Ministry of Foreign Affairs of the
Netherlands

Global Corporate Responsibility for Internet Freedom

Background paper

Introduction

The Internet, as a global network of networks, is not under the control of a single government or international entity. Instead, it is governed by a multitude of public and private sector organisations. The private sector has a central role in the Internet's development, as most of the infrastructure and services that make up the Internet are in the hands of the private sector.

The Internet's relative anonymity and borderless nature serve to ensure its open and free character. However, this does not mean that the Internet is immune to control. Since the Internet – and the cyberspace created by it – is a human construct, it can be monitored, manipulated and controlled[1]. As such, the Internet may also strengthen two key powers of authoritarian regimes: surveillance and censorship[2].

If authoritarian regimes wish to control the free flow of information they need the cooperation of those entities that control the infrastructure and services within their jurisdiction. In many, if not most, cases these entities are private enterprises. This means that companies may be forced by national governments to take measures that restrict the free flow of information and endanger freedom of expression.

Furthermore, regimes that wish to limit the free flow of information among their citizens may wish to shape the architecture of cyberspace in such a way that they can monitor, filter, block or otherwise control the information that flows over the Internet. To this end they may employ technologies and services developed by the private sector (e.g., monitoring, filtering and blocking technologies). Internet security and surveillance technologies are therefore something of a double-edged sword. On the one hand they may be employed by free societies to protect the public's rights and interests and ensure cyber security, but they may also be used by authoritarian regimes to exercise control over their citizens.

How companies (and particularly multinationals) should deal with these two issues is an important question of corporate social responsibility (CSR). In this background paper we describe the global CSR initiatives that exist and explore in more depth the debates set out in this introduction.

[1] In fact, 'cyberspace' is a portmanteau of cybernetics (the science of control) and space.
[2] Morozov, E. (2011), The Net Delusion: the Dark Side of Internet Freedom, New York: Public Affairs.

Global corporate social responsibility

As a result of globalisation CSR has become an international issue. In an effort to come to an international consensus on corporate responsibility, social responsibility standards have been defined within the context of international (governmental) organisations. Companies, be they SMEs or multinationals, can adopt these standards and commit themselves to social responsibility in areas such as labour conditions, sustainability and human rights.

Ruggie framework

In 2008, John Ruggie, Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, presented his framework for business and human rights[3]. The 'Ruggie Framework' sets forth three core principles: the State duty to protect against human rights abuses by third parties, including business; the corporate responsibility to respect human rights; and the need for more effective access to remedies. In March 2011, the Special Representative issued specific 'Guiding Principles' for the implementation of the framework[4]. The Guiding Principles were endorsed by the UN Human Rights Council in June 2011[5]. While the Ruggie Framework is not specifically tailored to the Internet, it provides an important general framework on the relation between human rights and business.

United Nations Global Compact

The UN Global Compact is a strategic policy initiative for businesses committed to CSR.[6] The Compact is a forum for discussion and has no enforcement mechanisms. It has formulated 10 principles, the first two of which are concerned with human rights. These state that businesses should support and respect the protection of internationally proclaimed human rights and make sure that they are not complicit in human rights abuses. During the second Global Compact summit in July 2007 the Geneva Declaration was adopted, underlining the importance of global corporate social responsibility.[7]

[3] Ruggie, J. (2008), Protect, *Respect and Remedy: a Framework for Business and Human Rights*, Human Rights Council, Eighth Session, Agenda Item 3, April 2008, A/HRC/8/5 7.

[4] Ruggie, J. (2011), *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Human Rights Council*, 17th Session, Agenda Item 3, 21 March 2011, A/HRC/RES/17/4.

[5] Human Rights Council , 17th session, Agenda item 3, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development; Resolution adopted by the Human Rights Council, *Human rights and transnational corporations and other business enterprises*, 6 July 2011.

[6] www.unglobalcompact.org.

[7] United Nations Global Compact Leaders' Summit, 5-6 July 2007 Geneva, Switzerland, Geneva Declaration.

