**U.S. Commerce Department General Counsel Cameron F. Kerry Delivers Keynote Address at the German Marshall Fund of the United States**

U.S. Commerce Department General Counsel Cameron F. Kerry today delivered the keynote address at the German Marshall Fund of the United States (GMF), which was his last public speech in this role. In his remarks, Mr. Kerry discussed how the privacy and national security debate intersects with international commerce and what significance it will have for the future of the U.S. economy. GMF President Craig Kennedy gave opening remarks and GMF Senior Transatlantic Fellow Laura Blumenfeld moderated a question and answer session following Mr. Kerry's speech.

###

*Remarks as Prepared for Cameron F. Kerry, General Counsel, U.S. Department of Commerce*

Thank you, Craig. I am very grateful for that kind introduction and this chance to reflect on the work of the Obama Administration over the past four-plus years to pave the way for the digital economy of the future.

I'd like to begin by looking back. Like colleagues focused on innovation in the Information Age, I joined the Commerce Department with the conviction that revisiting the E-Commerce Framework that has governed Internet policy since the 1990s is vital for sustaining America's growth. This framework called in essence for leaving the Internet alone to let it grow. This is still the right premise, but now flourishing digital technology and networked communications present new policy challenges that need addressing while preserving the creativity and dynamism that make these technologies such engines of growth and innovation.

The digital economy is a burgeoning. At last year's G-20, the Boston Consulting Group projected that by 2016 the digital economy by itself will amount to the fifth largest economy in the world, representing $4.2 trillion out of the G-20's collective GDP. And in the U.S. in 2010, the Internet accounted for some $684 billion, or 4.7 percent of all U.S. economic activity.

The digital economy also is an underlying driver of growth. The amount of trade enabled by data transfers is immeasurable. And recent data suggest that countries with higher broadband penetration tend to have faster economic growth.

The Commerce Department has been tackling these issues through its Internet Policy Task Force, which Secretary Gary Locke established to bring together several Commerce bureaus that cover information policy, intellectual property, trade, economics, and technological standards. With help from wide public input, this task force focused on commonsense rules for today's digital economy in four key areas: Privacy, Cybersecurity, Intellectual Property, and Global Free Flow of Information.

Our work in these areas is guided by the conviction that, to protect the dynamic innovation, economic growth, and freedom that globally-networked digital technology has enabled, we must act carefully. Thus, we have developed an approach focused on essential principles or frameworks that provide baseline parameters meant to be nimble, without detailed prescription,

especially by government. Instead, our approach operates by convening open and inclusive multistakeholder processes to flesh out these principles for the real world with consensus-based standards.

This model is articulated most fully in the White House Blueprint on consumer privacy released in 2012 under President Obama's signature. Based on the sources of privacy policy in the United States and around the globe, this Blueprint enunciated a Consumer Privacy Bill of Rights – seven principles that provide a baseline for consumers' and businesses' expectations of privacy. The Blueprint adapts well-recognized Fair Information Practice Principles (or FIPPs) to take into account the new world of increasing connectivity and interactivity that is evolving through new devices, new applications, and new tools for analyzing data that accelerate Moore's Law.

To put this into practice, the Blueprint endorses legislation to enact that Bill of Rights into law and multistakeholder codes of conduct to apply it in specific contexts.

Commerce's National Telecommunications and Information Administration has followed up with the first such multistakeholder process, convening a wide variety of stakeholders to develop a code of conduct on transparency for mobile applications on small screens. Last month, stakeholders moved from drafting to testing and implementing this code. At Commerce, we plan to announce another process soon.

We have been working hard to make the consumer privacy legislation a reality as well.

NTIA and my office have met with stakeholders and worked with other agencies on legislative language. I have spoken with leaders in the House and Senate committed to protecting consumer privacy and trust. I am grateful for the leadership in this area of the Senate Commerce Committee – Chairman Jay Rockefeller in particular – and to the House Subcommittee on Commerce, Manufacturing and Trade. House Subcommittee Chair Lee Terry and Ranking Member Jan Schakowsky recently formed a bipartisan privacy task on privacy, and we look forward to working with them and with all members of Congress.

Legislation should not wait for some data disaster to happen that undermines the trust essential to a successful digital economy. One byproduct of the unauthorized disclosures about NSA surveillance has been to heighten awareness of just how much data each of us generates: data about data, data from various devices, data traveling and residing on multiple networks.

