ICT/Internet and the Right to Privacy

Patrik Hiselius

1 Context of this Paper

Internet is an enabler for human rights. Therefore, ensuring a free, secure and accessible Internet has emerged as a key human rights challenge.

The UN Special Rapporteur on Freedom of Opinion and Expression and the Swedish Ministry of Foreign Affairs, with the assistance of the Swedish Raoul Wallenberg Institute of Human Rights in Lund, have invited to an expert meeting on human rights and the Internet in Stockholm, Sweden, 16-17 June 2010.[1] The meeting will address *freedom of expression*, right to *Privacy* as well as human rights aspects of *access to the Internet*. The discussions are to assist in the formulation of principles or recommendations on the application of human rights in relation to the Internet and offer clarification on how relevant human rights could be implemented in the Internet environment. Special considerations are to be given to *Internet Security*.

> "Right from the early days of electronic data processing in the 1960s, the protection of the privacy of data subjects has been an issue. Over the decades, it has become both more far-reaching in terms of social consequences and more complex in terms of definitions, contexts, technology, stakeholders, and so forth. Today, privacy is a prime component of almost every discussion of the networked information society."[2]

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):[3]

- **UDHR:** 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.
- **ICCPR:** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

1 Information about this expert groups meeting is available at "www.sweden.gov.se/sb/d/2059".

2 Bylund, M., Johnson, M., Lehmuskallio, A., Seipel, P., and Tamminen, S., *Privacy Research through the Perspective of a Multidisciplinary Mash up*. In Nordic Yearbook of Law and Informatics, Greenstein, S. (ed.) 2006-2008, p. 140.

3 In Europe hereto; 1) *European Convention for the protection of Human Rights and Fundamental Freedoms* (art. 8), "conventions.coe.int/Treaty/EN/Treaties/html/005.htm"; 2) *Convention n. 108/81 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data* (art 8), "conventions.coe.int/treaty/en/treaties/html/108.htm"; and 3) *The charter of fundamental rights of the EU* (art 8), "www.europarl.europa.eu/charter/pdf/text_en.pdf".

> "The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose."[4]

2 Purpose of this Paper

This short paper, written on behalf of Telia Sonera, aims to facilitate the expert meeting discussions on the right to Privacy. (This is a slightly revised version, mainly for the format of this publication.)

3 Privacy

What is 'Privacy'? In the European Union, instead of using the term 'Privacy', in general the notion 'right to data protection' is used.

It is recognized that the subject for protection, 'personal information', is something very difficult to define.[5] A simple reason is that, what I regard as private you might not, and what was private yesterday might not be so tomorrow. Privacy therefore is difficult to balance against other legitimate interests such as freedom of expression or protection against terrorism. Privacy is more of a process than a given, rather than something we 'have' it is something we 'do'. We choose what to share about ourselves, to whom and when. Privacy is not at first hand about hiding secrets or unwanted and illegal behavior. In practical terms, it is most often very every-day and simple information we choose to share, or not to share.[6] So, "privacy and the protection of privacy must be described as a highly dynamic phenomenon. This means, among other things, that the notions of privacy change over time, that privacy is context-dependent (not the least with regard to different cultural practices), and that the urge for privacy protection may be both emotional and rational."[7] It is an important and difficult task to assure that – when analyzing, debating and regulating Privacy – differences between large global cultures are taken into account.

---

4 The Global Network Initiative, Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies, 'Principles on Freedom of Expression and Privacy', "www.globalnetworkinitiative.org".

5 Global Network Initiative (GNI) Principles, Annex A., Definitions, **"**Participants are aware of the range of definitions for "personal information" or "personally identifiable information" and acknowledge that these definitions vary between jurisdictions". The GNI uses the term "personal information" and interprets this to mean "information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual".

6 Bylund, M., Personlig integritet – en ovanligt hal ål, July 1st 2009, "www.sics.se/~bylund/markustankar/?p=1".

7 Bylund et al., supra n 2 p. 140.

Privacy has since long been defined as a private sphere, 'the right to be let alone'.[8] While still valid, this starting-point "must be placed in a modern setting where it has to co-exist with people's interest in a networked life"[9]. In other words, also the rather new phenomenon of social media and its consequences as to the willingness to share personal information must be taken into account.

