The Internet and Human Rights: Building a free, open and secure Internet

Messages from Berlin

Chairpersons' Summary

of the 2nd Berlin Cyber Conference

September 13 and 14, 2012

The high level international conference "*The Internet and Human Rights: Building a free, open and secure Internet*" gathered approximately 120 experts from international/regional organizations, governments, the private sector, civil society and the technical and academic community on September 13 and 14, 2012 in Berlin. They discussed opportunities and challenges to keep the Internet free, open and secure. The conference was jointly organized and chaired by Aarhus University, Human Rights Watch, the Alexander von Humboldt Institute for Internet and Society and the German Federal Foreign Office.

The outcome of the conference is summarized below in the "Messages from Berlin". They reflect key ideas, expressed by speakers and participants in the two plenaries and six workshops of the conference. The conference chairs and the rapporteurs collected the participants input at the conference. All participants have been invited to contribute to the "Messages from Berlin" online. They can be perceived as policy recommendations on how to enhance international cooperation among all stakeholders and how to strengthen Human Rights in cyberspace. However, not all messages necessarily reflect the view of all participants or all four organizing bodies.

General messages:

1. All Human Rights which apply offline must also be guaranteed online.

2. If literacy in the 21st century means the ability to use a computer and to have access to digital information, providing access to the internet is crucial and the denial of access to the internet constitutes an infringement on Human Rights.

3. Freedom and security in cyberspace are not incompatible but complementary concepts. There can be no freedom without security and no security without freedom.

4. All stakeholders need to contribute on a conceptualization and approach to internet governance that also protects human rights, and promotes free and responsible use of the internet.

5. When protecting intellectual property rights, assurances have to be in place not to violate human and civil rights such as privacy and freedom of expression.

6. Freedom of expression and privacy in the internet are threatened both by governments which introduce state controlled surveillance and censorship and by companies which do not fulfill their responsibilities.

7. The export of sensitive Information and Communication Technologies requires governmental control as well as a voluntary code of conduct for enterprises and an attentive civil society.

8. The exercise of Human Rights in cyberspace requires an enhanced empowerment of individual users and the development of political-legal frameworks.

Messages to governments:

9. Governments should act in a transparent, open and inclusive way, taking account of public feedback and fully respecting existing international Human Rights standards.

10. Governments should apply international Human Rights standards in both their domestic and foreign policy

11. Governments should make it mandatory that ICT companies respect human rights through laws or regulations.

12. When developing national policies for the internet, governments should make better use of the expertise of NGO's and Human Rights activists and contribute more to awareness raising and the education of the public. Governments should work closely together in order to improve the efficiency of existing international Human Rights mechanisms.

13. Governments should promote the introduction of enhanced mechanisms for individual complaints in order to identify cases of Human Rights violations in cyberspace and Human Rights assessment procedures in order to ensure compliance of national law and international treaties with international Human Rights standards.

14. In the field of intellectual property rights governments should continue to protect the legitimate interests of right holders, promote access to knowledge and facilitate the introduction of new business models, taking into account the possibility of limiting the duration of related rights.

15. A crucial task for governments will be to implement and execute export controls vis-à-vis authoritarian regimes on hardware and software that can be used for surveillance, censorship and control.

Messages to the private sector:

16. Private sector organizations should commit to a clear set of principles to ensure that respect for Human Rights becomes a compliance issue and ranks high on their internal agenda.

17. Private enterprises should not become an executive agent of national governments for surveillance, cut-offs or other violations of Human Rights.

18. ICT enterprises should not trade with Human Rights violators.

19. Right holders of intellectual property should periodically review their need to maintain their rights and the possibilities to release material to the public domain for the sake of global common goods, e.g. education.

Messages to civil society:

20. Civil society should organize in more sustainable structures, act in a responsible way and represent legitimate interests of defined constituencies.

21. Civil Society should be more proactive in contributing to the development of internet related public policies by participating in multi stakeholder processes, respecting the specific roles and responsibilities of the other stakeholders.

22. Civil society should contribute to a better education of end-users on how to enjoy Human Rights in cyberspace while using the internet safely.

23. Civil Society should maintain its valuable function as a public watchdog by monitoring processes, publishing reports, organizing campaigns and supporting whistleblowers revealing Human Rights violations in cyberspace.

24. Civil Society should raise public awareness for human rights regarding the implications of intellectual property rights' enforcement by technology.

Messages to the technical community:

25. The technical community should strengthen its awareness of the political, economic and social implications of technologies, such as protocols and standards.

26. The technical community should enhance its dialogue with all other stakeholders, in particular with governments, and make its expertise available to better educate users and decision makers.

27. The technical community should develop solutions that by default protects against third-party surveillance and enhance privacy.

28. The technical community should introduce Human Rights assessment procedures for proposed architectures and technologies and respect Human Rights implications in technical codes, protocols and standards ("Human Rights by design").