Studies released last year from EMC and Nasscom estimate that 90 percent of what is being labeled "big data" was created in just the last two years. These enormous data flows create economic opportunities for entrepreneurs and innovators to create new products and improve our lives – so long as there is trust in the system. But the scope and pace of data collection exceeds what even the most informed consumer can adequately grasp, much less manage.

We cannot go backwards. I don't know what comes after yottabyte, but I know whatever it is soon will be used by data engineers and then enter general usage. Our cars, our appliances, our

streets, and other parts of the world around us will continue to expand the volume and variety of data streams. The data they generate is like water: it will find ways to flow.

We should not react in fear. We can only move forward, but we do need to appreciate both the risks and the benefits from the proliferation of digital data.

Big data – massive aggregation and mining of unstructured data – is about much more than business opportunity or convenience when we order books or films. Take, for example, breakthroughs in medical research from aggregated health care records that can produce information far more robust than the limited populations of medical trials.

The drug Herceptin was developed through identification of the HER-2 oncogene from records of 9,000 breast cancer patients. IBM is working with hospitals and the IBM-WATSON natural language system to collect anonymized medical records in ways that protect privacy and analyze unstructured data applying the power of new analytic technologies across many different text-based medical records previously unintelligible to computers.

But this same ability to apply predictive analytics and other tools to greater and greater volumes of information may have a real impact on individual autonomy. Correlation is not causation, big data sets are more granular but not necessarily more precise, and just because data says some outcome is probable does not mean it will happen. The more sensitive that outcome is, the more careful the use of that data must be.

Such risks cannot be addressed by the marketplace alone. We have a far-from-perfect market when only one side of a commercial bargain has good information about what is being exchanged.

The model that underlies U.S. consumer privacy protection today is notice-and-choice, but you don't need to be a privacy geek to understand this approach no longer is sufficient. It's simply not practical to read every notice, and there is a disconnect between what consumers think is true about the obligations online companies undertake and what some companies actually do: surveys show the majority of consumers see a link on a home page to a privacy policy and simply assume this means their privacy is protected.

We need a better approach that ensures consumers actually are treated in ways consistent with a common set of baseline expectations, regardless of where they live or what business they deal with. We need to move away from fictions and formalities around the collection of data to focus in practical terms on what happens to that data.

We need to do so in ways flexible enough to adapt to differing consumer expectations and differing business models, but clear enough to provide individuals with reasonable certainty that their information will not be misused. A cornerstone of the Blueprint is the principle that the relationship between a consumer and a business provides a context in which to understand the consumer’s privacy expectations and that uses by the business of the consumer’s information should be consistent with this context. No surprises.

This Context Principle recognizes that consumers understand the need to provide some personal information data to take advantage of online services and that, in an age of unstructured data with evolving uses, consent forms and pre-defined use limitations can be unnecessarily restrictive. The essence of the Context Principle, like the Blueprint as a whole, is to promote more interactive privacy practices across all sectors.

Work toward legislation will continue after I've left the Commerce Department and I know my Commerce colleagues stand ready to work on a bipartisan basis with Congress to make baseline privacy legislation a reality.

One major element of the White House Blueprint is international engagement. The interoperability of international privacy regimes is important because a significant proportion of international trade is enabled by flows of digital information across borders. According to OECD estimates, in 2008 among OECD members that reported information, over 50 percent of services exports and nearly 50 percent of services imports trade were enabled by information and technology services. This volume has only grown since then.

When it comes to engagement with Europe on privacy, much gets made of differences between the U.S. and European approaches. My task has been to emphasize our common ground. We share common principles with our European friends and others around the globe. The same FIPPs developed in the 70s in the United States that are a cornerstone of our Privacy Act of 1974 also underlie the 1995 European Privacy Directive and other international privacy frameworks.

And, by the process of accretion that is part of our common law system, the United States has developed a strong privacy system, building on robust protection in sectors with significant privacy concerns like financial and healthcare information and for vulnerable groups like children, and active enforcement by the FTC and state attorneys general to protect consumers from unfair and deceptive trade practices and data breach laws in most states. This approach seeks to achieve benefits like those in other jurisdictions, most notably Europe, and achieves outcomes – privacy practices – that are comparable.

As we meet today, though, I have to acknowledge the task of bridging gaps between the United States and Europe on privacy has gotten harder. The heated rhetoric in response to disclosures about U.S. Government surveillance has brought dark clouds over our engagement. Let me touch briefly on the programs discussed on so many front pages lately.

