LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 3 FALL 2015

INDEPENDENT OVERSIGHT OF FEDERAL COUNTERTERRORISM PROGRAMS

JANUARY 2015 SYMPOSIUM TRANSCRIPT

Elisebeth B. Collins

MS. MULLINS: As a really great follow up to Mr. Inglis, our next speaker will go into more detail about what you've heard regarding the 702 and 215 reports. She is on the board of the Privacy and Civil Liberties Oversight Board,[1] which are responsible for issuing those reports. This is Ms. Elisebeth Collins who was also previously with the Department of Justice for fourteen years.[2] And in 2008, she was unanimously confirmed by the Senate as Assistant Attorney General for Legal Policy.[3] Please welcome Ms. Collins.

MS. COLLINS: So, thank you, guys, so much. (Applause)

---

[1] *Elisebeth B. Collins*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/about-us/board/collins.html (last visited July 16, 2015). The views expressed are of Board Member Collins, and do not necessarily represent the Board or U.S. Government.
[2] *Id.*
[3] *Id.*

I just wanted to begin by thanking the Duncan School of Law for hosting this event and inviting me to speak. I can say the hospitality here has been delightful and the speakers quite provocative. So provocative, in fact, that I have spent most of the day completely rewriting my remarks. So, if, or really when, I can't read my own handwriting, please forgive me. And if I start going grossly over time because I now have no idea of how long my remarks are going to be, keep me in check, please. If you have a gong, use it.

So, briefly, as was explained, I am a Board Member of the Privacy and Civil Liberties Oversight Board.[4] This is a new independent, Executive Branch agency, which is charged with providing advice and oversight with respect to Federal counterterrorism programs.[5] To be clear, we are an independent Executive Branch agency.[6] I believe we were referred to here as President Obama's Board. We are not. And we are also distinct from the President's Review Group, which was mentioned previously.[7] We are a permanent Federal agency constituted by Congress with statutory responsibilities and authorities.[8]

So, the impact of spilling national secrets is obviously an interesting topic, but it is not by any stretch of the imagination a new topic. As we've seen throughout our nation's history, whether it's because of war, armed conflict, or a period of international tension, the public sentiment surrounding the open press and the public's right to know about its government has swung between periods of civil libertarianism and periods in which citizens are apparently more willing to potentially sacrifice degrees of their personal liberty for the prospect of being secure. And while technological advances, the internet, and changes to the government's ability to collect and retain information has changed the scope of the debate, many basic issues remain very much the same. Primary among those issues is what level

---

[4] *Id.*

[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/about-us.html (last visited July 16, 2015).

[6] *Id.*

[7] *Id.*

[8] *Id.*

of government transparency best serves both the nation's security interests and the need of an informed public in a representative democracy. So, concern about collateral effects from unauthorized disclosures of sensitive government information was foremost on the minds of the Founding Fathers, particularly in the context of protecting our strategic military advantage during the Revolution. For example, the Second Continental Congress established secret committees that were dedicated to what we are familiar with as modern day intelligence activities; counter intelligence operations, munitions, and arms acquisitions and foreign intelligence collection.[9] The Constitution itself recognizes that certain matters of government operations and debate are best conducted in an environment where there is some degree of confidentiality.[10]

In looking at the powers of both the Executive Branch and the Legislature, the Constitution grants both bodies the discretion when to publicly report or when not to publicly report. In Article I, this is granted to Congress by requiring that Congress keep a journal of proceedings "and from time to time, publish the same, excepting such parts as may in their judgment require secrecy."[11] For the Executive Branch, the lack of specificity in the language on the mechanisms, circumstances, or frequency with which the President is to report to Congress, aside from again saying from time to time, was according to the Federalist papers designed to provide the President a measure of flexibility for secrecy purposes.[12] But at the same time, we have throughout history established an entire infrastructure of policy, law, and oversight that is designed to regulate and manage those government operations that are determined to be too sensitive for public disclosure. Congress and especially the Executive Branch have implemented a number of policies and statutory frameworks that are designed to ensure that the need to protect national security information is equally balanced with civil liberties

---

[9] *Secret Committee of Correspondence,* OFFICE OF THE HISTORIAN, https://history.state.gov/milestones/1776-1783/secret-committee (last visited July 16, 2015).

[10] U.S. CONST. art. I, §5, cl. 3.

[11] U.S. CONST. art. I, §5, cl. 3.

[12] THE FEDERALIST NO. 70 (Alexander Hamilton).

and the public's right to know.

