Remarks by the Hon. Rachel L. Brand,

Member, U.S. Privacy and Civil Liberties Oversight Board,

Vienna Parliamentary Forum on Intelligence-Security, May 6, 2015,

Vienna Hofburg "Kleiner Redoutensaal" Vienna, Austria[1]

I want to thank you for your invitation to join this important discussion in this beautiful city. It is a privilege to join Congressman Pittenger and all of you for this dialogue.

As we engage in this discussion about the appropriate role of electronic surveillance in counterterrorism investigations, it is important for all of us to understand not only our own national legal systems and laws, but also those of other nations.

Today, I hope to shed some light on the protections for privacy in U.S. law – both for U.S. persons and for citizens of other nations.

I also look forward to learning more about your legal systems and the protections they afford both to your own citizens and to citizens of the United States.

Please note that any opinions I express are my own and that I will not be speaking for the rest of the Board on which I serve.

Although our nations' laws and systems differ, there are a few things that all of us have in common.

We all grapple with how to balance two imperatives – protecting our nations from the wide variety of threats that face us today, while also respecting privacy and fundamental freedoms. This is an ongoing challenge that we in the United States take very seriously, as I know you do.

Many, if not all, of us have also seen how current events can cause dramatic swings in public opinion on how to achieve this balance. After a terrorist attack,

[1] The Parliament of the Republic of Austria hosted the May 2015 Parliamentary Intelligence-Security Forum in Vienna. Approximately 70 invited representatives from 25 countries attended.

citizens demand more security. After a leak of an intelligence program, they are more focused on privacy.

These shifts in public opinion are natural and understandable. The challenge that we all face is to take the long view and not over-react in either direction based on current events.

The issues we are discussing today are of great concern not only in Europe, but also in the United States. They are being hotly debated in the public, in the press, and in our Congress.

There is always room for improvement in our system, as in any other. That is why our Congress created my agency, the U.S. Privacy and Civil Liberties Oversight Board. Our Board has recommended a number of refinements to the rules governing U.S. surveillance programs, which the Administration has implemented or is considering.

But it is important to remember that U.S. law already contained many privacy protections. We expect our intelligence agencies to follow these rules. I will explain some of them today, without getting into technical details.

The legal structure that governs our intelligence agencies and their activities has developed over the course of the last two centuries and has become quite complex. Frankly, most Americans are not familiar with it.

To start, every action taken by any U.S. government agency – including the intelligence agencies - must comply with three levels of law:

The first is the U.S. Constitution, including the Bill of Rights.

Second, statutes passed by Congress (such as the Foreign Intelligence Surveillance Act) further limit what the government may do.

And finally, the President and the agencies have imposed many rules upon themselves that even further limit what the government may do.

Protections for privacy and civil liberties run throughout all three levels of these requirements.

I think of the combination of these requirements as limiting the government's intelligence activities in four practical ways:

(1) First, there are limits on what *kind* of information the intelligence agencies may collect.

For example, under the National Security Agency's so-called "PRISM" program, the government may not target any person for surveillance unless he or she is likely to communicate "foreign intelligence." This is a term with a specific legal definition. Some believe that the definition is too broad, but it does prohibit surveillance of most people around the world, because they would not possess information relevant to the national security or foreign affairs of the United States.

Another limit on the type of information the government can collect is a rule that U.S. agencies may not collect information in order to provide U.S. companies with an economic advantage over foreign companies.

And it is absolutely fundamental under U.S. law and policy that our intelligence agencies may not collect foreign intelligence information for the purpose of suppressing or burdening criticism or dissent.

(2) Second are what we refer to as "thresholds." This refers to the degree of certainty the government must have that a person is connected with terrorism before the government may collect information about him.

Related to this are rules about what process the government must go through before it may collect that information. These rules vary in different contexts, but in general, U.S. law imposes stricter rules for intelligence methods that significantly intrude into individual privacy than for methods that are less intrusive.

For example, the standards and procedures for getting a wiretap to listen to communications in real time are stricter than the rules that apply to collecting "metadata," and the rules for collecting metadata are stricter than the rules for collecting information that is publicly available on the internet.

