Remarks by Secretary of Homeland Security Janet Napolitano: Achieving Security and Privacy

Release Date: May 3, 2012

Canberra, Australia
Australian National University
(Remarks as Prepared)

Thank you, Professor Young, for the kind introduction, and for inviting me here to Australian National University. I'm honored to join you today, and also honored to carry a message from President Obama.

As you may know, this week marks the 70th anniversary of the Battle of the Coral Sea. This battle prevented the invasion of Port Moresby by Japanese forces and helped turn the tide of World War II in favor of the Allies.

It was a moment that not only forged an enduring partnership between Australia and the U.S., but also preserved the freedoms on which that partnership rests.

And it was a great honor for me to meet some of the brave sailors and airmen who were there in May of 1942, and to deliver a message to them from President Obama.

In the decades since that defining battle, our nations have built an even stronger alliance– through mutual friendship, defense, and cooperation.

As President Obama and Prime Minister Gillard announced last November, that includes a stronger security partnership with closer collaboration between the U.S. Marine Corps and Air Force and the Australian Defense Force.

Over the next several years, a rotational force of up to 2,500 U.S. Marines will train alongside Australian troops, and live on Australian bases out of the Northern Territory. The first 200 Marines arrived last month.

We will also develop closer cooperation between the U.S. and Australian air forces – initiatives that will bring our militaries, already working together around the world, even closer.

And they will make it easier for our forces to train and conduct exercises with other partners in the region, including strengthening humanitarian assistance and disaster relief capabilities.

And, I'm happy to announce today, that our partnership is growing deeper and stronger in the homeland security arena as well, with the adoption of numerous agreements between our two nations.

In fact, part of the reason for my visit this week is to sign new agreements that will express our intent to: improve information sharing between the United States and Australia; continue to work together to secure the global supply chain; further cooperate to fight terrorism, transnational crime, and violent extremism; and facilitate travel for our citizens.

And in the coming days, I look forward to signing these remaining agreements with my counterparts.

Combating Today's Threats

These agreements show our deep commitment to a cooperative and global approach to the challenges and threats we all face.

The threats to our security come not only from established terrorist networks, but also from individuals and small groups who are radicalized to violence at home.

They come from international criminal organizations trafficking in human beings, smuggling illicit goods, or proliferating potentially deadly weapons. They can come from pandemic disease.

And, increasingly, they emanate from cyberspace. So as each and every one of our lives becomes more dependent upon systems that are networked, we face a heightened responsibility to act.

Moreover, these threats are evolving rapidly, requiring nimble action, by multiple nations and many partners.

Because today's threats do not recognize national boundaries, our responses must also transcend borders.

And in a globalized economy, our international responsibilities have become critical not only to our *physical security*, but our *economic security* as well.

Today, the very nature of travel, trade, and commerce means that one vulnerability or gap anywhere across the globe can impact security and economies thousands of miles away. And that means our security must be a *shared responsibility* – among governments, the private sector, individuals and communities.

So today, I would like to talk about some of these security challenges, and specifically, to express my belief that we can, and we will, meet them … while *simultaneously* protecting civil rights and privacy.

Rejecting the "scale of justice" model

As we work to meet evolving threats, we must protect our values, including the rights, liberties, and privacy of our peoples.

After all, everything we do to combat terrorism and violent extremism is rooted in the fundamental objective to secure for future generations the values and way of life that our countries share.

Privacy has long been one of these core values. In fact, the modern concept of privacy itself was formulated in the United States by Louis Brandeis in a seminal paper he published more than one hundred twenty years ago, in 1890, addressing then-modern technology, and "the right to be left alone."

Of course, Brandeis went on to become one of America's preeminent jurists, serving a long tenure on the U.S. Supreme Court. So privacy has been important to the formulation of U.S. laws and policies for some time.

Too often, in my view, however, we view the relationship between security and privacy as similar to a scale. If we emphasize one, we must diminish the other. We talk…mistakenly… about how to "balance" the two.

