

## PREPARED REMARKS AT UNIVERSITY OF CHICAGO LAW SCHOOL

Feb. 24, 2016

Thank you, Joe.

It's good to be here at the University of Chicago. Earlier this morning, I was a guest speaker at Professor Mortara's Federal Courts class, and I look forward to more good discussion here.

I always enjoy appearing before Federalist Society student chapters. In part, that's because I get an engaged and well-informed audience. And in part it's because of the wide variety of viewpoints I usually find in the audience. When I spoke to the national student symposium on this general subject a couple of years ago, it was clear that the audience represented the full gamut of views on national security issues. And I welcome that.

I'm here to talk about balancing national security and privacy, but before I dive into the subject matter, I want to pause and explain my current role in the federal government.

I serve as a Member of the Privacy and Civil Liberties Oversight Board (or PCLOB, as people call it), which is a federal agency that provides advice and oversight to other agencies to ensure that national security and privacy interests are balanced in the federal government's counter-terrorism efforts.

PCLOB was originally recommended by the 9/11 Commission, which – for those of you too young to remember it – was a temporary commission that investigated why our intelligence agencies failed to prevent the terrorist attacks of September 11, 2001. The Commission focused mainly on how to improve our government's ability to stop terrorist attacks, but it also recognized the need to ensure that these efforts weren't taken too far at the expense of individual freedom. To address that concern, it recommended the creation of a privacy and civil liberties oversight board.

In 2007, Congress established the PCLOB in its current form as an independent federal agency. Although statutorily authorized in 2007, the Board lay dormant until its first four members (including me) were confirmed by the Senate in 2012.

The Board is bipartisan, comprised of 5 members appointed by the President and confirmed by the Senate, only three of whom may be from the President's political party.

The Board's independence and access to classified information have enabled us to publish comprehensive reports about some of the intelligence programs that were disclosed in recent years, including the bulk telephony metadata program (the "215" program), and the Section 702 (or "PRISM") program. I'm not going to go into detail on those programs or reports, but you are welcome to ask me about them. We are a permanent agency of the U.S. Government, and we continue to review other U.S. counterterrorism programs and activities.

Enough about that. Let's talk about the substance – balancing national security and privacy.

This notion of balancing is often tossed around as though it's a simple or self-executing concept. This is far from true – it's very hard, especially for those engaged in the nitty gritty of policymaking, trying to balance these interests in practice.

I'm not here to give you all the answers on how to get this balance right because I don't think anybody has them. The answers will constantly evolve and require policymakers to continuously take into account changes to the threats facing the United States, the type of intelligence the government needs to combat them, the type of technology available to collect that intelligence, and the way that society perceives its own privacy interests, among other considerations.

Instead, what I'll do is raise a few of the big picture questions in this area, give you food for thought, and invite you to ask questions afterwards.

First, I'll point out that many people don't like the term "balancing" in this context. I think that's because the word "balance" suggests that this is a zero sum game – more privacy equals less security, or vice versa.

I agree that the word "balance" doesn't perfectly capture what we're talking about, which is how the government can get two things right at the same time. Perhaps "reconciling" or "aligning" interests would be better. But I'll stick with the word balance as a shorthand for now.

### **Question 1: What interests are we balancing?**

Before balancing interests, one needs to step back and understand what interests one is balancing.

Let's start with national security, which is the easier of the two interests to define. What is the government interest at stake and how important is it?

At its most basic, protecting the national security means protecting the nation against existential threats. Thirty years ago, we were focused on the Soviet Union and nuclear war. The Soviet Union no longer exists, but concerns about threats posed by nation states and traditional warfare have not gone away.

And of course national security extends far beyond threats posed by nation states. The 9/11 attacks made clear the threat that can be posed by non-state actors, and the attacks in San Bernardino show the threat that can be posed even by one or two individuals.

The importance of protecting the security of the nation – its sovereignty, its people, and its way of life – is self-evident. It is surely the *most* important function of the federal government.

Relatedly, since this is a Federalist Society event, I would note that national security interests are unique among government interests from a constitutional perspective.

I know from experience that Federalist Society audiences tend to be composed mostly of people with a very healthy distrust of government power generally and the consolidation of power in any one part of the government. I could not agree more with that sentiment in general.

But in my view, it is important not to lump all government functions together –we should think about the scope and locus of government power differently in different contexts.

National security is different from most policy topics in our federal structure.

Not only does the federal government have the primary role in protecting national security, but defending the national security is one of the few things the federal government *must* do.