For example, Congress has given the Judicial Branch a role through mechanisms like the Foreign Intelligence Surveillance Act which gives the FISA Court, which is comprised of sitting Article III Judges, an active role in approving and monitoring the government's intelligence collection activities.[13] This top secret court, as it was referred to earlier, is codified at 50 U.S.C. § 1861, which is a public document.[14]

Congress also has a direct oversight role, not only through the power of the purse, but more directly through the Select Committees on Intelligence in both the House and the Senate. And internal to the Executive Branch, there are oversight offices like the various offices of the Inspector General, the President's Intelligence Oversight Board, and the Privacy and Civil Liberties Oversight Board. But there can be no doubt that pressure for public education and transparency must be maintained consistent with national security imperatives. My agency, the Privacy and Civil Liberties Oversight Board, grapples with this balance every day. That's what we do. Increasing public information about counterterrorism programs and the oversight of those programs is not just a part of our mission statement or our strategic goal. We have a statutory mandate to make our reports available to the public to the most that we can and to hold open hearings that inform the public on our oversight and advisory roles.[15] To that end, we have had public hearings that were televised on C-SPAN or C-SPAN 3, depending on how interesting they were presumed to be ahead of time and sometimes at two in the morning, but that's all right. They're available. We have had public hearings on the 215 and the 702 Programs. And to date, we have published two extensive reports on the counterterrorism programs that we have been talking about today; the metadata program under 215 and the collection conducted under Section 702 of FISA.[16] These

---

[13] 50 U.S.C.A. § 1861 (West 2015).

[14] *Id.*

[15] 42 U.S.C.A. § 2000ee (West 2015).

[16] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/library.html (last visited July 16, 2015).

reports are both available on our public website.[17] And if you have the spare time to read about three hundred and fifty single spaced pages of information, there is a wealth of detail about the operation of the Section 215 and 702 Programs.[18] And I will talk more about these reports a bit later in my comments. But on the topic of transparency, both of these reports contain large amounts of information that was declassified for the purpose of this publication.

For example, in the 702 report, there are over one hundred factual details about that program that we were able to declassify and to publish.[19] Now, apparently, I'm also the ethics credit for today. So, I'll say here, this raises serious ethical considerations as to what facts to push for declassification, asking yourself, are you really in the best judge --position to judge whether or not declassification and publication of specific facts might eventually do harm to this country or our people. But this is what we've looked to every single day. This is what we do.

So, both of the reports also contain numerous recommendations for the intelligence community and the FISA Court, which we've talked about, that aimed at increasing the public's knowledge about these programs and the oversight of these programs, whether it would be through publication of the significant FISA Court documents, which we support, the declassification of previous opinions, which we have also supported, the declassification of the minimization procedures that Chris [Inglis] had referred to, which are the court-ordered rules for how agencies like the NSA, CIA, and FBI can handle information that is acquired pursuant to these types of programs, and also, by permitting service providers to talk in greater detail about their compliance with these government production orders.[20] In each of these recommendations, however, we recognized that all of this increased transparency would need to be taken

---

[17] *Id.*

[18] *Id.*

[19] David Medine et al., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014).

[20] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/library.html (last visited July 16, 2015).

consistent with the needs of national security. This balance, taken with thoughtful engagement of the intelligence community, is designed to maximize the flow of information to the public, which does include our enemies, while minimizing the dangers inherent in unauthorized disclosures.

Turning to those unauthorized disclosures very briefly, it is for others to judge the merit and the value of them, but I think it's fair to say the way I approach it is that we will not know today or tomorrow the damage that is done either by unauthorized disclosures or by deliberate approved disclosure, such as that is contained in our reports. This is something that we'll see only over time. I think there are indications that there have been significant repercussions from the unauthorized disclosures.

Last month, the Telegraph newspaper published an article about how GCHQ, which is Britain's equivalent of the NSA, is now blind to more than a quarter of the activities of the U.K.'s more serious criminals because they have changed their communication methods as a result of Edward Snowden.[21] Again, it can be applauded, there could be merit to these disclosures, but we also have to be cognizant of the consequences of these disclosures. And an article about one specifically particularly caught my eye. It said, "There had never been anything like it. It was as if an NSA employee had publicly revealed the complete communications intelligence operations of the agency for the past twelve years, all its techniques and major successes, its organizational structure and budget, and had, for good measure, included actual intercepts, secrets, and transitions of our communications not only for our adversaries, but of our allies, as well."[22] But this is actually a quote from a 1981 article in an NSA publication called "A Cryptologic Spectrum."[23] More surprisingly, the article is about a tell-all book you've actually heard reference

---

[21] Tom Whitehead, *GCHQ warns serious criminals have been lost in wake of Edward Snowden leaks*, THE TELEGRAPH (Dec. 21, 2014), http://www.telegraph.co.uk/news/uknews/law-and-order/11300936/GCHQ-warns-serious-criminals-have-been-lost-in-wake-of-Edward-Snowden-leaks.html

[22] National Security Agency, *The Many Lives of Herbert O. Yardley*, CRYPTOLOGIC SPECTRUM, Autumn 1981 at 10.

