Mark Chandler
Senior Vice President Legal Services, General Counsel and Secretary
Cisco Systems, Inc.
May 20, 2008
U.S. Senate, Committee on Judiciary
Subcommittee on Human Rights and the Law

Mr. Chairman, Members of the Subcommittee:

My name is Mark Chandler, Senior Vice President and General Counsel of Cisco. Thank you for the opportunity to address some very important and difficult issues that speak directly to the future of the Internet.

First, I'd like to share with you some background about the products our company is best known for. Networking equipment - routers and switches - forms the core of the global Internet and most corporate and government networks. Cisco has often been described as the "plumbers" of the Internet, as our technology constitutes the "pipes" that connect one location to another. Originally our products were designed for communications within private or corporate networks. When the public Internet emerged in the mid '90s, our products found immediate application for worldwide use. We now have many competitors around the world who build products that perform similar functions. When you send an email in your office to your children or grandchildren, the digital language that makes up that email is routed through equipment made by Cisco or our competitors

Over the last year, we have seen remarkable growth and transformation related to the Internet. The Internet continues to expand around the world and new applications such as collaboration tools and the use of video are transforming how we work, live, play and learn. More than 1.4 billion people now use the Internet, an increase of 300 million people in just one year. And new mobile devices such as the Apple iPhone have enabled millions of people to do what they want, when they want, with whom they want.

But at the same time, we have observed some troubling events and challenges related to the manipulation of Internet technology. Later this month will be the first anniversary of an unprecedented cyber attack that crippled the Estonian government and commercial networks. The attacks were labeled "cyber terrorism" and prompted NATO to create a new multi-national initiative to prevent such incidents. And in February, an ISP in Pakistan caused an international incident when it rerouted its computers to block YouTube from being watched in the country. The act had much broader implications by effectively hijacking the site for several hours worldwide. These incidents demonstrated that despite the Internet's redundant nature, it can still be disrupted by unilateral actions

and by cyberattacks. Every major corporate and service provider network is subject to nearly constant attack.

Attacks can take many forms, some of which are referred to as worms, viruses, denial of service attacks, and more. Network management and security capabilities are essential to mitigate attacks and thus enable information flow. No network can be administered by our customers without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet and the Internet would likely not exist as it does today. For example, without these tools, the Government of Estonia would have been powerless against the attacks it faced last year.

These tools are essential for many reasons. But the technology that is used to manage and protect against hackers or viruses is the same generic technology that filter or control Internet access by children, or the illegal downloading of copyrighted material. If, for example, a network administrator knows that a certain website is dangerous to her network because a virus or spyware has been downloaded from that site, or because the site is pornographic, she can use IP address blocking (each website and user on the Internet has an IP – Internet Protocol – address - the equivalent of a phone number) to protect her network from that site. This technology is a customary part of network management software of all major suppliers of Internet equipment -- Cisco's and our competitors' -- and is basic to network functionality. Whether for security or the management of information, the technology is one and the same. The filtering that occurs is implemented by the owner or administrator of the network using technology that is available regardless of the manufacturer.

In no country has the issue of the Internet and how it should be managed been more prominent than in China. China now has the largest Internet population in the world with 220 million users. There is no question that the Internet has been good for China and its people. It has provided unprecedented access to information. It's transforming China and its economy and it's helping the Chinese people engage more with the world.

Perhaps the most vivid example of the dramatic changes the Internet has brought to China is the response to last week's earthquake in the southwest region of the country. With mobile communications systems down or damaged, the Internet became a critical source of information for family and loved ones, as well as the rest of the world. Within minutes, pictures and videos from the region were online. That stands in stark contrast to the events in Tangshan 32 years ago, when the world received no official confirmation for months that a 7.8 magnitude earthquake had even happened, despite the deaths of an estimated 240,000 people and the destruction of much of that region.

As a company that supports free expression and open communication on the Internet, and believes that its products inexorably drive the world toward more open communication, Cisco respects the strength of conviction of those who bring concerns forward about efforts of various governments to censor freedom of expression on the Internet and persecute those who attempt to use the Internet for purposes of political speech. But we also must respond when Cisco is erroneously linked with these efforts.

