advisory board whose members are appointed by the White House and Congress, wrote in a 2012 report:

“The classification system exists to protect national security, but its outdated design and implementation often hinders that mission. The system is compromised by over-classification and, not coincidentally, by increasing instances of unauthorized disclosures. This undermines the credibility of the classification system, blurs the focus on what truly requires protection, and fails to serve the public interest. Notwithstanding the best efforts of information security professionals, the current system is outmoded and unsustainable; transformation is not simply advisable but imperative.”

It would be interesting to find out what the PIDB would do if it were to perform a review of IC classification guidance. What would the Board members see that others have missed? And how might they contribute to a more streamlined and effective classification system?

Another more focused sort of independent critique of specific classification practices could be solicited from the Privacy and Civil Liberties Oversight Board (PCLOB). This Board could be asked to identify current intelligence community classification practices that have significant implications for personal privacy, to assess their validity, and to recommend appropriate changes in secrecy policy.

There are other "best practices" for classification review that already exist and that could easily be incorporated throughout the intelligence community and the executive branch as a whole.

For example, the Department of Energy has a formal regulation (10 C.F.R. 1045.20) under which members of the public may propose declassification of information that is classified under the Atomic Energy Act. I have made use of this regulation myself. A similar provision could be envisioned by which the public could challenge the classification of privacy-related and other national security information throughout the government. While one can already request declassification review of a particular document, the proposed approach would go beyond that to challenge the classification status of an entire topical area, and to ask that it be independently revisited and reconsidered.

The current executive order on national security information allows for classification challenges, but only by security-cleared employees who have already have access to the information. Naturally, the key to a successful classification challenge is that it must be reviewed impartially by someone other than the original classifier. But that is entirely achievable. In FY2012, government employees filed 402 such challenges, one-third of which were granted in whole or in part (according to data compiled by the

Information Security Oversight Office). But even these internal procedures are not widely known in every agency.

Anyway, recall the remark by DNI Clapper that it would have been better if the government had openly acknowledged the fact of bulk collection of telephone metadata from the very start.

He didn't say that bulk collection was not properly classified. He said that even if it was properly classified, it should have been disclosed. Of course, that kind of open acknowledgment never happened, and it doesn't seem realistic that any agency would spontaneously or unilaterally disclose such information.

The only way it might happen is if key classification judgments are submitted to external critical review in some form. We all have blind spots, and we all have personal or institutional interests of our own, and what we see repeatedly is that those blind spots get translated into faulty, defective policies. But it doesn't have to be that way.

If you think that transparency has some virtue to it, and that unnecessary secrecy should be avoided if possible, then the point is that there are practical ways to move in that direction.

*

Beyond adjusting the nuts and bolts of the secrecy system, which is difficult but do-able, I think the IC could and should do more to release unclassified, open source analysis into the public domain.

The CIA World Factbook must be one of the most popular, widely used intelligence publications ever produced. But there is so much more where that came from. The Open Source Center which I mentioned earlier not only collects and translates foreign

news reports, it also does its own analysis of open source intelligence. A lot of that material is neither classified nor copyrighted and could be made available to the interested public. This would be a very direct, down to earth way for the IC to enrich the public domain and to provide the taxpayers with what you might call an increased return on investment. Unfortunately, as I said, the Open Source Center is moving in the opposite direction, blocking access to the kind of information people have relied on for decades. If I were the DNI, I would turn that around and direct the OSC to release as much unclassified material as it could.

*

In closing, I just want to say how much I appreciate your attention and your willingness to listen to my comments. I think that even when we disagree, we are all somehow part of the same enterprise. When we fight, we oppose each other with arguments, and within a framework of law. That is not something that anyone should take for granted, especially since it is not true in so many other parts of the world.

Steven Aftergood

saftergood@fas.org