While state and local governments are critical partners in protecting the national security, both the text of the Constitution and practical considerations put the federal government in charge.

And while the federal government could probably get out of certain areas of domestic policy entirely, either because they should be left to state and local

governments or because there's no legitimate role for government at all, that is not true of protecting national security.

Defining the interests on the other side of the ledger is harder. Some of those interests are well-understood. The right to free speech, exercise of religion, and assembly, for example, have been defined by centuries of caselaw.

But the concept of "privacy" is different.

Let's set aside for the moment Fourth Amendment jurisprudence. As you know, although the Fourth Amendment does not mention privacy, it has been construed by the courts to hinge on a "reasonable expectation of privacy." But my Board – along with policymakers around the government – is expected to consider privacy interests that may not be protected under Fourth Amendment caselaw.

What are those privacy interests?

There is no universally accepted sense – let alone a clear definition – of what "privacy" is.

There are many different possible definitions.

Privacy might be, for example, freedom from the exercise of government power.

It might be freedom from the risk of embarrassment or reputational harm.

It might be freedom from economic harm due to the misuse of personal information.

Another commonly used definition of privacy is the right to control information about oneself. This is not necessarily an interest in having nobody know anything about you, but a desire to control who knows what, and to limit what they can do with that information. Today, you might think of this as the Facebook-privacy-settings version of privacy, but it's not a new concept. For example, Charles Fried – my former boss – articulated this definition of privacy in a law review article in 1968.

Privacy is sometimes defined more generally as the "right to be left alone."

This definitional question is fascinating from a philosophical perspective, but the lack of a clear answer is a challenge for officials who are expected to embed privacy protections into government programs in real life.

There are certain definitions of privacy that, in my view, just don't work in practical policymaking.

The 'right to be left alone,' for example, is too vague and general to be useful in this context.

Some definitions can't realistically work because they depend on the subjective expectations and intents of individuals. Many government programs – particularly law enforcement or national security programs – have to operate on generally applicable rules. So the right-to-control-ones-information definition I mentioned earlier cannot be applied to programs where the government can't ask for the consent of each individual affected or apply a custom-made set of rules to information about each individual.

And even the definitions that can plausibly be applied to such programs might be in tension with one another, so that using one definition would counsel choosing policy option A, whereas another definition would point to option B. The Board has come across that tension in real circumstances.

This uncertainty about the nature of the interest at stake makes the task of balancing that interest with national security interests even more challenging than it would already be.

## **Question 2: How to balance transparency and secrecy**

Related to the general question of how to balance national security with individual freedoms is how to balance secrecy and transparency about the government's actions to protect national security.

Accountability of government is a fundamental tenet of a free democracy, and some degree of transparency is necessary to enable accountability. It is essential to the people's ability to control the state and protect themselves against governmental encroachment on their freedom. Even in the intelligence context, the government should tell the public as much as possible about the rules that govern federal agencies.

That said, in the national security context, transparency cannot be an absolute value. It must be balanced with the legitimate need for secrecy. In

contrast to many governmental functions, where there can often be transparency about virtually everything an agency does, agencies cannot effectively protect the nation's security without shielding their day-to-day work from public view.

To make a painfully obvious point, if agencies revealed the specific targets of their intelligence gathering, the identities of their sources, or exactly how they engaged in clandestine collection activities, the information would soon dry up. Intelligence agencies rigorously protect these "sources and methods."

But where to draw the line between transparency and secrecy is a very difficult question in practice. At one end of the spectrum, agencies should publish high-level rules about what kind of information they may collect and how they will ameliorate the privacy impacts of collecting that information.

But more specific rules about what the agencies can and can't collect and methods they can and can't use are more problematic. It's not easy to decide how much of that information can be released without providing a roadmap for legitimate targets to avoid surveillance altogether.

The agencies are grappling with this more and more, and the Director of National Intelligence just released – for the first time ever – transparency principles for the intelligence community. This is good public policy, but it's also in the IC's interests. Putting more information in the public domain will both help the public understand the intelligence agencies' mission and dispel some of the myths that have infected the public debate about foreign intelligence programs over the last few years.

And there has been no shortage of misconceptions and out-right mistakes in the press and commentary about these issues.

For example, if you read the press and the commentary about the so-called Section 215 program – the bulk telephony metadata program that was leaked by Edward Snowden and has since been ended – you might have thought that the NSA was listening to all of your phone calls, or at least that they knew exactly when you had called your psychiatrist, mistress, or priest. In reality, the program didn't collect the content of any telephone conversation or any personally identifying information about any caller. It collected phone numbers, the time that they called other numbers, and how long the calls lasted. The database was a system of numbers with no names attached to any of them. And because the database could only be searched to find out which numbers had been called by a particular number for which there was already evidence of a connection to a

specific terrorist group, the vast majority of those numbers were never looked at by any human being.

