REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

47, rue Vivienne
75002 Paris
0144 83 84 84
www.rsf.org

SECOND UNITED FORUM ON BUSINESS AND HUMAN RIGHTS GENEVA ON 2-4 DECEMBER 2013

WRITTEN SUBMISSION BY REPORTERS WITHOUT BORDERS

Reporters Without Borders (RWB) is an international organization which for 28 years has been defending press freedom and media workers. Based in Paris, it relies on a network of more than 150 correspondents in 130 countries, on 10 country chapters and on local and regional partner organizations. For nearly 10 years, RWB has been involved in policy debates concerning the role of information-technology and digital media companies.

Since 2003, the organization has been sending questionnaires to Internet company executives concerning their censorship and surveillance practices in countries that restrict freedom of information. In 2006, the organization revealed the involvement of Yahoo! Hong Kong in the court conviction of Chinese journalist Shi Tao, sentenced to 10 years in prison for having sent information by e-mail concerning censorship of information about the Tienanmen Square massacre. The disclosure prompted widespread media coverage as well as U.S. congressional hearings. These eventually led Yahoo! to acknowledge its responsibility and to apologize to Shi Tao's mother. The U.S. Congress, as well as the European Parliament, then summoned major Web companies to testify concerning their practices in repressive countries.

Subsequently, several of these firms agreed to a code of conduct developed by the Global Network Initiative (GNI). Reporters Without Borders participated in negotiations leading to formulation of the code, along with companies, NGOs, investment funds and academic experts. RWB did not sign the code, but greeted the initiative as a step in the right direction, given that the firms in question acknowledged for the first time their responsibility to protect freedom of expression in the countries where they operate.

In 2011, Reporters Without Borders requested sanctions against companies that sell surveillance and communication interception technology to repressive governments. The export of dual-use technology underlines the importance of corporate social responsibility to Internet freedom. In keeping with this understanding, RWB has demanded export controls on surveillance technology to countries that flout human rights.

More recently, RWB has joined Privacy International, the European Center for Constitutional and Human Rights, the Bahrain Center for Human Rights and Bahrain Watch in filing a formal complaint with the Organization for Economic Co-operation and Development against a company that produces digital surveillance software.

INTERNET SURVEILLANCE TECHNOLOGY MUST BE INCLUDED ON THE FORUM AGENDA

Censorship and surveillance on the Internet affect the exercise of basic rights. Freedom of expression on the Internet facilitates free debate on subjects of general interest, such as social and economic development, good governing practices and the enforcement of democratic freedoms. In the words of

Franck La Rue, special rapporteur to the UN Human Rights Council on the promotion and protection of the right to freedom of opinion and expression: "by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights."[1]

Internet surveillance enables identification of Web users and their contacts, and their locations, as well as the reading of their communications. In repressive countries, this surveillance results in the arrest and mistreatment of human rights defenders, journalists, netizens and other civil society members.

In a special edition on surveillance, the annual Enemies of the Internet report by RWB names five "digital era mercenaries." These companies' products have been or are being used by repressive governments to violate human rights and freedom of information. For example, surveillance and interception products by the Trovicor firm allowed the royal family of Bahrain to spy on and arrest media workers. In Syria, DPI (Deep Packet Inspection) products developed by Blue Coat enabled the regime to spy on dissidents and netizens throughout the country, leading to arrests and torture. Eagle products sold by the Amesys firm were found in secret police installations of the Muammar Gadaffi regime.

In recommendations included in a report of 16 May 2011 concerning freedom of expression online, Special Rapporteur La Rue addresses himself not only to governments but also to companies, with an emphasis on the responsibility that they bear.[2] Given the importance of the private sector in providing Internet services, he insists on the importance of preventing its involvement in governmental human rights violations.[3]

The Forum on Business and Human Rights should provide an opportunity to urge that the Guiding Principles for Implementing the UN 'Protect, Respect and Remedy' Framework, endorsed by the UN Human Rights Council on 16 June 2011, be put into practice in this vital sector.

To be sure, though the Guiding Principles are an important tool, they will not end censorship and surveillance of human rights defenders. Preventing private companies from facilitating state repression by developing ever more sophisticated devices and software is an essential task. Debate conducted in the framework of the Forum will prompt greater awareness of surveillance technology as a policy issue.

