Testimony of Daniel J. Weitzner
Associate Administrator for Policy Analysis and Development
National Telecommunications and Information Administration
United States Department of Commerce

Before the
Subcommittee on Human Rights and the Law
Committee on the Judiciary
United States Senate

Human Rights Challenges Facing the Technology Industry

March 2, 2010

I. Introduction.

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee, thank you for this invitation to testify on behalf of the Department of Commerce and the National Telecommunications and Information Administration (NTIA) on certain global challenges facing the Internet industry. As an advocate of economic growth, innovation, and exports, the Department of Commerce's goal is to support a global, open Internet as a platform for the free flow of information goods and services. In the Internet marketplace, as with all other major areas of economic activity, the Department of Commerce is committed to our role as partner with U.S. companies, large and small, as they grapple with the challenges associated with operating in countries that do not share the commitment of the United States to openness, transparency and the free flow of goods and services. The Internet is a globally interconnected network, meaning that even the smallest U.S. Internet start-up can be reached by any Internet user globally, and that, conversely, the U.S. economy can become the target of foreign laws, rules, and actions even where it has no foreign presence.

Since its commercial launch, the Internet has proven to be not only an extraordinary platform for information in sharing but also a primary medium for the efficient, free flow of goods and services. Over the last 15 years, it has been a driver of growth in virtually all sectors of the U.S. economy. This growth generates jobs, and it sustains our international competitiveness in an increasingly interconnected global economy.

Between 1999 and 2007, the U.S. saw an increase in business-to-consumer Internet commerce by over 500 percent. When business-to-business transactions are taken into account, online commerce in 2007 accounted for over three trillion dollars in business revenue for U.S. companies. It is critical that U.S.-based online commercial interests be able to operate under transparent rules and on a level playing field.

Today, I would like to summarize what the Department of Commerce has observed as some of the challenges facing U.S. industry, discuss the importance of transparency in the Internet, and update you on current Department of Commerce activities to support the worldwide commercial robustness of the Internet.

II. Challenges Faced By U.S. Companies.

U.S. companies face a number of challenges offering Internet-based goods and services around the world that threaten the continued growth of the Internet as a platform for global commerce. There are three specific challenges faced by U.S. companies that the Department of Commerce believes are particularly troubling.

First, an increasing number of foreign countries are imposing forms of censorship on the Internet. As a result, U.S. companies are often pressured to block or filter Internet content or

communications absent any evidence of illegality and based on rules that can be unclear, not committed to writing, or are enacted without adequate due process or transparency. U.S. companies are placed in the untenable situation of trying to divine what content they should filter in order to satisfy the arbitrary and not transparent requirements imposed by certain foreign nations. Often faced with threats of personal criminal or civil liability for their employees, U.S. companies have been forced to either over-block content to the detriment of their customers and their own business interests, or under-block (from the perspective of the foreign government) thereby risking loss of liberty or the ability to do business there. These restrictions impede the flow of legitimate products and services by placing unreasonable and vague compliance burdens on U.S. businesses.

Second, U.S. companies are often subjected to excessive and sometimes repressive surveillance demands from foreign nations. Foreign governments may require Internet Service Providers (ISPs) or other Internet businesses to provide assistance in electronic surveillance without due process or adequate judicial supervision. For example, some governments require that all Internet traffic be routed through one government-controlled access provider or facility, so that they can use monitoring software to track activities of individual users. Further, some governments require U.S. businesses operating within their borders to conduct surveillance or surrender stored information about users. Forcing U.S. Internet companies to comply with secretive government surveillance demands also undermines trusted consumer relationships between U.S. companies and their customers, both in the U.S. and worldwide.

Third, U.S. companies risk being the victims of hacking attempts sponsored by overseas criminals, foreign agents or loose-knit groups of the same. These threats place at risk the

integrity of data held in trust by U.S. companies on behalf of their employees and customers. It puts at risk valuable commercial information including intellectual property, customer data, internal proprietary information, and confidential business plans. And, in certain circumstances, these hacks can become the pretext for forced compliance with government imposed technical standards that are overly prescriptive. This last practice puts all network services at risk and unfairly disadvantages U.S. companies that tend to rely on global, voluntary consensus-based standards. Furthermore, in this era of globally-integrated services and cloud computing platforms, cybersecurity threats in one country have implications far beyond the borders of that country, putting proprietary information, customer data and operational readiness at risk of an entire global enterprise. These risks can constitute a price so high that U.S. companies may avoid doing business altogether in such environments.