OECD Guidelines for multinational enterprises

Within the OECD, Guidelines for Multinational Enterprises on corporate responsibility have been established.[8] These are recommendations addressed by governments to multinational enterprises operating in or from adhering countries. They provide voluntary principles and standards for responsible business conduct in a variety of areas, including employment and industrial relations, human rights, the environment, information disclosure, competition, taxation, and science and technology.

ISO 26000

In November 2010, the International Organization for Standardization launched ISO 26000, the standard for social responsibility.[9] The standard is a tool for organisations that want to operate in a socially responsible manner. It defines seven core themes, one of which is respect for human rights. It is important to note that while most ISO standards contain specific requirements and are considered management standards, ISO 26000 is aimed at providing guidance on social responsibility. As such, organisations cannot be certified against the standard as they can with management standards like ISO 9000.

[8] OECD (2011), *OECD Guidelines for Multinational Enterprises*, OECD Publishing.
[9] www.iso.org/iso/social_responsibility.

Internet-specific CSR initiatives

While the initiatives described above set out standards and guidelines for social responsibility in general, they do not emphasise the issue of internet freedom, or the relationship between the Internet and human rights. Companies that are involved in discussions on internet freedom (either because they operate in countries that limit internet freedom or because they provide goods and/or services that may be abused by authoritarian regimes) can only derive general guidance from these frameworks. Therefore, internet-specific CSR initiatives, in which the private sector participates, have emerged in recent years.

Global Network Initiative

The Global Network Initiative (GNI) is a multi-stakeholder coalition of ICT companies, human rights organisations and academia. The goals of the GNI are to prevent internet censorship and protect online privacy[10]. Private sector participants include Google, Microsoft, Yahoo!, Evoca (a small American mobile recording company) and Folksam (a Swedish insurance company).

The GNI has defined a set of principles that define the commitment of its members to online freedom of expression and privacy. These principles provide high-level guidance to the IT industry on how to respect, protect and advance freedom of expression and privacy. In particular, it includes guidance on how to deal with government demands for censorship and disclosure of users' personal information.[11] A specific implementation guideline provides more detailed information on implementing the principles within a company and on multi-stakeholder decision-making.[12] Finally, the governance, accountability and learning framework sets out a multi-stakeholder governance structure, a system of accountability and a framework for education on the initiative and its principles.[13]

Internet Rights & Principles coalition

Within the framework of the Internet Governance Forum, an International Rights & Principles Coalition has been formed. The mission of this dynamic coalition is: *"to make rights on the Internet and their related duties, specified from the point of view of individual users, a central theme of the internet governance debate held in the IGF context"*.[14] The Internet Rights & Principles Coalition has compiled a list of ten key internet rights and principles, rooted in international human rights standards, that derive from the Coalition's emerging Charter of Human Rights and Principles for the Internet.[15] The Internet Rights & Principles Coalition is made up of both private sector companies and governments.

[10] www.globalnetworkinitiative.org.
[11] www.globalnetworkinitiative.org/principles/index.php.
[12] www.globalnetworkinitiative.org/implementationguidelines/index.php.
[13] www.globalnetworkinitiative.org/governanceframework/index.php.
[14] www.internetrightsandprinciples.org/.
[15] www.internetrightsandprinciples.org/.

Civil society initiatives

Civil society regularly calls upon the private sector to take responsibility on issues related to internet freedom. NGOs generally take two approaches to promoting CSR: engaging with the private sector or confronting the private sector.[16]

An example of an initiative aimed at engaging with the private sector and strengthening CSR is the Silicon Valley Standard. The Standard was created as part of the 2011 Silicon Valley Human Rights Conference.[17] It is a principled statement incorporating the issues discussed during the conference.

The Silicon Valley Standard is an initiative by Access, an NGO with a dedicated agenda on promoting internet freedom. The Standard covers topics such as jurisdiction, social media, 'human rights by design' and intermediary liability. While not a CSR document in itself, it is aimed at supporting existing frameworks for human rights, internet freedom and corporate social responsibility. Access hopes that the IT sector will embrace and apply the Silicon Valley Standard following the conference.[18]

[16] Winston, M. (2002), NGO Strategies for Promoting Corporate Social Responsibility, in: *Ethics & International Affairs*, Volume 16.1 (Spring 2002).