4 Understanding the Role and Position of ICT in Respecting and Promoting Privacy

ICT enables more and more people to access and expose more information about each other. ICT also allows for anonymity and retaining of Privacy. Digital storage of personal information, arguably, can be more secure than traditional storage. Services can be designed to give control over Privacy preferences. ICT-companies can take actions to prevent unauthorized access to personal information, only disclosing it when required by law, exercise special care to prevent unauthorized disclosure and expect suppliers and contractors to support international standards on human rights. But there are also risks.[10] There is little information available about the real costs of Privacy and Privacy incidents; it is still an under-researched area.[11]

The ICT-industry, with the Internet, has become more and more global. Internet has also brought about convergence. There are *many industries* to consider in a dialogue regarding protection of Privacy; access provides, hosting providers, carriers, Internet-companies, manufacturers, on-line content providers, collecting societies, software providers, security providers, on-line gaming and on-line gambling providers, the e-advertising community, the financial sector (credit cards and on-line banking), etc.

When debating and regulating issues that affect Privacy it is important to have *Data Protection Authorities* and *Consumer Organizations* on board.

8 Warren, S. D. and Brandeis, L. D. 1890. The right to privacy. Harvard Law Review.

9 Bylund et al., supra n 2 p. 142.

10 BSR, 'Human Rights in a Wired World – How Information & Communications Technology Impacts Human Rights', June 2009, "www.bsr.org/research/human-rights-wired-world. cfm". Personal information can be accessed by third parties, IP addresses can be tracked. User actions and words may be monitored without the user's knowledge. The Internet can reveal someone's private information (true or false) to millions of others. Map services can visually expose information, etc.

11 PRIME (Privacy and Identity Management for Europe), Contract No 507591, 25th of May 2008, (page 144).

5 'Internet Security' and Privacy

Issues regarding 'Internet Security'[12] range from *consumer aspects*, protection against spam and viruses in the individual's device, all the way to issues of *national security* and international fight against denial-of-service attacks and terrorism. And these two ends overlap. Both the end-user and the society benefit from robustness, redundancy and surveillance – but only if balanced and built on *trust*. Many companies at every level of the ICT-sector have worked to build and maintain trust. States have put in place regulation for the protection of Privacy, in balance with freedom of expression and security needs. Most consumers/users/citizens feel comfortable engaging in a range of communications and transactions generating personal information. Caution is needed in protecting and preserving this balance.

Actions based upon *corruption* pose problems both for States and businesses. Work against corruption is to the benefit of human rights in general, including Privacy.

6 'Access to the Internet' and Privacy

Infrastructure deployment as well as provisioning of new on-line services *disregards national borders*. To provide for a level playing field and a global minimum level of protection of Privacy, there is a need for a harmonized regulatory framework. The aim should be a level playing field for all market players on the global Internet, regardless of the fact where the specific data controller has its establishment.

Regulation of ICT is often, to allow for needed flexibility, amended by market-driven standardization. Global product and services standards should, to the extent possible and feasible, be designed to protect and promote Privacy.

Regulation regarding international data transfers can, especially in a cloud computing scenario, be problematic for groups of companies. It should be noted that the 'Madrid Resolution' (see below) refers to 'transfer carried out within corporations or multinational groups'. Could this economic reality be considered as a new approach in connection with data protection rules?

The Cloud – The evolution of the Internet has enabled the evolution of a new kind of business model – one built on virtual networks and software, for remote access by users no longer constrained by physical locations. Terminals are becoming access-devices. Hereby, access becomes even more important for the user. Trust and security will be one of the key differentiators in the market-place.

12 Other terms of relevance: 'Data security'; Confidentiality, integrity and availability of data. 'Network Integrity'; Measures put in place to protect the information in transit from disclosure or unauthorised change.

7 Challenges to Meet in Promoting and Protecting Privacy

A main challenge lies in use of *definitions*. As an important example, the North American 'Privacy' approach (mainly market-driven) and the EU 'Data Protection' approach (the State having an important role) imply significant differences.