[23] *Id.*

to earlier today that was published in 1931 by one of U.S. Government's most prolific code breakers, Mr. Herbert O. Yardley.[24] In the book, called the "American Black Chamber", Yardley disclosed scores of details about our ability to break foreign communication codes, including the notorious Japanese "Purple Code."[25] Academics have argued that these disclosures caused our enemies to adopt more complex encryption standards to better secure their methods of communication. This, in turn, they suggest is related to the intelligence failures that led to the attack on Pearl Harbor. So, we will have to wait and see about the impacts of these unauthorized disclosures and of our authorized disclosures in our reports over time. They may be merited, but they will have consequences.

Let me turn just a little bit more to the Board itself and the reports that we have issued, which again are available for a quick, light read at night from our website.[26] So, the 9/11 Commission Report recognized that changes to U.S. counter-terrorism programs would require greater coordination and collection capabilities for the U.S. intelligence and law enforcement agencies.[27] But to balance this need, the Commission recommended that the Executive Branch establish a Board whose responsibility it was to balance the security needs of the government with the privacy interests of American citizens.[28] In following this recommendation, President Bush created the first incarnation of the Board by Executive Order in 2004. At that time, the Board was chaired by a Deputy Attorney General --the Deputy Attorney General and consisted of twenty-two additional members from across the Federal Government. That Board met six times. And I think it's safe to say it did not, it did not advance the cause of privacy or civil liberties in any sort of meaningful way.

Congress then reacted to this Executive Branch attempt by implementing a statutory version of the Board, but housed it once again in the Executive Office of the President. So,

---

[24] Herbert O. Yardley, The American Black Chamber (1931).
[25] *Id.*
[26] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/library.html (last visited July 16, 2015).
[27] Thomas H. Kean et al., The 9/11 Commission Report (2004).
[28] Id.

within the direct purview of the President. Only the Chair and the Vice Chair of the Board were subject to Senate approval. This version folded under a perception that it was insufficiently independent. So, in 2007, the Board underwent its most recent legislative reorganization with the passage of the implementing of the recommendations of the 9/11 Commission Act.[29] The Board is now comprised of five members, of which I am one, all serving upon nomination of the President with the advice and consent of the Senate.[30] And we serve staggered six-year terms.[31] Four of the members, including myself, are part time. We are barred by statute from working more than one hundred and twenty-nine days out of the year on Board work.[32] Our Chairman is full time. And we are fully independent, which made it extremely difficult to get up and running the first couple of years, but I think in terms of both substance and optics is the correct formulation for the Board and the correct organization. So, in 2014, and pursuant to requests from both the White House and members of Congress, the Board undertook two deep dives, one into Section 215 and one into the 702 Program.[33]

So, turning to the Section 215 program, which I had no idea of how much education I was going to do by this point in the afternoon, I will cut to the chase. Section 215 was designed to be the national security equivalent of a subpoena, which is

---

[29] *Id.*

[30] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/about-us.html (last visited July 16, 2015).

[31] *Id.*

[32] The four non-Chairman Board Members are currently designated as Special Government Employees ("SGEs"), 18 U.S.C. § 202(a), which means they do not plan to work more than 130 days in a 365-day period. Office of Government Ethics Memorandum 00x1, at 5 (Feb. 15, 2000), *available at* https://www2.oge.gov/Web/OGE.nsf/All+Advisories/DDABAE34F0273E5F85257E96005FBDDE/$FILE/00x1.pdf?open. If Members work more than 130 days during that period, they are still considered SGEs, but should consider whether to be re-designated for the next 365-day period. *Id.*

[33] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/library.html (last visited July 16, 2015).

available in grand jury proceedings.[34] And pursuant to that authority, the FISA Court issued an Order that directed certain telephone companies to produce certain call detail records to the NSA; specifically, as we've heard, the calling and receiving numbers and the time and length of the call, but not subscriber information. The FISA Court's Order resulted in the production of call detail records in bulk, huge amounts of bulk, leading to a fast government repository of this type of information. The Board fundamentally split in our assessment of the program with the majority concluding that it was unlawful and ineffective and that it raised significant Constitutional concerns.

In my separate, dissenting statement to the 215 report, which I commend to you is a pithy five pages, a very easy read if you have the time, I agreed with the majority of the Board's recommendations, but departed from the Board in three important areas. First, while the majority of the members felt that the collection of bulk telephone data did not have an adequate statutory basis, my view of the program was that it fit within a permissible interpretation of the statute. At the time, no fewer than a dozen Federal Judges had reached the same conclusion. Second, I did not agree with majority's Constitutional analysis, which I viewed as aspirational rather than actual. The majority concluded that the program raised concerns under both the First and Fourth Amendments. On the Fourth Amendment question, I believe, as did the FISA Court in approving the government's applications, that the government was entitled to rely on the Supreme Court's case law regarding metadata, such as digit styled and the third-party records doctrine. It is certainly true that Fourth Amendment law may dramatically shift. Justice Sotomayor and Justice Alito each have indicated a willingness to re-examine fundamental Fourth Amendment concepts, but it has not happened yet. Similarly, with regard to the First Amendment, I believed that the majority was analyzing a program that did not actually exist, and in doing so, had a concern about the chilling effect of the program that I thought was divorced from the reality of the program, which, as we've