[17] www.rightscon.org/silicon-valley-standard/.

[18] www.rightscon.org/silicon-valley-standard/.

Government pressure to limit internet freedom

Each legally distinct corporate entity is subject to the laws of the countries in which it is based and operates.[19] As such, governments can set rules and regulations that govern the behaviour of companies that fall within their jurisdiction. Policies for governing the Internet may be at odds with freedom of expression, privacy, or other human rights.

In order to enforce their (internet) policies effectively, governments need the cooperation of private sector entities that provide infrastructure and services (e.g. telecoms companies, ISPs, social networking sites, search engines and user generated content sites). To limit the free flow of information, governments can ask companies to limit internet access, block and filter content or search results and relinquish subscribers' contact details. Countries that try to force private sector entities to regulate the free flow of information include China,[20] Iran[21] and Egypt.[22]

For those companies involved, the question is how to deal with requests from governments to impede the free flow of information and/or hand over user details. Should they comply or resist? Resisting is most likely a violation of local laws, and may put both the business and its local employees at risk, while complying may result in companies being complicit in human rights violations. When it comes to limiting the free flow of information at the behest of a government, there is also the question of which is the lesser of two evils: complying with a certain level of censorship but keeping access to the service open for citizens, or shutting the service down completely, thereby denying people access to information altogether?

The following example illustrates the difficulty facing a multinational company in dealing with local requests for censorship. In June 2010 Google stopped complying with China's request to filter search results and began redirecting users from the Chinese version of Google (www.google.cn) to the Hong Kong version of Google (google.com.hk).[23] In response, China threatened not to renew Google's internet content provider licence, which would effectively mean Google's being shut down in China.[24] Google and China ultimately reached an agreement: users were no longer automatically redirected, but a link on the Google search page to google.com.hk was placed there for users who want unfiltered access

[19] Ruggie, J. (2008), *Protect, Respect and Remedy: a Framework for Business and Human Rights, Human Rights Council, Eighth Session*, Agenda Item 3, April 2008, A/HRC/8/5 7.
[20] BBC News (2010), China condemns decision by Google to lift censorship, March 23 2010 (online version).
[21] Open Net Initiative (2009), *Iran country report*.
[22] Schonfeld, E. (2009), *Twitter is blocked in Egypt amidst rising protests*, TechCrunch, 25 January 2011.
[23] BBC News (2010), *China condemns decision by Google to lift censorship*, 23 March 2010 (online version)
[24] The Official Google Blog, *An update on China*, 28 June 2010 (updated 7 July 2010)

to Google.

There is no easy answer to this question in respect to corporate social responsibility. The general CSR frameworks (such as the Ruggie Framework), and the specific internet-oriented frameworks (such as the Global Network Initiative) provide guidance for companies dealing with requests from governments that may be at odds with the rights of citizens. But it is important to note that the standards and levels of commitment required of the private sector vary from one CSR framework to another. Therefore, the private sector companies involved have to make individual policy decisions on the extent to which they are willing to comply with the requests from authoritarian regimes, what their general attitude towards authoritarian regimes is, and the extent to which they wish to make their services 'dissident friendly'.[25]

[25] For instance by using stronger (optional) security measures or allowing dissidents to use pseudonyms rather than their real names.

Export of information and communication technologies

While many still consider the Internet an environment that is more or less immune to regulation, surveillance and enforcement can actually be very effective in the online world. The reason for this is that internet use can be controlled through technologies and applications that monitor, filter and block information flows. The technologies and applications are largely developed by the private sector. Examples include professional firewalls, filters, wiretapping software and digital forensics and analysis tools. These are used to combat cybercrime and to strengthen cybersecurity and thus serve legitimate purposes. However, they may also be acquired by authoritarian regimes and used for the purpose of surveillance and censorship. To undermine the surveillance and censorship capabilities of authoritarian regimes, their access to these technologies must be limited.

