Security and Privacy in Cyberspace

Rikke Frank Joergensen
Co-Chair, WSIS Civil Society Human Rights Caucus

> *Never have we seen such political pressure to expand surveillance. Never has the public been so fearful. Democratic Institutions all over the world are being tested now. Will they pass the test? If not, we will wake up to a different kind of society*[1]

Despite the fact the privacy is a core human right and crucial to the economic, social and technological developments, which we call the "Information Society", it has proven very difficult to get it acknowledged and protected within the WSIS process. This contribution will provide a brief analysis on privacy as a human right, why privacy protection is crucial in the Information Society, privacy and WSIS, and the challenges ahead.

Privacy as a human right

Privacy is a core human right; enshrined in the Universal Declaration of Human Rights in Article 12[2], and in Article 17 of the International Covenant of Political and Civil Rights, which is legally binding upon United Nations Member States. Its importance as a basis for the development of a democratic society is stressed time and again by the United Nations Human Rights Committee and by the United Nations High Commissioner for Human Rights. It has also been emphasized by regional instruments such as the European Court of Human Rights. Privacy protects the essence of human rights: human dignity. Knowing everything about someone reduces that person to a set of known facts, traceable and controllable. As long as a zone of autonomy exists around the individual, the opportunities for abuse and oppression are lessened.

---

[1] Marc Rotenberg, Director of Electronic Privacy Information Center (EPIC), at the Privacy Commissioners annual meeting in Wroclaw, Poland, 14-16 September 2004.
[2] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Universal Declaration of Human Rights Article 12.

Privacy is closely linked to other human rights such as freedom of expression and freedom of assembly, since the protection of the individual against arbitrary state interference is a precondition for exercising political rights in a democratic society. The right to freedom of expression includes not only the right to speak freely or to print, but the right to distribute, the right to receive, the right to read and inquire, the freedom of thought, and the freedom to teach. Also, the freedom to associate and privacy in one's associations are intertwined. Protection of privacy enables us to interact politically without fear, to speak our mind without retribution, and to meet without membership. Privacy enables societal participation and political engagement, and is thus a fundamental component to freedom.

The right to privacy includes both the protection of physical integrity, family life, territories such as the home or the public space, and personal information and correspondence. In relation to the Information Society, it is especially the protection of personal information and correspondence that is at stake.

Why privacy protection is crucial in the Information Society

When a large amount of our interactions take place online, this fundamentally changes the conditions for privacy protection, since the mere nature of digital communication puts privacy in the defensive. Whereas monitoring the individuals' behavior and communication in the physical space requires physical tracking and wiretapping, the point of departure in cyberspace is different. When we do our whereabouts online, our footsteps remain visible unless we take active precautions to hide them. As every footstep leave tracks behind, this gives access to surveillance, which by far exceeds the means and scope for surveillance in the physical world. Thus it is relatively simple for a state, an employer or a commercial party to follow these tracks, to record them, store them, compile them, and combine them. The many ways of surveillance on the Internet allows for widespread and intensive mapping of the life and habits of individuals as more and more services become on-line. What are our buying patterns? Which newspapers are we reading? Which newsgroups and communities do we visit? What are our political or religious beliefs? In a context, where almost all attributes of an individual can be known, all interactions mapped, and all intentions assumed based on records, the need for protection of privacy is crucial to retain a sense of freedom. This calls for active measures to ensure that privacy is still protected and promoted. Measures to ensure that the essence and the principles enshrined in the Universal Declaration of Human Rights continues to be guiding norms for our societies.

Privacy and WSIS

Despite the crucial importance of privacy standards guiding the means to retain, access and use personal information, the WSIS Declaration of Principles contains only a minor

reference to privacy in the section which deals with confidence and security in the use of ICTs: "Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade.(…)."[3]

The following paragraph stresses the support for United Nations activities "to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights".[4]

During the WSIS process, civil society groups have time and again expressed their concern with the strong focus on national and international security and criminal use of ICTs vis-à-vis a state commitment to civil liberties such as privacy and freedom of expression[5]. "Security" is a flexible and vague political term, which can – and has been – used to circumvent civil liberties. The discussions and language around security would be enhanced by a clear definition relating it to network security and by emphasizing that security can only be achieved through measures that are compliant with human right standards, particularly the right to privacy. There remains a tendency to speak of privacy as something that has to be balanced against security, rather than something which is a fundamental premise for security. The rhetoric of "balance" is dangerous, since it addresses human rights as something that can be adjusted according to other state interests. The protection of privacy is fundamental for, rather than contradictory to, the state obligation to protect people within its jurisdiction. In line with this, incursions are only allowed in specific circumstances. In the United States this involves due process, warrants, and situations involving reasonable expectations of privacy. Under the European Convention on Human Rights, incursions must be lawful, and represent the least invasive measure to serve the legitimate aim.

