



**Testimony of Nicole Wong, Vice President and Deputy General Counsel,
Google Inc.
Before the U.S. Senate Judiciary Committee Subcommittee on Human
Rights and the Law
Hearing on "Global Internet Freedom and the Rule of Law, Part II"
March 2, 2010**

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee.

Thank you for bringing attention to the important issue of Internet censorship and for giving me the opportunity to discuss today's global challenges to freedom of expression and access to information online. Internet censorship is a growing global problem that not only raises important human rights concerns, but also creates significant barriers for U.S. companies doing business abroad. As Google's Vice President and Deputy General Counsel, I lead the team that helps Google promote free speech around the world.

The number of governments that routinely censor the Internet has grown from a handful in 2002 to more than 40 countries today. Even in countries that are just beginning to make the Internet available to their citizens, governments are simultaneously building sophisticated tools for blocking and filtering content. Repressive regimes are developing ever more advanced tools to use against dissidents and are sharing censorship tactics across borders. Human rights observers have noted that these governments are "baking in" censorship tools for the Internet rather than chasing after criticism that has already been aired.

The lack of transparency and accountability in blocking and filtering is also a grave concern. Over the last several years, we have seen an increasing number of governments, even democratic ones, choose to blacklist certain sites that they deem harmful without providing any formal oversight of process or meaningful ability to appeal. In the next few years, the Open Net Initiative predicts that we will see more targeted surveillance and increasingly sophisticated malware being used to make the monitoring and documentation of government activity even harder.

But despite these challenges we remain optimistic about the ability of technology to empower individuals and realize the potential for a global Internet community. We believe that maximizing the free flow of information online can help to increase openness and prosperity even in closed societies.

As Google invests in new countries, we look to the following three principles to help us protect online freedom of speech and increase access to information:

- **Access** - maximizing access to information on the Web and tools for the creation of content.
- **Transparency** - notifying users when information has been removed by government demand.
- **Trust** - retaining the trust of our users by protecting their privacy and security from governmental acts intended to chill speech.

With those principles in mind, I would like to address four main issues in my testimony:

First, our situation in China.

Second, the global challenges Google and other U.S. companies face every day from governments who seek to limit free expression online.

Third, the economic implications of censorship.

And finally, the need for governments around the world to do more to reduce Internet censorship and support free expression online.

China Update

So let me start by updating you on the situation in China.

We launched Google.cn, our Chinese search engine, in January 2006 in the belief that the benefits of increased access to information for people in China and a more open Internet outweighed our discomfort in agreeing to censor some results. While we have faced challenges, especially in the last 12 to 18 months, we have also had some success.

Google is now the second most popular search engine in China, behind Baidu, and we were the first search engine in China to let users know when results had been removed to comply with Chinese law. Use of our maps, mobile and translation services is growing quickly. And from a business perspective, while our China revenues are still small in the context of our larger business, the last quarter of 2009 was our most successful quarter ever in China.

However, in the last year we have seen increasing attempts to limit free speech on the Web in China. Numerous sites including YouTube, The Guardian, Facebook, Twitter, Blogger and Wikipedia have been blocked, some of them indefinitely. In addition, last June the Chinese government announced that all personal computers sold in China would need to be pre-loaded with software that could be used to filter online content. After a public outcry and pressure from companies, the proposal was later withdrawn.

Most recently, in mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China. What at first appeared to be an isolated security incident -- albeit a significant one -- turned out upon investigation to be something quite different.

First of all, at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--were similarly targeted.

Second, we believe that a primary, albeit unsuccessful, goal of the attack was to access Gmail accounts surreptitiously.

Third, we discovered in our investigation that the accounts of dozens of U.S.-, China- and European-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. I want to make clear that this happened independent of the security breach to Google, most likely via phishing scams or malware placed on the users' computers.

The attack on our corporate infrastructure and the surveillance it uncovered — as well as attempts over the past year to limit free speech on the Web even further — led us to conclude that we are no longer willing to censor our search results in China and we are currently reviewing our options. This decision is in keeping with our pledge when we launched Google.cn that we will carefully monitor conditions in China, including new laws and other restrictions on our services. As we stated then, if we determine that we are unable to achieve our objectives, we will not hesitate to reconsider our approach to China.

