UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

United Nations Working Group on Human Rights and Transnational
Corporations and Other Business Enterprises
Via email: wg-business@ohchr.org

December 8, 2011

Dear Expert Members of the UN Working Group on Human Rights and Transnational Corporations and Other Business Enterprises,

In response to the invitation of the UN Working Group on Human Rights and Transnational Corporations and Other Business Enterprises (the "Working Group") for input regarding the group's key thematic priorities and activities, the Citizen Lab at the Munk School of Global Affairs, University of Toronto, respectfully submits its views on the urgent need for greater assessment of, and provision of guidance to, the surveillance and Internet filtering technology sector. Companies in this industry have thus far demonstrated a serious lack of regard for the negative human rights impacts of their products and services. In general, company reactions to allegations concerning compromise of human rights suggest an absence of company policies and due diligence measures to identify or prevent such abuses, let alone mitigate or remedy them.[1] The Citizen Lab therefore urges the Working Group to include investigation of and development of guidance surrounding this sector as the Working Group carries out its mandate.

[1] One notable exception to this approach is the reaction of Websense, a U.S.-based provider of Internet filtering technology and other information security tools. Websense stated in response to increasing reports of the use of Western technologies by repressive regimes, "Is it appropriate for American businesses to claim that technology is morally neutral, and therefore absolve themselves of responsibility for its use? No. American software companies should take strong measures to prevent the misuse of their technologies where it would be harmful to the public good. And it's long overdue for American technology companies to step forward and address this problem. . . . We challenge all other American technology vendors to join us in prohibiting repressive regimes from using American technology to prevent open communications." See "Websense statement on improper use of technology for suppression of rights and in violation of trade sanctions," November 1, 2011, http://community.websense.com/blogs/websense-insights/archive/2011/11/01/websense-statement-on-improper-use-of-technology-for-suppression-of-rights-and-in-violation-of-trade-sanctions.aspx. Websense has also joined the Global Network Initiative, a multi-stakeholder initiative to protect and advance freedom of expression and privacy in the ICT sector. See Global Network Initiative, "Websense Joins the Global Network Initiative," December 8, 2011, http://www.globalnetworkinitiative.org/newsandevents/Websense_Joins_the_Global_Network_Initiative.php.

The Citizen Lab, founded in 2001, is an interdisciplinary laboratory based at the Munk School of Global Affairs, the University of Toronto, Canada, focusing on the intersection of digital media, global security, and human rights. Its mission is to undertake advanced research and engage in development that monitors, analyses, and impacts the exercise of political power in cyberspace. Recent Citizen Lab research reports include *The Canadian Connection: An investigation of Syrian government and Hezbullah web hosting in Canada*,[2] and *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*,[3] both of which analyze the use of Western-supplied technology by repressive regimes in furtherance of activities that compromise human rights. The Citizen Lab is also one of the founding partners of the OpenNet Initiative (ONI) -- a consortium of institutions that includes the Berkman Center for Internet & Society at Harvard University and the SecDev Group -- which aims to empirically document patterns of Internet censorship and surveillance worldwide in a non-partisan manner. ONI research has investigated the use of commercial filtering products since 2002, including reports on the use of Western-supplied technologies in countries such as Iran,[4] Saudi Arabia,[5] and Burma,[6] as well as a recent investigation into the use of these technologies throughout the Middle East and North Africa.[7] As a result of its ongoing research and analysis, particularly its work in support of the *Behind Blue Coat* report, the Citizen Lab is deeply concerned about the growing trend among private companies in the surveillance and filtering technology industry to equip regimes and other entities that violate human rights with the tools to do so.