[3] WSIS Declaration of Principles, para. 35, 12 December 2003, Geneva
[4] Ibid, para. 36
[5] The potential use of ICTs by criminals, and as a threat to international stability, have been emphasized all through the WSIS process, not least through the US and European delegations, who have promoted the Council of Europe Cybercrime Convention as a model for future global cooperation and agreement in this field.

In order to give privacy independent priority at a time when means for misuse of personal information are greater than ever, the Privacy and Security Working Group have called for a specific paragraph on privacy[6]. The paragraph or other language to that effect, was never included in the Declaration of Principles. Also, the Plan of Action pays little notice to privacy initiatives, which are limited to two identical initiatives in sections C5 and C6, whereby "c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy", plus some reaffirmation stating that "initiatives to promote security or exchange health data must respect the rights to privacy"[7].

With regard to the controversy between the national political agenda and the international obligations, this can be found in the WSIS Declaration of Principles paragraph 39 (in section 6 on "enabling environment"") in which it is stated that the regulatory framework is expected to reflect national realities[8]. The civil society Human Rights Caucus have time and again expressed concern that the rule of law and the regulatory framework are expected to "reflect national realities" instead of being consistent with the legally binding obligations of States according to the human rights treaties they have ratified.

Finally, it should be mentioned that the Geneva Summit itself had a number of privacy violations, such as RFID tagging of participants without prior notice, and without any information or privacy policy on the retention, use, disclosure, and deletion of the personnel information being collected[9].

What are the challenges ahead?

There are a number of challenges ahead in order to secure just a minimum level of privacy protection within the WSIS context.

The above-mentioned deficits in the Declaration of Principles and Plan of Action (WSIS I) should be remedied in the appropriate sections of the Political Chapeau and the Operational Part (WSIS II), which is currently under negotiation. There still remains a big challenge in

[6] "The right to privacy is a human right and is essential for self-determined human development in regard to civic, political, social, economic, and cultural activities. It must be protected online, offline, in public spaces, at home and in the workplace. Every person must have the right to decide freely whether and in what manner he or she wants to receive information and communicate with others. The possibility of communication anonymously must be ensured for everyone. The collection, retention, use and disclosure of personal data, no matter by whom, should remain under the control of the individual concerned". Privacy and Security Working Group, 22 September 03.
[7] WSIS Plan of Action, 12. December 2003, Geneva. Privacy is mentioned in Section C5, C6, C7 and C10.
[8] "39. The rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centred Information Society.(...) WSIS Declaration of Principles, adopted 12 December 2003, Geneva
[9] A list of problems related to the Geneva WSIS Summit can be found in "How was the Summit ?", Compiled by Rik Panganiban and Ralf Bendrath, 16 December 2003, on http://www.worldsummit2003.org

getting governments to acknowledge that a human rights-based information society is not accomplished by reaffirming existing human rights treaties. It requires political will and priority to effectively protect and promote human rights at national level.

To serve this aim, precise indicators should be defined, in order to evaluate the realization of an information society protecting and promoting human rights. These should be the benchmarks by which we measure progress and by which we review state legislation and policies. One suggestion by civil society have been to establish an Independent Commission on the Information Society and Human Rights, composed of highly qualified experts with a broad geographical representation, to monitor and assess practices and policies on human rights in this context. This is particularly urgent, given the tendency in many countries – both North and South – to sacrifice human rights in the name of security.

With regard to the ongoing controversies on Internet governance, this has important impact on human rights, not least issues of privacy and freedom of expression. Any decision resulting from WSIS must ensure that future Internet governance bodies and mechanisms comply with human rights both through their composition and governing structures and through the substance of their decisions. Internet governance must not result in a lawless zone escaping human rights protection[10].

Human rights learning, and specifically capacity-building on the specific privacy challenges should be included explicitly in the WSIS implementation. Human Rights learning is crucial for people to actually understand and claim their rights, just as it is crucial for state representatives to know the substance of the rights, they are obliged to protect and to promote those rights also with regard to private parties.

Last but not least, it must be ensured that security measures taken during the Tunis Summit follow international privacy principles, including rule of law, transparency, prior notice, least invasive measure, and fair information practices.

[10] In some of the thematic papers issued by the Working Group on Internet Governance, there is a tendency to address privacy as something that is rather peripheral to Internet Governance. This is e.g. the case in the paper on Consumer Protection, as pointed out in the response from the Privacy and Security Working Group,