Global Free Flow of Information on the Internet

A Response to a Notice of Inquiry

From the Department of Commerce's Internet Policy Task Force

Written by Steven L. Moxley

On behalf of The Futurist Society

On Monday, November 15, 2010

Microsoft's MSN service in China blocks the words "freedom," "democracy," and "human rights."[1] Journalist Shi Tao was sentenced to "a ten-year prison term for sending information about a Communist Party decision through his Yahoo email account to a website based in the United States" after Yahoo Holdings (Hong Kong) Ltd. released his information to a criminal prosecutor.[2] While China's efforts to control the flow of information are the most extensive and most publicized, we should not pretend that in China is an isolated case. Nor should we pretend that we, as Americans, are isolated from its effects.

The Open Net Initiative, a partnership between the University of Toronto, Harvard University, the University of Cambridge, and Oxford University, currently monitors online censorship "in over 95 countries."[3] The scope of the problem is magnified when one considers the ends to which online censorship may be put. In testimony before the Senate Judiciary Committee, Shiyu Zhou, the Deputy Director of Global Internet Freedom Consortium, explained:

> In Iran, Cuba and certain other totalitarian countries, information control is often used for manipulation and indoctrination and whipping up anti-US sentiment, as illustrated by the xenophobia fostered online in the People's Republic of China (PRC) following the Tibet crackdown and the Olympics Torch Relay. Violence begins with hate, and hate begins with distorted information.
>
> Information control can also cost lives. When the PRC leadership chose to suppress news of the SARS outbreak in 2002, the virus spread far beyond China's borders to places like San Francisco, causing the death of at least several hundred victims and almost a global pandemic.[4]

Suppressing information threatens not only the rights of censored individuals, but also strategic U.S. interests. The U.S. government, therefore, has a vested interested in promoting the free flow of information online.

It is an unpleasant fact that American technology is often used to censor online communication. A simple solution to this problem would be to place the offending pieces of technology under strict export control regulations. Such a move, however, would inevitably hinder American companies. Mark Chandler, the Senior Vice President of Legal Services at Cisco Systems, Inc. defended his company's sales to China on the grounds that technology is value neutral; it is the *use* of technology with which we may agree of disagree. "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… *Whether for security or the management of information, the technology is one and the same*."[5] In other words, the technology that allows a network administrator to protect a network from attacks that would hinder the flow of information is exactly the same technology that allows information to be blocked. Legitimate business transactions may be unduly impaired by strict export control regulations.

Thankfully, there are more creative solutions that would not unduly burden U.S. companies operating in politically repressive nations. First, we must realize that there is a middle ground between offering uncensored services that may be blocked by authorities and censoring services in advance in order to avoid being blocked. Nicole Wong, the Deputy General Counsel for Google Inc., testified that Google launched Google.cn, a local version of its website that offers "a filtered search service that operates in China in conformity with local laws, regulations, and policies on illegal content. In doing so, and to provide transparency to our users in China, we became the first search engine in that country to post a notice on the search results page when certain links have been removed."[6] This gives Chinese users more sources of information from which to choose.

She emphasized that "Our Google.cn website supplements, and does not replace, our unfiltered (but periodically interrupted) Chinese-language interface on Google.com.[6]"

Companies who offer web-based services should be legally required to follow Google's lead. Arvind Ganesan of Human Rights Watch pointed out that "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. The FCPA has been in force for more than 30 years and U.S. 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."[7] The FCPA could be amended to require any company operating in a country known to censor the internet to provide an uncensored (but periodically blocked) website in addition to a website that fully complies with local censorship laws, provided that they inform the user when information is being withheld. As Google argued, "there is value in letting our users… know that the information that they searched for exists but cannot be made available because of limitations imposed by their government."[6] Legally requiring U.S. companies to provide such a disclosure would inform people about censorship and make them more likely to advocate political change.

The U.S. should leverage its role as a leader in international politics to promote the free flow of information. One way to do this is to "institutionalize and continue the work of the Global Internet Freedom Task Force (GIFT) created by the State Department in 2006."[8] This office could compile an authoritative list of countries that censor online communication, similar to the State Department's list of state sponsors of terrorism. This list could then guide American diplomacy. "For example," the Center for Democracy and Technology points out:

> The Foreign Assistance Act could be amended to include Internet freedom as an explicit factor to be considered when allocating development assistance. See 22 U.S.C. § 2151n(c). Additionally, Congress annually appropriates money to help fund the Millennium Challenge Account, managed by the President's Millennium Challenge Corporation, and could ensure that these funds are used to advance Internet freedom in country grantees.[8]

Finally, although 165 states are party to the International Covenant on Civil & Political Rights,[9] only 113 have signed the subsequent First Optional Protocol, which allows individuals who have exhausted all domestic remedies to seek a redress of grievances from the UN Human Rights Committee.[10] Broadening support for this enforcement mechanism would help individuals whose own countries are unwilling to protect their rights.

Finally, the U.S. can directly assist people who seek to avoid their country's content filtering systems. Tor is software that provides a distributed, anonymous network to its users by encrypting their Internet traffic and passing it through virtual tunnels. After initial development by the U.S. Navy, Tor's source code was publicly released and is available for free. According to their website, "Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses. Journalists use Tor to communicate more safely with whistleblowers and dissidents."[11] The growth of Tor users, however, has outpaced the growth of Tor servers, and performance suffers as a result. The U.S. could substantially aid Tor users by placing a Tor server in every U.S. embassy around the world. Purchasing the server, paying someone to configure it, and buying enough

bandwidth would likely cost $10,000 per embassy per year, or less than $2 million annually.[12]

References

1. "Microsoft censors Chinese blogs." *BBC News*. BBC, 14 June 2005. Web. <http://news.bbc.co.uk/2/hi/technology/4088702.stm>.

2. "Implicated companies." *Amnesty International USA*. Web. <http://www.amnestyusa.org/business-and-human-rights/internet-censorship/implicated-companies/page.do?id=1101584>.

3. Rohozinski, Rafal. "Q&A: Worldwide surveillance and filtering." Interview by Mirko Zorz. *Help Net Security*. 6 Oct. 2009. Web. <http://www.net-security.org/article.php?id=1314&p=1>.

4. *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (May 20, 2008). Testimony of Shiyu Zhou, Ph. D. Web. <http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7187 >.

5. *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (May 20, 2008). Testimony of Mark Chandler. Emphasis added. Web. <http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7185>.

6. *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (May 20, 2008). Testimony of Nicole Wong. Web. <http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7183>.

7. *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (May 20, 2008). Testimony of Arvind Ganesan. Web. <http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7184>.

8. *Global Internet Freedom: Corporate Responsibility and the Rule of Law* (May 20, 2008). Testimony of Leslie Harris. Web. <www.cdt.org/testimony/20080520harris.pdf>.

9. "International Covenant on Civil and Political Rights." *United Nations Treaty Collection*. 21 Oct. 2009. Web. <http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en>.

10. "Optional Protocol to the International Covenant on Civil and Political Rights." *United Nations Treaty Collection*. 21 Oct. 2009. Web. < http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-5&chapter=4&lang=en >.

11. "Tor: Overview." *Tor: anonymity online*. Web. <www.torproject.org/about/overview.html.en>.

12. $4,000 per server + $1,000 per technician + $5,000 per bandwidth allocation
    = $10,000 per embassy
    $10,000 per embassy * 200 embassies = $2 million