Changing public perception after the press has made a mistake or only provided half the story is no easy task, especially in this context. That is in part because intelligence programs and the rules controlling them are very complex, and explaining why an allegation is wrong or misleading often takes longer than most people are willing to listen. But that could be said of most complex policy issues.

This is an old problem. Jonathan Swift wrote in the early 1700s that “Falsehood flies, and the Truth comes limping after it; so that when Men come to be undeceiv’d, it is too late; the Jest is over, and the Tale has had its Effect....”

What makes it even harder in the national security context is that the government often can’t correct a mistake or provide an explanation without disclosing more sensitive information and thereby further damaging the national security.

It didn’t help that the intelligence agencies – by their nature secretive – are not good at public relations. In the past, although the agencies provided a great deal of information to their oversight bodies in the Congress, the judiciary, and the executive branch, they spent less time explaining their mission to a public audience.

As a result, there was very little public understanding of what the intelligence agencies do or why they do it. There was almost no public discussion, for example, or what foreign intelligence is or why we need it.

If people don’t understand why we need good intelligence, it’s hard to expect them to support a robust intelligence capability.

There is a lot more to be said about that, and I’d be happy to talk about it in the Q and A.

### **Question 3: How do we ensure democratic accountability of secret programs?**

This discussion of transparency and secrecy leads to a third important question, one that Professor Mortara asked me to address. Given the need to maintain a fairly high degree of secrecy about national security efforts, how do we ensure that the agencies follow the law? How do we prevent the abuses that preceded the Church and Pike Committee investigations in the 1970s?

A big part of the answer is effective oversight by bodies in all three branches of government that can keep secret information secret but have the authority to make policy changes and impose consequences for misconduct.

When constructing an oversight regime, several attributes are important.

First, the overall oversight regime should consist of two general types of oversight. One is ensuring that agencies and their employees obey the law and imposing discipline if they don't. That is mainly about compliance. The other is reviewing the rules that govern programs and changing them when necessary. That is primarily about policy development. So oversight is not just about making sure the rules are followed, but making sure the rules are right.

A second important attribute is independence. If an oversight body is independent of the agencies it oversees, it can candidly counsel changes in policy or impose consequences for misconduct, depending on its role. On the other hand, an independent body is unlikely to be fully integrated into the day-to-day work of an agency, which means it won't be aware of every opportunity to provide advice or every instance of misconduct. This is why, in addition to independent oversight from inspectors general, the Intelligence Oversight Board in the White House, the PCLOB, and other institutions, agencies need internal oversight mechanisms such as general counsel's offices and agency privacy officers.

A third important attribute is involvement by all three branches of government. This is true of oversight of national security programs in the United States, despite the common misperception that these agencies operate in the Wild West with no rules. I'm fairly confident that no country has an oversight system for counter-terrorism programs that is more robust than ours.

I've already referred to some of the executive branch oversight mechanisms. They exist within the agencies – general counsel's offices; "Civil Liberties and Privacy Officers;" and inspectors general – and outside particular agencies, including my agency, the Director of National Intelligence, and several offices within the Executive Office of the President.

There is oversight from the other branches of government as well. Starting with the judiciary, "oversight" may be an inapt term, because the courts generally only review specific cases and controversies that come before them; for constitutional and practical reasons, they do not have a free-ranging mandate to oversee the executive branch. But the FISA Court does play a role different from other courts, in that it has frequent interaction with the executive branch concerning surveillance activities that it has authorized under the Foreign Intelligence Surveillance Act.

And last but far from least, there is congressional oversight. The House and Senate Intelligence committees conduct oversight of specific activities by the intelligence agencies and control their budgets. The agencies have a statutory requirement to keep the intelligence committees “fully and currently informed” of their activities, and they take it seriously.

When thinking about democratic oversight, it is important to remember that we live in a representative democracy. In areas where there are legitimate reasons for the public not to know every detail about what the executive branch is doing, we have to rely on our elected representatives to exercise oversight on our behalf.

I know that some take a dim view of the effectiveness of congressional oversight, but if we cannot trust Congress to conduct rigorous oversight of the executive branch, then we have a crisis of government that extends far beyond classified national security programs.

Thanks very much for your attention. I hope this has been thought-provoking, and I look forward to your questions.