[2] Citizen Lab and the Canada Centre for Global Security Studies, “The Canadian Connection: An investigation of Syrian government and Hezbullah web hosting in Canada,” 2011, http://citizenlab.org/2011/11/the-canadian-connection/

[3] Citizen Lab, “Behind Blue BlueCoat, Investigations of commercial filtering in Syria and Burma,” 2011, http://citizenlab.org/2011/11/behind-blue-coat/

[4] OpenNet Initiative, “Internet Filtering in Iran in 2004-2005: A Country Study,” 2005, http://opennet.net/studies/iran2005

[5] OpenNet Initiative, “Saudi Arabia,” 2009, http://opennet.net/studies/saudi

[6] OpenNet Initiative, “Burma,” 2009, http://opennet.net/studies/burma

[7] OpenNet Initiative, “West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011,” March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

There are two significant challenges to addressing the human rights risks presented by the surveillance and filtering technology sector. First, this sector lacks transparency, making it difficult to assess the true scale of, scope of, and participants in the market. While a number of companies have emerged as well-known providers of technology products that include filtering components -- such as Blue Coat, Fortinet, and NetSweeper -- others are relatively obscure. Civil society and the media appear to have only scraped the surface regarding details of industry participants providing "off-the-shelf surveillance technology," both at home and abroad.[8] In light of resource limitations and other constraints on access to information about this sector, it is probable that numerous surveillance and filtering technology companies -- including those based in countries beyond the West -- operate largely under the radar of public discourse.

Second, a wide array of surveillance and filtering technology is "dual use." Law enforcement agencies, commercial entities, as well as private institutions and individuals regularly use such technology for legitimate and beneficial security purposes. Accordingly, any attempt to regulate the sector must address the dual use issue, which will require nuanced consideration of who is using the technology, what the technology is used for, and the entity against which the technology is used -- a far broader calculus than simply designating specific technologies as offensive.

In spite of these challenges, it is clear that action to increase accountability and respect for human rights in this sector is essential. Surveillance and filtering technologies designed in the West are increasingly discovered within the "tool-boxes" of repressive regimes cracking down on legitimate expression, particularly political content.[9] Yet it is typical for representatives of companies in this sector to reject any assertion that they should concern themselves with the human rights impact and end uses of their products, which they consider the responsibility of the government. For example, Jerry Lucas, the president of the company that organizes the annual

[8] See, e.g., Bureau of Investigative Journalism & Privacy International, "The State of Surveillance: The Data," December 1, 2011, http://bigbrotherinc.org/; "The Surveillance Catalog," *Wall Street Journal*, http://projects.wsj.com/surveillance-catalog/?mod=djemalertNEWS#/; "Wikileaks: The Spy Files," http://wikileaks.org/the-spyfiles.html.

[9] OpenNet Initiative, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011," March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011; Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," August 30 2011, *Wall Street Journal*, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html; F-Secure, "Egypt, FinFisher Intrusion Tools and Ethics," March 8, 2011, http://www.f-secure.com/weblog/archives/00002114.html.

Intelligence Support Systems (ISS) World Americas conference for surveillance technology, stated, "[it's] just not my job to determine who's a bad country and who's a good country. That's not our business, we're not politicians … we're a for-profit company. Our business is bringing governments together who want to buy this technology."[10] It is unclear whether this cavalier attitude is the result of a lack of awareness or expertise, willful ignorance, or deliberate disregard.

Proper implementation of the Guiding Principles on Business and Human Rights ("Guiding Principles")[11] in this industry could contribute significantly to addressing and preventing the negative human rights impact of industry products and services. In particular, the following steps are essential to curbing the harmful practices of the surveillance and filtering technology sector:

- Surveillance and filtering technology companies must first acknowledge their own role and responsibility in the compromise and protection of international human rights. In this regard, companies must be encouraged to recognize the applicability to their business of Principle 11: "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved." As stated in the commentary to that principle:

  > The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. *And it exists over and above compliance with national laws and regulations protecting human rights.* [Emphasis added.]

[10] Ryan Gallagher, "Governments turn to hacking techniques for surveillance of citizens," *The Guardian*, November 1, 2011, http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance

[11] U.N. Human Rights Council, "Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," U.N. Doc. A/HRC/17/31, March 21, 2011, http://www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/17/31.