---

[34] David Medine et al., Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (2014).

heard, was actually a highly programmed --cabin program. In the actual programs, the odds were something along the lines of .00001 percent that your number would ever be associated in any way with your subscriber information. And, again, it is true that the Court may take into consideration the ability to -- We connect the dots not just about our enemies, but also we have the potential to connect the dots about our own citizens. And the Court may eventually have that as a First Amendment matter. But they are not there yet. So, I thought it was unfair of the majority to analyze a program that didn't exist under case law that is not where the majority thought it was. I also did not join with the majority of the Board as to their conclusion as to the efficacy and utility of the bulk program. In today's world of multiple threats, complex methods of communication, and technological advancement, a tool that helps investigators to prioritize information and to triage information and to focus on those who are more likely to be doing harm to or in the United States, I think it's both good government and potentially more protective of privacy. The only question about efficacy of government programs should not be how many plots has this particular tool thwarted --Although I fault the government, as well, because the first thing that the government does every time to defend a program is to say, well, we've thwarted x, y, z. And those numbers typically change over time as we start to unpeel them. That's how many plots this specific tool has thwarted. I think we need to take a more holistic view of how we assess the efficacy of counterterrorism programs. And that's one of the major recommendations that the Board has unanimously made to the intelligence community, to the Administration.

For policy reasons, not for legal or Constitutional reasons, I did sign on to ten recommendations, including limitations on the interim operation of the program. I also agreed that the public trust could benefit from changes to the operation of the FISA Court. Our recommendations included the establishment of a special advocate to bring some adversariality to the operations of the FISA Court and, as I had mentioned earlier, an emphasis on drafting opinions so that they could be declassified at least in part, and an effort to go back and start declassifying important opinions of the Court.[35]

---

[35] *Id.*

So, the second report, which I will turn to briefly, was on the 702 Report. In this report, we again examined an intelligence program that was a major product of the Snowden disclosures.[36] This time, however, the Board found that the program conducted under Section 702 operated under sound Constitutional and statutory authority, and that it contained protections and procedures that were reasonably designed to protect against the unauthorized use of personal information.[37] Further, the Board recognized the considerable intelligence value that this method of collection provided the government.[38] This is as to the core of the program. That said there are serious Fourth Amendment implications to the Section 702 Program. And although the government does not take the position that there are no Fourth Amendment implications, I'm not sure where that has come into, into the ether or why that was stated earlier today. Instead, what they stated is there's not a specific warrant requirement, but that the Section 702 Program does meet the reasonableness prong of the Fourth Amendment. And it needs to meet that because of the amount of incidental collection of American citizens' communications. And here I'm talking about what's been discussed earlier, which is where you target a non-U.S. person overseas, but they're calling to the United States. This is called incidental collection. And it was a major focus of the Board's work, the Board's concern about the potential Fourth Amendment implications.

And to that end, a number of our key recommendations are for the NSA to take a serious look at what is the scope of this incidental collection.[39] To date, the NSA had refused requests, primarily based on feasibility grounds, by members of Congress, such as Wyden, to look at the issue of, well, how much is being collected that is actually U.S. person communication. I am proud to say that after approximately six weeks of negotiation, the NSA is moving forward on four different types of reports. They are doing an

---

[36] David Medine et al., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014).

[37] *Id.*

[38] *Id.*

[39] *Id.*

assessment to try and figure out how much of this personal information is in there because, of course, that informs both the Fourth Amendment analysis and the policy consideration. So, we were unanimous in our 702 Report. And I think both of those demonstrate just a few things that I would like to leave you with because I know that I'm perilously close to running late. You know, there are a couple of issues at the margins of the 702 Program that I think are difficult legal questions that the Court has thus far, other than the FISA Court, declined to weigh into. One of them is the incidental communications. The other is something that was raised earlier today. And that is, how do they use this information? So, for example, should information collected pursuant to Section 702, which has a lower threshold than probable cause, an individualized determination, should that be available to or used in criminal investigations?

And I'll pose an ethics problem for you, which is, should it be required to be made available to criminal investigations because there may be exculpatory information in the 702 collected communications and metadata? I look forward to questions from you all. I think this has been a fantastic event. I hope that I have left you with at least a small interest in going to www.pclob.gov. I'm serious. Our mission is to educate you and inform you about what the government is doing on your behalf. So, thank you. (Applause)

(End of excerpt of Symposium.)