A private player cannot undertake to break *national law*. Any international instruments must be without prejudice to and understood in conjunction with the obligations applicable to companies, their employees and their activities under national law. Governments have a variety of concerns widely accepted, defined on the level of national security, through Parliaments and by Governments. Private players most often lack sufficient knowledge and ability to question government determinations about local security interests. As an example, when authorities demand personal information, written demands are preferable. It is, however, recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written. Businesses should, as it has been formulated by the BLIHR companies[13], "strive to uphold the spirit of internationally recognized human rights while still complying with law". But what does that mean in practical terms? Could ICT-companies assess that buyers will use its products or services to violate human rights? How could a company interpret the intended use of a product or service when the same functionality can be used for good and/or for ill?

CDT has recently identified[14] five *technological trends that pose special challenges* to Privacy; cloud computing[15], behavioral advertising, deep packet inspection[16], location awareness and re-identification of seemingly anonymous data.

Transparency builds trust. Both states and businesses should seek to be transparent as to decisions and activities balancing Privacy vis-à-vis other interests.

Internet is *global*, a fact that needs to be reflected in a Dialogue. Participants need to represent all parts of the Globe. Interaction and results should be taking place and be considered in several large languages.

---

13 BLIHR #4, Business Leaders Initiative on Human Rights, Policy Report 4, 7. Appendix.

14 Comments of CDT, the Center for Democracy & Technology, to the European Commission in the matter of the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data, Submitted December 31, 2009, "www.cdt.org/files/pdfs/CDT%20Comments%20to%20the%20European%20Commission.pdf.".

15 "Limiting cross border data flows is becoming increasingly difficult and impractical" writes CDT, supra n 13, Section 1.a.

16 "In part because the Internet was developed around the end-to-end principle, consumers have come to expect that their Internet communications pass through the network without being snooped on the way. DPI dramatically alters this landscape by providing an ISP or its partners with the ability to inspect consumer communications en route. Thus, deploying a DPI system likely defies the expectations consumers have built up over time." CDT-comments, supra n 13, Section 1.c.

There might be a need to decide on narrowing the *scope* of specific discussions. Should discussions cover also Privacy issues in employer/employee relations? Protection as to data relating to legal persons? Should there be other limitations?

8 On-going Processes in Relation to Protection and Promotion of Privacy

- The portal of the UN Special Representative on Business and Human Rights, "www.business-humanrights.org/SpecialRepPortal/Home".
- The Global Network Initiative (*GNI*), "www.globalnetworkinitiative. org/"-
- *Business Leaders Initiative on Human Rights* (*BLIHR*) – Policy Report 4, March 2009, "www.blihr.org/Legacy/Downloads/BLIHR%20Report %202009.pdf".
- *The Madrid Resolution*[17], November 2009, "www.gov.im/lib/docs/odps/ madridresolutionnov09.pdf".
- The European Stockholm Programme for further development of freedom, security and justice. The aim is to preserve Privacy beyond national borders, December 2009, "ec.europa.eu/justice_home/fsj/intro/ fsj_intro_ en.htm"-
- The on-going negotiations for an Anti Counterfeit Trade Agreement, *ACTA*. The draft document, April 2010, "trade.ec.europa.eu/doclib/ press/index.cfm?id=552", needs to balance protection of IPR's with Privacy.
- The Internet Governance Forum (*IGF*) in Vilnius, Lithuania, in September 2010, "www.intgovforum.org/cms/the-preparatory-process/ 475-preparing-the-igf-2010-meeting-". A range of sessions, workshops, forums and dynamic coalitions[18] will be held on access, openness as well as on security and Privacy.

17 Data protection authorities from over 50 countries approved these international privacy standards. The resolution includes a series of principles, rights and obligations that any privacy protection legal system must strive to achieve. The purpose of the document is to 1) Define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and 2) Facilitate the international flows of personal data needed in a globalized world.

18 "The meeting will provide space for active Dynamic Coalitions to meet and further develop their efforts. Meetings of Dynamic Coalitions should not be workshops. They should be action oriented and make an effort to ensure that a broad range of stakeholders can bring their expertise to the discussions." 'Internet Governance Forum (IGF) Programme for the 2010 Meeting', July 2010, "www.intgovforum.org/cms/".