The surveillance and Internet filtering technology sector must not continue to operate on the basis of minimum standards, disregarding the human rights implications of their products and services until specifically instructed by government to do otherwise. This technology is designed for the purpose of monitoring and controlling digital information, such that its impact on individual rights of privacy and freedom of expression is inherent and obvious. The legitimacy of restrictions on these rights in the first instance is a logical consideration to include in a company's due diligence and risk management efforts.[12]

Furthermore, addressing human rights impact *proactively* is crucial in this sector. Surveillance and filtering technology is developing in a rapid and non-transparent manner that may outpace the regulatory efforts of state bodies. At the same time, conflict situations in which the products and services of these companies are most likely to be exploited are often unpredictable. A surveillance or filtering technology company must therefore carefully consider how its products and services are used on an ongoing basis, as waiting to respond until prompted by a home government may be too late to prevent irreparable harm.

- Surveillance and filtering technology companies must promptly operationalize human rights commitments. While the Guiding Principles encourage such operationalization by all companies, operationalization is of urgent importance in the surveillance and filtering technology sector, the products and services of which have the potential to significantly compromise the key enabling rights of freedom of expression and privacy. Current practice in that sector appears to fall far short of the standards articulated in the Guiding Principles, including Principle 15, which recommends that companies incorporate a human rights policy commitment, ongoing human rights due diligence, and remediation processes.

  In particular, company efforts to "identify, prevent, mitigate and account for" human rights impacts can prevent serious human rights compromises stemming from surveillance and censorship technologies. For example, after the hacktivist collective Telecomix and other civil society actors, including the Citizen Lab, documented the

[12] Indeed, to allow for better customization of a technology solution, clients may occasionally even make a company aware of purposes the technology will serve that clearly compromise human rights. See Don Clark, "Falun Gong Practitioners Sue Cisco," *Wall Street Journal*, May 23, 2011, http://online.wsj.com/article/SB10001424052748704083904576335980445655322.html

discovery of Blue Coat Internet filtering devices at work in Syria and Burma, Blue Coat admitted that it had the capacity all along to monitor its servers for contact originating from devices in Syria -- a country subject to U.S. sanctions.[13] Clearly, Blue Coat was in a better position than unrelated third-party entities to track such activity and address this serious issue. Use of Blue Coat's filtering technology by the Syrian government to compromise the human rights of Syrian citizens may have even been avoided if Blue Coat had taken steps on its own to ensure its devices were not active in the country.

- Surveillance and filtering technology companies must engage with their networks of resellers and distributors to ensure human rights compliance -- and these networks must themselves become more accountable. Sales of surveillance and filtering technology are often facilitated through networks of third-party distributors and resellers, which may also provide services to end users related to the technology provided. Given this sales model, as well as the existence of "grey markets," a company that manufactures the technology may not be involved in the final sale of that technology to the end user. Some companies have argued that, given their lack of direct contact with end users, they are not responsible for sales to end users that may employ their products to violate human rights. For example, Blue Coat asserted that its devices in Syria were shipped through a distributor from Dubai and destined for the Iraqi Ministry of Communications, and that it had no knowledge of how the devices ended up in Syria.[14]

  However, the multi-layered sales structure prevalent in this sector does not reduce the need for technology manufacturers to proactively address the human rights risks posed; rather, it increases the need for due diligence measures. As enumerated in Principle 13, companies should "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts." Surveillance and filtering technology companies should explore ways to ensure that resellers or distributors with whom they engage are accountable concerning the end users to whom they sell -- either through a

[13] Valentino-Devries, J., Sonne, P. and N. Malas, ‘U.S. firm acknowledges Syria uses its gear to block web," Washington Post, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

[14] Ibid.

strict selection process for inclusion in a distribution network, or through explicit contractual provisions.

- States should develop a clearer approach to human rights-related requirements in the surveillance and Internet filtering technology sector, including detailed guidance for companies regarding compliance with sanctions regimes. States' fulfillment of the duty to protect, in accordance with Principle 1, as well as with Principle 7 regarding conflict-affected areas, is essential with respect to this sector. Ironically, some states have recently found themselves in an awkward situation, whereby their foreign policy statements on "Internet freedom" are contradicted in practice by companies operating from within their own jurisdictions.[15] While it is a matter of debate whether increased government regulation and sanctions offer a real solution to managing the human rights risks of this sector -- particularly given the dual use challenge -- governments under the jurisdiction of which these companies fall should carefully assess company policies and practices, and the applicable regulatory frameworks, to determine whether there is need for greater or more precise government intervention to prevent human rights violations.