But I don't like the word "balance" because I think we have to cast aside the notion that our liberty and our security are two opposing values that are on the opposite sides of a seesaw, that when one is up the other necessarily must be down.

The plain fact of the matter is that you cannot live free if you live in fear. Security is a prerequisite if we wish to exercise the rights we cherish. So in this way, our security and our liberty are not mutually exclusive. They are mutually reinforcing.

Of course, our countries have different frameworks for privacy and individual rights. Our constitutional protections work in different ways. But we should remember that our values are more broadly similar than they are different.

Our different systems are largely trying to achieve the same results: justice, security, protection of privacy. The United States and Australia share a common commitment to civil rights and freedoms, including privacy. Together we seek to protect these rights, while securing the systems of travel, trade, and commerce on which our economies rely.

So while our histories, cultures, and government organization differ, as democracies with a common political ancestry, we share certain values which are reflected in our privacy principles. And we must work together to protect these common interests.

Value of Information Sharing

Let me give you an example. We all agree that information, especially actionable intelligence, is one of our most valuable tools for serving the needs of our communities.

But we must collect, use, and share information consistent with constitutional rights and privacy principles, having them embedded into our systems.

Information can be crucial in preventing the kinds of terrorist acts we've seen over the past decade, that have taken the lives of many of our citizens and military personnel, and of our partners as well. Acts like the terrorist attacks on 9/11, and in Bali.

Information also helps us secure our borders, administer our immigration system, prevent terrorists and criminals from getting on airplanes, stop terrorist financing and money laundering, and protect children who are the targets of human traffickers.

Much of our respective governments' ability to use and share information, therefore, stems from a mutual recognition of purpose. In the law enforcement and security context, our agencies need to be able to access information about potential threats and share it with each other.

This cooperation has helped us prevent terrorist incidents and led to criminal arrests and prosecutions. For example, information sharing among nations helped us foil the 2010 air cargo plot in which individuals from Yemen attempted to ship explosives disguised as printer cartridges aboard commercial aircraft.

By sharing immigration-related information, beginning with a data-sharing pilot that began in 2006 between Australia, the U.S. and three other countries, we have also enabled better decision-making about who can enter our countries and receive immigration benefits, in the process thwarting "asylum shoppers" and other bad actors seeking to fraudulently obtain refuge in our countries.

The Five Country Conference under which this information-sharing has taken place gives us a cooperative and cost-effective approach to sharing important security information. And it has done so while upholding stringent safeguards for privacy.

DHS Approach to Privacy

Privacy rights, civil rights, and civil liberties are values that we constantly pursue in these kinds of information sharing arrangements and agreements. They are an important part of how the United States ensures rights and liberties, in addition to the protections offered by our judicial system.

It is why the department I lead has a Congressionally-mandated Chief Privacy Officer who leads the DHS Privacy Office. This office is designed to serve as an integral part – from the earliest stages – of our policy-making process, and to ensure that privacy protections are built into the department's systems and technologies.

Having a Chief Privacy Officer within the department and at the negotiating table ensures privacy concerns are addressed from the very beginning and that we are formulating programs and policies consistent with the law. Concerns like what information is collected, who gets to use it, and how long it is kept.

In the U.S., for example, our laws require federal government agencies to notify the public when we collect or maintain personal information in a system of records. This process is built on transparency, accountability, and security.

We publish Privacy Impact Assessments. The Privacy Impact Assessment process ensures privacy protections are fully considered in the development of our programs. And ongoing Privacy Compliance Reviews confirm that the privacy protections that were proposed in the development of the programs are being implemented.

In addition, through the Freedom of Information Act, all individuals have the right to ask for information held by the government. My agency alone receives more than one hundred seventy-five thousand of these requests annually, responding to individuals around the globe.

These values are shared in Australia. While you have different structures committed to ensuring some of the same privacy goals, together, both of our countries have developed privacy frameworks that implement the globally recognized Fair Information Practice Principles effectively and transparently.

