Testimony of

Arvind Ganesan

May 20, 2008

Global Internet Freedom: Corporate Responsibility and the
Rule of Law

Written Testimony of Arvind Ganesan
Director, Business and Human Rights Program, Human Rights Watch
To the Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law
Tuesday, May 20, 2008

Mr. Chairman:

I welcome the opportunity to speak on the important matter of global internet freedom. I would also like to thank Senator Coburn, the ranking minority member of this Subcommittee. As someone who is from Oklahoma and whose family still lives there, I'm proud to say that my parents are thrilled at the prospect of delivering my testimony in front of one of their senators.

Human Rights Watch believes that the internet is a transformative force that can help open closed societies and provide the near-instantaneous flow of information to inform the public, mobilize for change, and ultimately hold institutions accountable. We have warned, however, that there is a real danger of a Virtual Curtain dividing the internet, much as the Iron Curtain did during the Cold War, because some governments fear the potential of the internet, want to control it and the companies that provide the services and products tied to it; and users fear the consequences of using it as a medium for openness and accountability.

Today, I would like to address three issues in relation to global internet freedom:

? The actions by some governments to restrict the flow of information and to punish individuals who exercise their right to free expression through this medium.

? The ongoing efforts by industry, nongovernmental organizations (NGOs), academics, and financial institutions to press for self-regulation to ensure that leading companies who provide internet technologies and services are not complicit in abuses or forced by governments to capitulate to their repressive demands.

? The prospects for government-led change and opportunities to ensure respect for human rights, particularly in regard to companies.

Governments

In 2006, the human rights problems related to the internet in China came to light through Congressional hearings; reports by Human Rights Watch, Amnesty International, and other NGOs; and the press. Through those revelations, the public learned that the US company Yahoo! had provided user information to Chinese authorities that led to the imprisonment of online activists for years. We also learned that US companies, including Google, Microsoft, and Yahoo!, censor their search engines in China, in anticipation of what Chinese censors expect and in addition to what the Chinese government's firewall prohibits.

However, China is not the only government that actively tries to suppress its critics in the virtual world. Since 2006, there are other examples, both of activists being intimidated or silenced for their efforts and of restrictions that governments impose on the internet by controlling both providers and users:

? Just two weeks ago, on May 7, 2008, Egyptian officials beat Ahmed Maher Ibrahim, a 27-year-old civil engineer. His crime? He used Facebook to support calls for a general strike on May 4, President Mubarak's 80th birthday. Few people actually participated in the strike, but three days later, he was abducted by Egyptian officials in civilian clothes, beaten and insulted at New Cairo police station, then taken to the headquarters of the Interior Ministry's State Security Investigations (SSI) department where he was subjected to more beatings, and threatened that they would sodomize him with a broomstick. He was released without charges on the morning of May 8, but his captors asked him for the password to the Facebook group that he reportedly started, asked him about other participants in the group (whom he did not know), and threatened to beat him even more severely the next time SSI detained him.

? In Russia, Saava Terentev, a musician in a town a little over 600 miles east of Moscow, is being tried as an "extremist" because he spoke out about corruption in Russian law enforcement after reading a newspaper story about a newspaper being harassed by the authorities for reporting on corruption. He issued a harsh critique of corrupt police in a blog posting and an extremely offensive, but clearly ironic, "modest proposal" that they be burned in the public square. It was shortly deleted by the blog's owner, but now the authorities are prosecuting him for his sarcastic rant. We believe that this is the Russian government's first test case to try to use a law to restrict free speech on the internet. Additionally, the government has promulgated a decree that allows unfettered surveillance of the internet and other communications mediums without telling the user or the provider. But they do require the provider (potentially companies) to pay for the surveillance equipment. There are also some troubling proposals that are being circulated in the Duma. One is to regulate websites that receive more than 1,000 hits a day. Another is to separate the Russian internet from the rest of the world, along the lines of the Chinese firewall, so that the government could monitor content and shut down the link between the Russian internet and the rest of the world. Between those efforts and the attempts to go after bloggers it appears that the internet, which is perhaps one of the few open forums left in Russia, is now falling under government control.

? During its crackdown, following protests by monks, Burma's military junta shut down the country's internet connections to make sure no information got into the country and more importantly, that little information got out of the country. In total, the OpenNet initiative found that the junta blocked about 85 percent of e-mail service providers and virtually all of political opposition and pro-democracy sites. Then, in late September 2007, the government apparently disconnected the main telecommunications lines in two cities to stop the flow of information. Some bloggers, however, used satellite and cellphone services. This is a chilling example of how far certain governments will go to stop the flow of information.