I want to stress that while we know these attacks came from China, we are not prepared to say who is carrying out these attacks. We do know such attacks are violations of China's own laws and we would hope that the Chinese authorities will work with US officials to investigate this matter.

Because this is an ongoing investigation, I am not prepared to say any more about these attacks. However, before moving on to the broader, global challenges we face, I would like to stress that the decision to review our business operations in China was driven by our executives in the United States, without the knowledge or involvement of our employees in China who have worked with dedication and determination to make Google.cn the success it is today.

Other Global Challenges

As I mentioned earlier, Google has become a regular focus of governmental efforts to limit individual expression because our technologies and services enable people with

Internet connections to speak to a worldwide audience. More than 25 governments have blocked Google services over the past few years.

- YouTube: Since 2007, YouTube has been blocked in at least 13 countries including China, Thailand, Turkey, Pakistan, Morocco, Brazil, Syria, Indonesia, Iran, Saudi Arabia, Myanmar, Bangladesh and Turkmenistan.
- Blogger and Blog*Spot: In the last two years, we have received reports that our blogging platform has been or is being blocked in at least seven countries including China, Spain, India, Pakistan, Iran, Myanmar and Ethiopia.
- Orkut: Our social networking site, Orkut, has been blocked recently in Saudi Arabia, Iran and the United Arab Emirates.

This growing problem was underscored by Secretary of State Hillary Clinton in her recent speech on Internet freedom, when she cited cases from Tunisia to Uzbekistan to Vietnam. Let me just highlight one prominent recent example:

This past June, during the protests that followed the presidential election in Iran, the government of Iran ejected foreign journalists, shut down the national media and disrupted Internet and cell phone service. In spite of this, YouTube and Twitter were cited by traditional journalists and bloggers alike as the best source for firsthand accounts and on-the-scene footage of the protests and violence in Tehran.

With YouTube effectively blocked, Iranians continued to upload videos that documented demonstrations, violent clashes between police and protesters, and other scenes of unrest. You may remember, in particular, the graphic video of Neda Soltan's murder on YouTube that became a testament to the vital role that technology plays in giving a voice to those who once were silenced.

In countries like Iran, online platforms like Twitter, YouTube and Blogger are often the only means for speech to emerge from communities closed off by authoritarian governments - particularly in times of political unrest. So it's imperative for governments, companies, and individuals to do more to ensure that the Internet continues to be a powerful medium for expressing political opinions, religious views and other core speech without restriction.

Economic Implications

The debate on Internet censorship is, of course, not only about human rights. At issue is the continued economic growth spurred by a free and globally accessible Internet.

Barriers to the free flow of information online have significant and serious economic implications: they impose often one-sided restrictions on the services of U.S. and global Internet companies, while also impeding other businesses who depend on the Internet to reach their customers.

When a foreign government pursues censorship policies in a manner that favors domestic Internet companies, this goes against basic international trade principles of non-discrimination and maintaining a level playing field. Local competitors gain a business advantage, and consumers are deprived of the ability to choose the best services for their needs. And when a government disrupts an Internet service in its entirety – e.g., blocking an entire website because of concerns with a handful of user-generated postings – the government is restricting trade well-beyond what would be required even if it had a legitimate public policy justification for the censorship.

Opaque censorship restrictions can also be very damaging to the 'host' nation, because they undermine the rule of law and make it very hard for foreign companies to navigate within the law, which has negative consequences in terms of foreign direct investment.

The U.S. government has taken some positive steps to address the means and effects of censorship through trade tools. The United States Trade Representative has sought explicitly to address some of these issues in trade agreements – most recently, in the U.S.-Korea Free Trade Agreement – and we applaud these efforts. And the Commerce Department and USTR have been helpful in the context of particular incidents we have encountered in the past.