The debate on the use of applications and technologies for controlling information flows on the Internet is closely related to the debate on 'dual-use items'. Dual-use items are items that have both civilian and military applications. As a consequence, use of these technologies may raise concerns in areas such as national security, nuclear non-proliferation, regional stability, crime control and terrorism. The export of these technologies is therefore regulated and in some cases prohibited. Items that can be used for human rights violations may also be classified as dual-use items. Article 8, paragraph 1 of the European Dual-Use Regulation, for example, allows member states to impose authorisation requirements on the exports of goods for reasons of human rights considerations.[26]

The current political discussion concerns the extent to which internet monitoring, filtering and blocking technologies should fall under the scope of dual-use item regulations. Including these technologies and applications will make it clearer to the private sector under what conditions they may be exported and to whom.

Within the EU, the application of the dual-use item regime to internet technology is gaining increasing support. The European Parliament, the European Council and the European Commission are currently working on ways to translate this concept into concrete measures. On 30 June 2011, the European Commission adopted a Green Paper on the dual-use export control system.[27] A public consultation on this paper was held, inviting other stakeholders to share their views. The Commission's principle aim is to achieve common understanding on the general notion that ICT technologies that can be used to infringe human rights online are in fact dual-use items that fall within the scope the EU regime of export controls. In September, the EU Parliament voted on an amendment to the Dual-Use Regulation that prohibits the granting of general EU authorisations for export of telecom-

[26] Council Regulation (EC) No 428/2009 of 5 May 2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

[27] European Commission (2011), *The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world*, green paper, Brussels, 30 June 2011 COM(2011) 393 final.

munication technologies that can be used "*in connection with a violation of human rights, democratic principles or freedom of speech (…) by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use*". [28]

In the United States, a similar system of specific limitations to exports of dual-use items is in place. The Bureau of Industry and Security of the U.S. Department of Commerce is responsible for regulating the export of most commercial items.[29] Companies that wish to export goods need to verify whether an export licence is required for the type of product they wish to export. They also need to 'know the customer' and verify that the customer is not on a list of prohibited persons or entities.[30]

Apart from government-regulated export of dual-use items, companies also have their own corporate social responsibility to ensure that their products are not used for human rights violations. So apart from legal compliance, companies may themselves take additional positive steps to act in a social responsible manner. In this area, the civil rights organisation Electronic Frontier Foundation (EFF) has proposed the adoption of a robust 'know your customer' programme for companies wishing to export ICT technologies that could be used for surveillance, filtering and blocking. The EFF states that the most effective solution would be the voluntary implementation of such a programme by companies.[31]

[28] www.europarl.europa.eu/nl/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports.

[29] www.bis.doc.gov/licensing/.

[30] export.gov/regulation/eg_main_018229.asp.

[31] Cohn, C., York, J. C. (2011), *"Know Your Customer" Standards for Sales of Surveillance Equipment*, Electronic Frontier Foundation, 24 October 2011.

Conclusions

The private sector has a central role in protecting and furthering internet freedom, as most of the infrastructure and services that make up the global Internet are owned and controlled by the private sector. How companies deal with the issue of internet freedom is an issue of corporate social responsibility.

The precise scope of companies' responsibility in relation to internet freedom and human rights online is difficult to define. In his report, the UN Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises notes that while corporations may be considered 'organs of society', they are specialised economic organs, not democratic public interest institutions. As such, their responsibilities cannot and should not simply mirror the duties of states.[32]

Nevertheless, the baseline responsibility of companies is to respect human rights. Whereas governments define the scope of legal compliance, the broader scope of the responsibility to respect human rights is also defined by social expectations. This may entail the need for positive steps, rather than just a passive responsibility not to do harm. Guidance on how to meet these expectations is provided by the general corporate social responsibility frameworks, as well as the internet-specific CSR frameworks that are gradually emerging.

[32] Ruggie, J. (2008), Protect, *Respect and Remedy: a Framework for Business and Human Rights*, Human Rights Council, Eighth Session, Agenda Item 3, April 2008, A/HRC/8/5 7, p. 16.

Ministry of Foreign Affairs of the
Kingdom of the Netherlands
P.O. Box 20061 | 2500 EB The Hague