  The surveillance and filtering technology sector could benefit in particular from government guidance, tailored to this sector, on sanctions compliance. Companies are most likely to restrict their sales or services within a particular country when sanctions are applied, given that sanctions typically involve heavy penalties for non-compliance. However, the scope of sanctions regimes -- which may focus on particular types of goods or services, or include important exceptions to overarching restrictions -- often lacks clarity, which may result in misinterpretation within the industry. In light of the increasing importance of technology to civil society movements in countries under the rule of repressive regimes, and the active use of technology by the regimes themselves to control such movements, governments should issue careful guidance to and engage in dialogue with technology companies concerning what sanctions compliance requires of them, in order to prevent over- or under-reaction.

[15] See, e.g., Helmi Noman, "When a Canadian company decides what citizens in the Middle East can access online," OpenNet Initiative, May 16 2011, http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online; Ronald Deibert, "Canada lauds UAE ISP that pervasively censors political, religious, and gay and lesbian information, using Canadian software," OpenNet Initiative, July 1, 2011, http://opennet.net/blog/2011/07/canadian-government-lauds-uae-internet-service-provider-pervasively-censors-political-r.

States should also consider, as set forth in Principle 25, enhancement of judicial and other remedies available against surveillance and filtering technology companies the products of which are used to violate human rights. For example, states may encourage greater company respect for human rights by developing frameworks for remedy that incorporate safe harbor provisions for those companies taking adequate precautionary steps and actively monitoring their distribution and resale networks.

The urgent attention of the Working Group to the surveillance and filtering technology sector would be a welcome first step toward integration of the Guiding Principles by companies in this sector.

The Citizen Lab respectfully urges the Working Group to consider the following options in addressing the challenges posed by this sector and carrying forward its mandate:

- Investigate the policies and practices of surveillance and filtering technology companies, including through direct inquiries to these companies, with a particular emphasis on companies the products of which are used in conflict-affected areas.

- In consultation with the industry and civil society, encourage development of a human rights compliance assessment tool designed for this sector, incorporating sector-specific indicators, as well as other tools that may improve these companies' ability to proactively address human rights concerns.

- Include a focus on the surveillance and filtering technology sector at the UN Forum on Business and Human Rights, in order to enhance transparency of the sector, raise awareness among technology developers of their human rights responsibilities, and disseminate the Guiding Principles within the industry. The Forum may also be an appropriate venue in which to explore a mechanism for sharing best practices and human rights challenges within the industry.

- In consultation with the industry and civil society, develop advice and recommendations for states regarding proper regulation of the surveillance and filtering technology sector, including with respect to the dual use challenge.

- Collaborate with other UN mechanisms concerning human rights compliance within the surveillance and filtering technology sector, and evaluation of grievances related to the products and services of such companies. UN mechanisms with which to coordinate could include the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and the Special Rapporteur on the promotion and protection of human rights while countering terrorism.

The Citizen Lab welcomes the opportunity to assist the Working Group in its efforts. Please feel free to contact us with any questions or for additional information.

Sincerely,

Professor Ronald J. Deibert
Director, The Canada Centre for Global Security Studies and The Citizen Lab
Munk School of Global Affairs
University of Toronto
1 Devonshire Place
Toronto, Ontario
Canada M5S 3K7

Appendix: Additional Resources

Citizen Lab. (2011). *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*. http://citizenlab.org/2011/11/behind-blue-coat/

Citizen Lab. (2011). *The Canadian Connection: An investigation of Syrian government and Hezbullah web hosting in Canada*. http://citizenlab.org/2011/11/the-canadian-connection/

OpenNet Initiative. (2011). *West censoring East: The use of Western technologies by Middle East censors (2010-2011)*. http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf

OpenNet Initiative. (2011). "When a Canadian company decides what citizens in the Middle East can access online," May 16, 2011, http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-accessonline

OpenNet Initiative. (2009). *Burma*. http://opennet.net/studies/burma

OpenNet Initiative. (2009). *Saudi Arabia*. http://opennet.net/studies/saudi