I won't recapitulate the mechanisms in place to protect liberty and privacy in the context of surveillance authorized by law. My colleague Bob Litt of ODNI did a thorough and thoughtful job of that a few weeks ago. I have profound respect for the job that lawyers and privacy staff at ODNI, NSA, DOJ, and other agencies have done to put in place safeguards to insure compliance with the Constitution, laws, and good privacy practices. To put into perspective the breadth of collection and review of Internet traffic, the NSA recently released an analysis of its information-gathering from this traffic. It showed that, once you take into account the volume of traffic they "touch," and then the limited traffic actually reviewed, this amounts to

only 0.00004 percent of Internet traffic. Very simply, the United States Government is not listening to or reading everything said by every citizen of any country.

A White Paper released yesterday by the Hogan Lovells law firm analyzed the published transparency reports of companies that have received government requests for information and found that, taking into account differences in population and Internet usage, "the U.S. government requests information from these providers at a rate comparable to – and sometimes lower than – that in other countries, including many European Union member states."

President Obama has made clear his – and his Administration's – commitment to privacy by welcoming a discussion about privacy and national security; directing the U.S. intelligence community to declassify more information; expressing his desire to work with Congress on reforms to the Section 215 program and to improve confidence in the oversight of the FISA Court; meeting with the Privacy and Civil Liberties Oversight Board and backing its independent review; and directing creation of an independent group to review our technical collection capabilities. This group will examine whether we employ these capabilities in ways that optimally protect our national security and advance our foreign policy as well as other policy considerations and make recommendations to the President. The PCLOB intends to report on the Section 215 and 702 programs, including collection of bulk metadata, and plans to report as much as possible in unclassified form.

The Administration also has voiced support for updating the Electronic Communications Privacy Act (ECPA). Republicans and Democrats, law enforcement and the tech sector, and advocates of all stripes have argued that we must update ECPA for modern communications technologies. We are encouraged by the progress in Congress toward a proposal that enhances privacy by creating a baseline warrant-for-content approach, while accounting for certain limited government functions where such a requirement could pose a problem.

Let me to underscore a theme of my remarks here. Privacy is deeply embedded in American values and laws and the United States is the source of many of the privacy principles that underlie modern privacy regimes around the globe. Transborder trade – and especially transatlantic trade – now relies on the continued open flow of data, and cutting off these flows would cause significant and immediate economic damage. Moreover, it would lead to loss of competitiveness on both sides as other economies around the world that embrace open Internet architectures and freedom to experiment with data analytics offer havens for innovators. Our economic future is at stake in our international engagement.

I do not take European concerns about privacy protection lightly. I understand the experiences that inform some European privacy laws. I bear some of the same imprints. My mother was one of the refugees who flooded out of Paris in front of the Nazis. Her sister was interned by the Vichy government for harboring fugitives, my grandparents' house was destroyed because it might offer a spotting post for Allied troops, and another grandmother's brother and sister were transported from Terezin to die at Treblinka. As a child, I lived in an occupied Berlin still scarred by bombed and burned and shot-up buildings.

As President Obama has said, there is room for debate about the scope of intelligence-gathering, and publicly disclosed audit reports reflect that systems are human, not perfect. We welcome that discussion. But we should have an honest discussion that is based on facts.

If we are going to have a discussion about the United States, let's also look at how other countries compare. How many other countries have an independent Privacy and Civil Liberties Oversight Board to review their intelligence-gathering? How many other countries have Privacy and Civil Liberties Officers within their intelligence and law enforcement agencies? How many other countries subject their intelligence-gathering to audits? How many other countries have a body like the FISA Court that supervises some form of foreign intelligence collection directed at citizens of other countries?

The issues relating to surveillance are part of a broader discussion about global norms online. Most trade agreements carve out actions taken to further the national security of the parties and both the 1995 European Privacy Directive and draft Regulation include exemptions for national security data processing activities. The United States does not use its intelligence capabilities to repress citizens of any country because of their political, religious, or other beliefs. It does not use intelligence capabilities to steal trade secrets of foreign companies and enable our companies to compete unfairly in the global marketplace.

As this discussion continues, I hope that heated and disproportionate rhetoric, protectionism, and politics will not crowd out a thoughtful discussion of evolving norms. We cannot let that vital debate devolve into mutual recriminations that undermine the free flow of information over global communications networks and technology that are bringing extraordinary progress to economies, societies, and freedom around the globe.

This is especially true in the relationship with Europe. The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, and supporting millions of jobs on both sides of the Atlantic. Both economies have the ambition to expand the relationship and support job creation through the Transatlantic Trade and Investment Partnership (TTIP). Data flows will be a major part of that negotiation.