But governments need to develop a full set of new trade rules to address new trade barriers. We encourage further efforts along these lines, by the U.S. government and other governments to redress favoritism shown by some governments for indigenous companies over U.S.-based corporations. We should continue to look for effective ways to address unfair foreign trade barriers in the online world: to use trade agreements, trade tools, and trade diplomacy to promote the free flow of information on the Internet.

How Governments Can Support Free Expression

Internet censorship is a challenge that no particular industry -- much less any single company -- can tackle on its own. However, we believe concerted, collective action by governments, companies and individuals can help promote online free expression and reduce the impact of censorship.

As I noted previously, our business is based on the three principles of access, transparency, and retaining the trust of online users. These principles are not exclusive to Google, and there are ways that the public and private sectors can work together to advance them.

First, making every effort at both the grassroots and government level to maximize access to information online. The State Department recently issued a request for proposals on projects to help citizens on the ground access information they would not otherwise be able to share or receive. Google supports the joint commitment of Congress and the Obama Administration to provide funds to groups around the world to

make sure people who need to access the Internet safely get the right training and tools. This is a great step forward, and we believe much more can be done to support grassroots organizations that develop technology to combat Internet censorship.

Second, establishing transparency as a norm when governments attempt to censor or request information about users, or even when a company's network comes under attack. This is a critical part of the democratic process, and governments must strike a balance between law enforcement and proper disclosure, allowing citizens to hold their lawmakers accountable. In many cases the cloud of secrecy around cyber attacks only works to the attackers' advantage because it enables them to operate more easily under the radar. Some of the sensible ideas we've heard discussed to improve transparency include: requiring annual company reports on the levels of filtering being complied with and requests for personally identifiable information from government officials; and greater engagement by the U.S. government with countries that censor the Internet, so any company disclosures result in concrete actions by the U.S. government.

Third, retaining users' trust by committing to protect their privacy and security. There is nothing new about governments using surveillance and intimidation tactics to chill speech about uncomfortable ideas. What is new is the growing deployment of online surveillance toward these ends. To be clear, we fully support lawful investigation by government authorities to protect individuals and companies. But we are committed to protecting our users against unlawful and overbroad government demands for their personal information and ensuring the security of our networks. The global trend toward increasing government access to online communications is of great concern and demands serious review and oversight. In addition, the U.S. should push for improved international cooperation to protect user privacy.

We are also grateful for the efforts of lawmakers -- and in particular your leadership Mr. Chairman -- to bring more companies into the Global Network Initiative (GNI).

As a platform for companies, human rights groups, investors, and academics, the GNI requires its members to commit to standards that respect and protect user rights to privacy and freedom of expression. Additional corporate participation will help the GNI reach its full potential -- and we look to the Members of this Committee for continued leadership.

And finally, ensuring that the U.S. government makes the issue of Internet openness, including the free flow of information, an important part of foreign policy, trade, development and human rights engagement. This includes prioritizing the issue as a matter of U.S. foreign policy, including in various dialogues that the U.S. government pursues with regimes that are heavy Internet restrictors; using trade tools where possible; and perhaps also making it part of the criteria for receiving development aid. Ultimately, governments that respect the right to online free expression should work together to craft new international rules to better discipline government actions that impede the free flow of information over the Internet. We need forward-looking rules that provide maximum protection against the trade barriers of the new technology era.

On the multilateral human rights front, enforcing and supporting the mechanisms of the International Covenant on Civil and Political Rights and others under the UN system (*e.g.*, the UN Human Rights Committee) to demand accountability from governments for Internet censorship is helpful. At the very least, these mechanisms can be better used to shine light on government abuses.

Conclusion

I would like to conclude by thanking Chairman Durbin, Ranking Member Coburn, the members of the Senate Judiciary Committee Subcommittee on Human Rights and the Law and other Members of Congress who have spoken in support of our actions to highlight the importance of upholding the right to online free expression around the world and the challenges faced by U.S. companies. It is only with the attention and involvement of leaders like yourselves that we can make real progress in the effort to protect these basic human rights. We look forward to working with you and other government officials to find viable solutions to maximize access to information, increase transparency and protect users around the world.