(3) Third, every agency has extensive rules for what the government may do with information *after* it is collected.

These rules include "minimization procedures" intended to mitigate the privacy impact of what happens to information after it is collected. In many situations, for example, they require agencies to block out individuals' names before sharing information with another agency.

Many programs also have what we call "retention limits," which means that the agency must delete information after a certain period of time.

In addition, some types of information can only be used for specific purposes, such as investigations of counter-terrorism or serious crimes.

There are very strict rules for when information gathered for foreign intelligence purposes may be used in a criminal proceeding.

Many programs also have limits on which government employees may see the information collected.

And there are many other similar rules intended to protect privacy – too many to discuss in a short time.

(4) The fourth type of protection is oversight. By "oversight" I mean that we do not assume that the intelligence agencies are following all the rules I just described; we check that they do, and we impose discipline if they don't.

I view this as critically important in the intelligence context. For obvious reasons, much of what the intelligence agencies do is done in secret. The public does not know the details, and they cannot know the details without undermining the intelligence operation.

The United States has made great strides in enhancing transparency surrounding intelligence activities. Our Board's lengthy reports on two of the NSA's programs were entirely public. The intelligence agencies themselves are putting more information than ever in the public domain. And our Board has recommended a number of changes to increase transparency even further.

But there will always be a high degree of secrecy in this area.

The way I see it, the greater the secrecy, the greater the need for effective oversight by people who can be trusted to keep information confidential, but who are independent and who can impose consequences on anyone who breaks the rules.

Fortunately, there are many levels of oversight that already exist in U.S. law, and our Board has recommended several ways in which that oversight can be strengthened.

To take the "PRISM" program as an example, there is first oversight within the NSA itself. The individual employees who decide where to target surveillance

have their decisions reviewed by multiple levels of supervisors and lawyers. Many of their actions are then reviewed by lawyers at the Department of Justice.

The Foreign Intelligence Surveillance Court, made up of independent judges with life tenure, has to approve the rules of the PRISM program and supervise the way it operates.

This is real review – the Court may refuse to authorize proposed surveillance, and may impose conditions or restrictions it if does approve.

Then there is our Board, which is empowered by Congress to review any information relating to the government's counter-terrorism activities, report on the privacy and civil liberties implications of what we find, and recommend improvements.

And finally there is Congress. You will hear tomorrow from the Chairman and Ranking Member of the U.S. House Intelligence Committee, which oversees all of the intelligence agencies in great detail and, ultimately, controls their budgets.

I know that you are probably most concerned about how all of this affects your citizens.

Many of the rules I just discussed do explicitly distinguish between "U.S. persons" (which is a legal term that refers to U.S. citizens and lawful permanent residents), and non-U.S. persons (which is everyone else). In a variety of ways, they do provide greater protection to U.S. persons. This should come as no surprise, as I suspect that most nations are understandably more concerned about their own citizens than those of other nations.

But there are a number of ways in which our laws protect U.S. persons and non-U.S. persons alike.

For example, the rule that agencies may only collect "foreign intelligence information" significantly limits the communications – of Americans or others – that may lawfully be collected.

In addition, the President recently issued a directive that requires agencies conducting signals intelligence to include non-U.S. persons within several of the privacy protections that already applied to U.S. persons.

In general, he ordered the intelligence agencies to apply the same safeguards for personal information to both U.S. persons and non-U.S. persons to the maximum extent possible.

In particular, he ordered the agencies to apply to people of *all* nationalities the rules limiting the sharing of personal information between agencies.

He also ordered the agencies to apply the same retention periods to information about both U.S. persons and non-U.S. persons.

Finally, he ordered the intelligence agencies to recommend to him other ways in which the privacy protections that currently apply to U.S. persons could also be applied to non-U.S. persons. Our Board is engaged in an ongoing consultation with the Administration on this subject.

I am not here to argue either that the U.S. system is perfect or that our system should be your system. But I do hope this was helpful to you in understanding how U.S. law protects privacy in the intelligence context.

As I mentioned at the beginning, I am interested in learning more about how your systems address these questions, and particularly how you exercise oversight of your intelligence agencies.

I want to conclude by expressing once again my gratitude to our hosts in the Austrian Parliament.