Privacy Office International Engagement

As you may be aware, the United States -- like Australia – has executed a series of Agreements with the European Union related to the collection and use of Passenger Name Record data, or PNR.

Under U.S. law, we require airlines flying to the United States from foreign countries to provide basic information about their passengers, such as name, date of birth, citizenship or nationality, and passport number.

We also require PNR, which includes information that travelers provide to airlines when booking their flights, such as itinerary, address, and check-in information, up to 72 hours prior to departure. I understand Australia has a similar PNR legal requirement.

Analysis of PNR, in particular, has been extremely effective – enabling us to identify both known and unknown individuals that are either a threat to aviation, or the United States, and to prevent them from either flying to, or entering the United States.

In fact, during 2008 and 2009, PNR information helped us identify individuals with potential ties to terrorism in more than 3,000 cases, and in fiscal year 2010, approximately one quarter of those individuals denied entry to the United States for having ties to terrorism were initially identified through analysis of PNR.

Clearly this is a valuable tool. But we have to ensure that PNR is collected, used, stored, and eventually destroyed in a manner that is consistent with privacy laws and protections – not just in the U.S. but for our partner nations as well.

Over the past nine years we have had four agreements with the EU to share PNR, with the most recent – and final – PNR agreement finalized last month in Luxembourg. As with many international information sharing agreements, our Privacy Office was involved in each round of negotiations to make certain that privacy protections were embedded into the Agreement.

In fact, during the most recent negotiations, my Chief Privacy Officer was a key part of the negotiating team. Transparency and collaboration are the cornerstones for international information sharing; and having privacy integrated into the process from the very beginning and throughout implementation is critically important.

It's also important to note that the overall framework for our approach to assessing threats, managing risk, and separating low risk travelers and cargo from those we need to scrutinize more closely, not only builds on our core values of privacy protection and data and information assurance, but can create new efficiencies for travelers.

For example, with respect to our trusted traveler programs, we basically offer travelers a choice: if you agree to provide us more information about yourself in advance of your trip so that we can make an assessment about your level of risk, we promise to do two things.

We will maintain the information you have given us in confidence and use it only for the purposes of making a risk determination. In return, we will provide you the benefit of expedited clearance through our ports of entry.

This is what I mean by not necessarily viewing security and privacy as opposing forces. In this case, we are able to enhance security AND the privacy of travelers through our use and protection of information.

It is, therefore, no surprise that about 1.3 million people have enrolled in the Department's various trusted traveler programs, including Global Entry, which provides expedited clearance for pre-approved, low international risk travelers. In fact, this program has reduced wait times for travelers by 70 percent.

One of the agreements I will sign during my visit here allows us to explore participation by our citizens in each other's expedited traveler programs so that as we take steps to protect our shared transportation networks, we will continue to facilitate travel between our countries, for Americans and Australians alike.

And, in addition, in the United States, we have strong administrative redress procedures for travelers. People who feel their privacy or rights may have been violated may file a complaint with a division of the appropriate executive agency.

In the Department of Homeland Security, that redress process is called the Traveler Redress Inquiry Program, or TRIP. TRIP provides a single point of contact for travelers who have inquiries or are seeking resolution about difficulties they have experienced in their travel screening. These include watch list issues or instances where travelers believe they have been unfairly delayed or denied boarding.

TRIP is an effective recourse where there is not necessarily the ability for someone to access American courts. And, of course, we have strong, independent Inspectors General across the U.S. government who also look into and investigate instances of violations.

Conclusion

When we talk about security cooperation, we are not just talking about sharing technologies, procedures, investigations, and information. We are talking about our joint national interests and shared values, like privacy. They are not a secondary part of the conversation. They are a fundamental part of the conversation.

Australia and the United States have a strong partnership with respect to security and also with respect to safeguarding human rights and individual liberties. It is a partnership forged over many years and one that will only grow stronger in time, as together we confront our shared challenges. Working together, we will both be stronger than working alone. Thank you.

This page was last reviewed/modified on May 3, 2012.