The structures in place to protect the private data of citizens on both sides of the Atlantic support billions of dollars of economic activity and a wide variety of creative and innovative activity that have made our lives better, safer, and healthier.

A vital bridge for these connections has been the U.S.-EU Safe Harbor Framework. Put in place over a dozen years ago by the Commerce Department and the European Commission, this framework enables U.S. companies that transfer personal data of EU citizens to servers in the United States to certify their adherence to privacy practices the EU recognizes as adequate.

Today, more than 4,000 companies have subscribed to the Safe Harbor Framework. Many of these are U.S. subsidiaries of EU companies that also rely on the framework. The Federal Trade Commission (FTC) provides robust enforcement of companies' Safe Harbor commitments. FTC actions against some of the largest U.S. tech companies have included allegations that they failed

to abide by the commitments under Safe Harbor. And the resulting consent decrees are protecting hundreds of millions of European citizens today.

Safe Harbor is a fundamental building block of the trade relationship between the United States and Europe. In March, 2012, Commerce Secretary Bryson and EU Vice President Reding issued a joint statement "reaffirm[ing] their respective commitments to the U.S.-EU Safe Harbor Framework" and recognizing that the Safe Harbor "is a useful starting point for further interoperability" in our approaches to privacy protections.

As we seek to deepen the U.S.-EU trade relationship through the TTIP, this starting point for interoperability only becomes more important. A 21st century, free and open transatlantic marketplace will depend even more on digital information to transact business and move goods and services across the Atlantic and around the globe. Any step back from Safe Harbor would send the trading relationship between the U.S. and the EU backward, just as the U.S. and Europe are trying to find common ground toward reducing regulatory barriers and increasing regulatory cooperation.

We also have broader stakes in common with Europe than TTIP and our commercial relationship. We have been united in our commitment to an open environment that allows free communication among citizens of the world, enabling flows of information, creativity, innovation, and freedom around the world. A bulwark of this commitment has been two decades of support for an open Internet, and for an Internet governance structure primarily led by the private sector.

It would be a sad outcome of the surveillance disclosures if they led to an approach to Internet policy making and governance in which countries became a series of walled gardens with governments holding the keys to locked gates. But that is where we will end up if all data has to stay on servers located in the nation in which a citizen lives or where a device is located. The digital world does not need another Great Firewall – in Europe or anywhere else.

Let me circle back to my beginning – the work of the Commerce Internet Policy Task Force. We began that work because it is vital to a foundation for sustained economic growth, especially in sectors that are leaders of the U.S. economy. We believe that building this foundation requires new rules for the digital economy that would augment the rules of physical world in ways that are adapted to rapidly-changing technology operating in global networks.

I have learned that there are no easy answers; that transposing to digital space rules that apply in the physical world is possible, but it takes thoughtful attention to unintended consequences; and that such consequences can cascade quickly – adverse consequences can spread like a virus.

These challenges span a broad range of issues. One of my roles in the Obama Administration has been to bring into discussions of security and law enforcement – cybersecurity, IP theft, telecommunications supply chain integrity, network operations, surveillance authorities – a set of business and technology issues: the impact on business, trade, on Internet governance, on innovation.

In the past four years, the Commerce Department has been at the forefront of interagency efforts to get the right answers on critical policy issues such as concerns about the potential impacts of the SOPA/PIPA copyright legislation or the privacy risks of the CISPA cybersecurity proposals. Our goal, then as now, has been to preserve and promote a vibrant online platform for innovation, economic growth, and citizen engagement.

So, this is an important conversation to have – here in the United States, with our European allies, with countries and citizens around the world: about privacy and about intelligence gathering, yes, but also about cybersecurity and intellectual property, about Internet governance and freedom, about norms of due process, and about innovation and our economic futures. And this is a conversation in which the Commerce Department will remain at the forefront.

It is a discussion I welcome because I know the United States cherishes liberty and privacy, as well as security and growth. It was a European – a Frenchman, Alexis De Tocqueville – who observed that "The greatness of America lies not in being more enlightened than any other nation, but rather in her ability to repair her faults." In that spirit, we are prepared to have a serious discussion at home and abroad, with honesty and humility. We hope our international partners will do the same.

I look forward to continuing to be engaged in this conversation even after I leave government. While I will miss very much the chance to participate as a member of the Obama Administration, I know my voice will still be heard as a citizen.

Thank you, and I look forward to your questions.