To set the record straight, it is important that the Committee understand that Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information. Furthermore, Cisco sells the same equipment worldwide. Finally, Cisco is not a service or content provider, nor are we a network manager. Allegations that Cisco has built a "great firewall" in China or elsewhere confuse the provision of the basic pipes of the Internet, which include basic security features that every network must have, with more specific technological mechanisms which may be implemented to achieve the invasive effects that have raised specific concerns.

Some countries have chosen to restrict or limit access to information on the Internet based on political considerations, rather than on the freedoms that we enjoy in this country. While many have commented on the activities of the Chinese government in this regard, the issue is, in fact, global. Some Middle Eastern countries, for example, block sites critical of their leadership. And judicial action has been taken in France due to the failure of an operator to block local users' access to some types of information.

Cisco, however, has not and does not design products to accommodate political censorship. The tools built into our products that enable site filtering are the same the world over, whether sold to governments, companies or network operators. The features in our equipment are "off the shelf" and not altered in any way for any market or region. Similar technology is available from at least a dozen other US, Canadian, European and Chinese companies. Because of the threats to network operations that I previously mentioned, which exist around the world, there is no feasible way to manufacture equipment without these capabilities and it would not be desirable or sensible to do so. The management of information flow by a customer cannot be prevented by Cisco unless we are to also prevent the originally intended use of this technology, which would expose the Internet to the full risks of inevitable daily attacks. Networks attached to the Internet would literally stop working.

Cisco <u>does</u>, however, comply with all U.S. Government regulations which prohibit the sale of our products to certain destinations, or to certain users or to those who resell to prohibited users. We have not sold and do not sell our equipment to the countries listed on the U.S. Department of Treasury's OFAC (Office of Foreign Assets Control) list of embargoed nations, and we comply fully with all aspects of the Foreign Relations Authorization Act passed by Congress in the wake of Tiananmen Square.

More broadly, Cisco has played a leading role in helping to make Internet technology ubiquitous, allowing hundreds of millions of people in nearly every nation around the world to access information and ideas previously unavailable or inaccessible. Because our products are designed to expand the reach of communications systems, we build to open, global standards, and we vigorously oppose attempts by certain governments to balkanize the Internet by setting country-specific security requirements. We do not design custom or closed Internet systems. The Internet technology may not be perfect -- and the Internet itself can be misused -- but there has been no greater force in spreading

the power of ideas than the single worldwide Internet. The key to its growth and the flow of information it enables has been the standardization of one global network. This has been and remains the core of Cisco's mission.

For some, the Internet is a tool that liberates individuals from the constraints of time and distance, empowering those who previously had no access to the world's store of information. Some are fearful of this liberation as a mechanism for empowering non-state actors. Still others see the Internet as a tool used by governments to control content.

The policy response is complex. Among the questions that we have historically raised are: Has the Internet helped promote a dramatic increase in access to information in regions where content is nonetheless subject to certain limitations? Does active public engagement in such countries help to influence policy decisions? What policies will best help constrain political and other censorship contrary to First Amendment principles? If countries that engage in censorship are to be denied U.S. Internet technology, will those countries establish closed-standard Internets of their own to further restrict access to information?

To that end, policies that encourage governments to build their own Internets could be highly counter-productive by removing the leading platform for free expression. At the same time, Cisco sees benefit in the U.S. Government in making freedom of expression an integral part of its diplomacy. One means to do that that has been proposed is through the creation of an Office of Global Internet Freedom within the International Broadcasting Bureau. In doing so, the U.S. Government would be unambiguous about its intentions.

When the Internet first became a societal tool, it was largely available in western countries with broadly shared viewpoints about freedom of expression. It is inevitable as the Internet grows globally that there are differing viewpoints about its role in society. That has been true of every transformational technology, for example the television in the 20th Century.

Our challenge going forward is to ensure that as the Internet is globalized, we don't let it be balkanized in a way contrary to our goal of expanding its reach and liberating power.

Thank you for inviting us to appear before you today.

END