? The government of Syria regularly restricts the flow of information on the internet and will arrest individuals who post comments that the government deems too critical. Internet use in the country has exploded in the last few years and could be a crucial medium for the flow of information. However, Human Rights Watch has documented at least five cases since 2005 in which the government has arrested individuals because they posted comments critical of the government online, sent critical e-mails, or posted other information on the web. For example, on June 30, 2007, military intelligence arrested Tarek Biasi because he "went online and insulted security services." He was held incommunicado by the authorities and then sentenced to three years imprisonment on May 11, 2008, for "diminishing national feeling" and "weakening the national ethos." These are not the government's only tactics. Security services often force internet café owners to spy on their customers. In one case, an internet café owner filmed a customer who was sending comments and information to opposition websites outside of the country. On July 25, 2007, the government promulgated regulations that required all website owners to display the name and e-mail of the author of any article or comment on their website. This brazen regulation is clearly intended to chill critical speech by making it easier for the government to identify its critics online, particularly as anonymous postings have become a crucial means for individuals to avoid surveillance, or worse. Finally, the government also blocks websites, most notably those that are critical of the government, such as Arabic opposition newspapers' websites outside of the country.

These are just some of the cases around the world in which governments try to restrict the internet and silence users. What is clear is that government efforts to control the internet have multiplied around the world. While China has in many ways become the poster child for our efforts to stop censorship abuses, for other repressive governments such as those I have mentioned, China provides a model to be replicated. If that model is the ideal for internet repression,

then the role of companies cannot be overlooked since they are clearly part of the Chinese government's efforts to censor the internet and obtain user information. As we have previously documented, Microsoft, Google, and Yahoo! censor their search engines in anticipation of what the Chinese government expects. Blogs have been shut down, and user information has been turned over to the government.

A Voluntary Code of Conduct

On January 17, 2007, leading companies including Yahoo!, Microsoft, Google, Vodafone, French Telcom, and Telia Senoria, along with human rights organizations (including Human Rights Watch, Amnesty International, Human Rights First, the Committee to Protect Journalists, Human Rights in China, Reporters without Borders, and the World Press Freedom Association), socially responsible investors, and academics, started on a process to develop a voluntary code of conduct and process of enforcement to try to curtail censorship and protect user information. We believe a system with three critical features could make a real difference in many censoring countries. These features are: a strong but reasonable code of conduct, an effective but not overly bureaucratic governance process, and independent monitoring of companies that sign on to ensure they actually take steps to curtail censorship and protect their users. Now, almost 18 months later, it would be great to tell you that a code is finalized and a system is in place to address these problems, but instead, we are still negotiating, and in the meantime, internet users are no safer, and censorship continues.

Not every company is in the same place nor is it fair to say companies don't care about human rights. After a high profile lawsuit by the families of jailed cyber dissidents, Yahoo! settled and has set up a fund to help cyberdissidents obtain legal aid. Google has used technologies like Google Earth to monitor some of the world's worst human rights crises, such as Darfur.

However, as laudable as those efforts might be, they do not address steps companies should take to ensure that their operations do not contribute to violations of human rights, such as censorship or the persecution of cyberdissidents. Some companies have been more aggressive, especially those that have faced the most controversy. Yahoo! has raised these issues with the Secretary of State, and some companies, such as Microsoft, have become more rigorous about censorship and the circumstances under which they will take down blogs.

Much more remains to be done. While companies have developed differently in regards to their human rights procedures, a voluntary industry initiative is only as strong as its weakest link. Without disclosing the details of discussions that are under the Chatham House rules, I can say that a fundamental problem is that some companies continue to be very resistant to the idea of independent monitoring, in particular to a system that would allow for an independent third party to assess: 1) whether companies have put policies into place that demonstrate a respect for freedom of expression and user privacy; 2) that those polices are diligently implemented; and 3) that their implementation is effective in curtailing these human rights problems. Unfortunately, we do not have such a system. Right now, the preferred option for companies is a system in which they will decide who the monitors are and what they will see, while companies implement those standards at a pace convenient to them.

In other words, companies will express support for human rights but also ask the public to basically trust them to do the right thing. There are several problems with that approach. First, this is exactly the situation that led to the problems we are trying to solve. Companies have already been opaque and exercised discretion over their actions, and to claim that the same approach will change things is dubious. For example, in China, Google and others choose what to censor. Even though Google and other companies now provide a disclaimer to notify users that censorship occurs, they still decide what to censor and whether they will even challenge the government's actions.

Second, it is difficult to point to a company within the voluntary standards process that has robust human rights policies and procedures in place more than two years after the problems in China were disclosed. Google, for example, has actively resisted such efforts. On May 8, Google's board voted down two shareholder proposals, including one sponsored by Amnesty International and the NYC Pension Funds, calling on the company to implement policies and procedures to protect human rights and another calling for a board committee on human rights. Sergey Brin, the company's co-founder, abstained from the vote and expressed support for human rights, but felt these proposals were not the appropriate way to approach the issue. What he did say was, "I think it makes sense to have

a separate, a group of independent people in Google who meet regularly to discuss [these issues]." Frankly, that is not good enough.