III. Greater Transparency is key to the operation of the global, open Internet.

Secretive, aggressive treatment of Internet users and online service providers such as those described here threaten one of the most important aspects of the Internet's *modus operandi* – transparency. Transparency has been a vital feature of the Internet's technical design, its cooperative administrative systems, and many of the business arrangements that have led to its breath-taking, global success. Open technical standards have enabled rapid innovation, high quality technical design, and global interoperability of underlying network services and the applications that run on those networks. Threats to global technical transparency for the purpose of sheltering domestic activities and vendors in a single country are barriers to global online commerce and pose a threat to leading U.S. technology companies

– as well as other companies that operate in countries dedicated to openness and due process of law. Just as important as technical transparency is openness and clarity of laws that apply to Internet-based commercial and non-commercial activity.

Transparency is an indispensible foundation of the Internet's global reach. Without technical and operational transparency, the ability of the Internet to function as a single, global platform will be gradually undermined. While recent security threats have directed our attention to vulnerabilities in the Internet's infrastructure, we must not lose sight of the extraordinary engineering achievements that enables to citizens and business of the world to communicate through a common platform.

In looking ahead towards any new U.S. government involvement in this arena, the Department of Commerce will continue its tradition of working with stakeholders in the U.S. and abroad to develop government-industry-civil society partnerships that encourage all businesses to operate with transparency, wherever located. From a public policy perspective, we fully understand that safeguarding the Internet's openness – and even fostering greater openness – is a complex task. For the most part, Internet governance historically has done well with private sector leadership. And despite recent challenges, we are hopeful that industry will continue to foster concrete, evolutionary changes in the way businesses respond to overly intrusive government restrictions. As evidenced by the creation of the Global Network Initiative (GNI) several years ago, industry, civil society organizations, investors and academics all have vital leadership roles to play in helping businesses develop credible, accountable systems. We will know that these systems are succeeding when they enable us to assess both company and country compliance with openness and internationally recognized human rights

laws and standards. The Department of Commerce and NTIA have been heartened by GNI's ongoing efforts to develop and refine a voluntary code of conduct for technology companies that do business in challenging governmental environments. We continue to monitor their progress. At the same time, we believe we have an ongoing obligation to assess whether and, if so where, greater government support to the private sector might be warranted.

IV. Commerce Department Initiatives to Address the Broad Challenges of Internet Policy.

Ensuring that the Internet is open for innovation and social progress both domestically and globally is a vital task for the nation and, therefore, for the Department of Commerce. To that end, our Department assembled months ago an Intra-agency Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment. Along with this public policy assessment, we are exploring steps to assist companies to operate responsibly and competitively even in markets that lack the level of openness, due process, and respect for internationally recognized human rights laws and standards that we believe to be vital to the Internet.

The Department of Commerce is drawing upon our expertise across many bureaus, including international communications policy, trade, intellectual property, business advocacy, and corporate responsibility, to develop comprehensive responses to these issues. Our work began with the Administration's efforts in developing an Internet privacy and cyber-security framework that meets the needs of the 21st Century information economy. Thus far, the Task Force has convened listening sessions with officials from major U.S. corporations and technology companies across the country. In these sessions, Commerce representatives

solicited private sector input on how to enable innovation in information services, while protecting individual privacy rights and security both in the United States and around the world. We have now added to that agenda consideration of trade barriers such as the concerns identified in this hearing, along with online copyright enforcement and the future of multi-stakeholder governance. In the coming months, the Task Force will be releasing a Notice of Inquiry in the Federal Register to reach out further to American industry and civil society groups. It is anticipated, that based on this feedback, the Task Force will make formal recommendations to the Secretary of Commerce on public policy positions and operational initiatives to enhance the free flow of information goods and services on the Internet.

V. Conclusion.

Today, in certain parts of the world, U.S. companies face increasing pressure to comply with policies and official practices in ways that conflict – or at least create substantial tension – with internationally recognized human rights laws and standards. This impedes the free flow of information goods and services on the Internet and has a negative impact on global economic growth and innovation. The Department of Commerce believes that greater transparency is essential to preserving an open Internet, which, in turn, is a key priority of the Obama Administration. Transparency shines a positive light on effective national policy and regulatory practices and is equally important as a tool to draw attention to impediments to the free flow of information goods and services. We look forward to continuing our work with our colleagues at the State Department, other federal agencies, and Congress to develop the most effective

policy framework to enable U.S. companies all citizens of the world to have access to an unfettered flow of information goods and services online.