---

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/17/27 - 16 May 2011 - § 22

[2] "*While States are the duty-bearers for human rights, private actors and business enterprises also have a responsibility to respect human rights.*" *Ibid*, § 45

[3] "*Given that Internet services are run and maintained by private companies, the private sector has gained unprecedented influence over individuals' right to freedom of expression and access to information. Generally, companies have played an extremely positive role in facilitating the exercise of the right to freedom of opinion and expression. At the same time, given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression.*". *ibid, f* § 44

RECOMMENDATIONS

Reporters Without Borders proposes several recommendations directed to the sectors involved. The organization hopes that discussions in the Forum and the activities of the working group will lead to examinations of the roles and obligations of each of them.

1) TO THE STATES: REGULATIONS TO PROTECT HUMAN RIGHTS ARE URGENTLY NEEDED.

Many countries, aware of the growing importance of cyber-security, have developed and exported surveillance technology. This technology is susceptible to dual use. That is, while legitimate in the context of anti-cybercrime measures, the technology can become a formidable censorship weapon in the hands of authoritarian regimes. Failure to control commerce of these "digital weapons" allows authoritarian governments to identify media workers and netizens, to arrest and even to torture them, as has been the case in Bahrain and Syria

In keeping with Guiding Principle 3, states must create legislative and regulatory frameworks to control these companies' activities.

States must commit themselves to regulating trade in surveillance products and to control the activities of the companies in question, including foreign activities. Guiding Principle 2 states: "States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations."

The European Union and the United States have prohibited the export of surveillance technology to Iran and Syria. While this action is commendable, it is insufficient to control companies' activities. European governments must adopt a harmonized approach to controlling these exports. Likewise, the Obama administration should adopt a policy along the lines of the Global Online Freedom Act. The European Parliament on 11 December 2012 endorsed a "Digital Freedom Strategy" as part of European Union foreign policy. The strategy, proposed by Marietje Schaake, must be put into action by the EU and its member states.

States must commit themselves to ensuring that these repressive technologies be included in the Waassenaar Arrangement of July 1996. The accord is designed to promote "transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations." The Arrangement now has 41 participating states, including France, Germany, the United Kingdom and the United States.

In all international bodies and forums whose mandate includes telecommunications and the Internet, the states must maintain their commitment to uphold human rights and freedom of expression.

Legal and non-judicial mechanisms must be put in place (see Principles 25 and 26) in order to enable action against companies involved in these activities.

2) TO INFORMATION TECHNOLOGY COMPANIES: ADOPT AND APPLY THE GUIDING PRINCIPLES TO THEIR RESEARCH AND COMMERCIAL ACTIVITIES.

Principle 13 effectively requires that the companies make a fundamental shift in the way they operate. Ethical codes and export tracing mechanisms must be put in place.

The companies should commit themselves to the obligations that follow from Principle 16 (adopt a human rights Policy); 17 (carry out human rights due diligence); 21 (provide transparency and accountability); 22 (provide remediation for adverse impacts); 29 (establish grievance mechanisms).

Companies should take up the issue of technology's effects on human rights at every stage of work,

starting with research and development, as part of putting the Principles into effect.

3) TO THE FORUM AND THE WORKING GROUP: TAKE A SECTOR-SPECIFIC APPROACH AND INITIATE ENQUIRIES

In the framework of the second Forum, the issue of companies' responsibility for protecting Internet freedom must be addressed so that the Guiding Principles may be implemented in the information technology sector.

The Working Group must take up this issue in its missions to various countries. For example, during the mission to the United States scheduled for 22 April-1 May 2013, it would be important to hear directly from executives of American companies named by NGOs as having transferred surveillance technology. A declaration in favor of passage of the Global Online Freedom Act is also recommended.

Victims of online surveillance should have access to the Working Group during its missions.

Collaboration with Special Rapporteur Franck La Rue should be considered, to enable joint work on the issue of information technology companies' responsibilities.

In the framework of the Forum, interveners including RWB experts, European parliamentarians such as Marietje Schaake, or American members of Congress such as Chris Smith, could provide recommendations to the Working Group.

CONTACTS :

- Hélène Sachstein, RWB's representative : sackstein@rsf-ch.ch, tel : +41 79 696 61 33
- Lucie Morillon, Head of Research Department : internet@rsf.org, tel: +33 1 44 83 84 71

Paris, 10 April 2013