Google's resistant stance and the lack of consensus on voluntary standards raise a fundamental question: What is holding up these corporations from finding an effective means of protecting user privacy and curtailing censorship? It can't be technical or technological challenges because industries like pharmaceuticals are very complex yet regulated. And in the case of internet companies, nobody is calling for a massive new bureaucracy like those that regulate other industries, just an agreement to be independently monitored.

Mr. Brin also recently defended Google's activities in China. "Google has a far superior track record than other search companies with respect to making information freely available," he said. This is a bold statement, but on what basis is he making it and what assurance is Google giving to the public to support this claim? Without some form of independent assessment of their activities, assertions like this simply are not credible.

A key purpose of our joint voluntary initiative is to provide the public with real assurance so that they can have confidence in companies or an industry that claims to oppose censorship and respect user privacy. After all, it will be the public and users who are the victims of censorship and whose information may be turned over to authorities. But that assurance is unlikely without meaningful oversight. A useful analogy is that of airlines. We would not accept that the best way to monitor airline safety is to allow airlines to do it themselves. Instead, we insist that someone else oversee them and are rightly critical of both the airlines and the monitors if they fall down on the job. Independent oversight is a critical component in protecting the public interest and it should be in the case of protecting freedom of expression and user privacy. Independent oversight is especially important with a medium and technologies that have the power to open societies, and because companies have already shown that they cannot or will not do it themselves.

Government Intervention

While we hope and plan to work towards an effective voluntary standard, it is unlikely that voluntary initiatives alone will be sufficient. A voluntary initiative will not apply to companies that do not join and it is difficult to see how it will get effectively implemented in countries where the government is very good at dividing and pressuring companies to capitulate to its demands, sometimes in exchange for access to a lucrative market. And most importantly, a voluntary initiative may be least effective in curtailing governments' efforts to obtain user information about cyberdissidents from companies, because a voluntary effort is not sufficient to stand up against the pressures a government can assert against companies.

For those and other reasons, we believe a regulatory approach is a necessary complement to a voluntary initiative. It would help to ensure that the playing field is level for human rights since rules would apply to far more companies than those who join a voluntary initiative; that there are meaningful consequences for companies who do not respect those standards; it would make it more difficult for governments to force companies into becoming complicit in human rights abuses; and could encourage a more assertive US foreign policy on these issues. There have been proposals circulating in Congress and one is in the House. We believe that any regulation should, at a minimum, contain the following elements:

? A requirement that companies have effective policies and procedures in place to safeguard human rights modeled after provisions in the US Foreign Corrupt
Practices Act.

? A provision that requires companies to catalog and record efforts by governments to censor information.

? A process in which foreign government requests for user information can be referred to US diplomatic channels so that a company and its personnel are at less risk of pressure or retaliation.

? A requirement that companies locate personal information outside of jurisdictions that punish individuals exercising their right to free expression where the authorities may try to obtain personal data to do so.

? A private right of action so that victims can seek redress against companies that violate their rights.

? Clear and aggressive steps that the US government should take to combat censorship and protect user privacy through its foreign policy, trade policy, and other means.

? An examination of whether certain types of hardware and software, such as servers and other equipment, should be subject to export controls because of their capacity to be used by governments to spy on individuals and censor information.

? Effective penalties to deter companies from violating human rights.

? Restricting access to federal funds for companies that do not abide by these standards.

A useful model for this approach is the Foreign Corrupt Practices Act (FCPA). That act allows for companies to face penalties if they do not have adequate systems in place to prevent bribery as well as penalties if they actually engage in corruption. That approach could work quite well in regards to the internet and would easily complement a voluntary initiative since it would require a company to put systems into place to prevent abuses and would also hold it accountable were the company party to abuses. The FCPA also disproves the notion that regulations intended to protect the public good limit companies' ability to do business. The FCPA has been in force for more than 30 years and US business is still thriving abroad. Indeed, Microsoft, Google, and Yahoo! did not even exist when the act was passed, yet they seem to be doing reasonably well.

Companies have said that they might support regulation in theory, but seem to oppose existing efforts. Much like human rights policies and a voluntary initiative, they support them in principle, but apparently, not in practice. It would be helpful to understand how the companies and the industry intend to move forward effectively and credibly in terms of voluntary and mandatory standards. I would welcome the opportunity to come before you again or at regular intervals to report on such progress and would hope that the other witnesses today would do the same.

Thank you again for this opportunity to speak on this important subject.