

DG INTERNAL POLICIES OF THE UNION

Policy Department Economic and Scientific Policy

**Internet of the future: Achieving Transparency,
Pluralism and Democracy**

Briefing note

(IP/A/ITRE/WS-IC-2008-139)

This study was requested by the European Parliament's committee on Industry, Research and Energy (ITRE).

Only published in English.

Author: Prof. Yves POULLET
Professor and Director of the CRID
University of Namur
rempart de la vierge 5
5000 Namur (Belgium)
yves.poullet@fundp.ac.be
<http://www.crid.be>

Administrator: Maya GADZHEVA
Policy Department Economy and Science
DG Internal Policies
European Parliament
Rue Wiertz 60 - ATR 00L0xx
B-1047 Brussels
Tel: +32-2-2832858
Fax: +32-2-2846929
E-mail: maya.gadzheva@europarl.europa.eu

Manuscript completed in January 2009.

The opinions expressed in this document do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised provided the source is acknowledged and the publisher is given prior notice and receives a copy.

E-mail: poldep-esc@europarl.europa.eu.

TABLE OF CONTENTS

- Executive Summary 3**
- Introductory Remarks 3**
- 1. The Information Society: major trends 4**
 - 1.1 Trends as regards the technologies themselves 4
 - 1.2 Trends as regards applications 5
- 2. Liberties and Information Society 7**
 - 2.1 Privacy and Information Society 7
 - 2.2 Freedom of Expression and Information Society 12
- 3. Final statements..... 17**
 - 3.1 ICT challenging or enhancing liberties? Towards a value sensitive design of the technologies 17
 - 3.2 Crucial role of the state 17
- Bibliography 20**

EXECUTIVE SUMMARY

The title quite ambitious leads to analyse the main challenges our fundamental freedoms have to face in our Information Society. Our reflections start with a description of the main characteristics of the technological landscape and their significance. This description introduces two main debates:

- the first one is related to the impact of new ICTs on our privacy considered in the broadest sense as the condition for each individual to dignity and self determination;
- the second one analyzes how freedom of expression is threatened in our Information Society.

On these two issues, certain avenues of inquiry will be developed and solutions will be suggested in order to avoid interference with these two fundamental liberties. In conclusion we will address reflections about the role of the Technology, the State and the Citizens.

INTRODUCTORY REMARKS

ICT a major tool for our liberties - Information Communication Technologies (ICTs) with their ubiquitous and universal characteristics are drastically modifying our environment as well as our economic and social relationships. This trend will increase in the future in a way which is only partially predictable at the time being. The ICT are used in an increasing number of contexts and are offering to each of us a place without limits where we are able to better express ourselves, where we have access to more and more personal services but also where the physical or social barriers which separated the various visions of the world tend to disappear. In this sense, ICTs create a unique opportunity to develop ourselves and to enter into a dialog founded on the recognizance of a large diversity of opinions. This might contribute to a cultural, economic, intellectual, democratic and human enrichment of the global society.

Between dream and nightmare - Nevertheless, if we are not cautious, this dream – which is inherent to the potential development of the Information Society – might turn into a real nightmare. The way in which the technologies are presently designed and applied can severely affect the development of our liberties and of our democracies. Our contribution aims to define the challenges raised by the development of ICTs in order to propose certain reflections and possible solutions both at the European level and at the global level in the context of the next IGF.

1. THE INFORMATION SOCIETY: MAJOR TRENDS¹

1.1 Trends as regards the technologies themselves

About Moore's Law - The development of ICT can be firstly described in a continuous and tremendous growth of computer and communication systems capacities. The so-called Moore's Law predicts that every 18 months the storage capacity of a computer is multiplied by two for the same price, which implies the multiplication by 1,000 in fifteen years. It is becoming possible to store on a personal computer the records of all the events of my life and to set-up a central GRID collecting the basic identification data of all people around the world. This capacity of storage doubled by an increasing capacity of processing and transmission explains how Google can validate your request, scanning in less than 10 seconds more than a thousand million sites worldwide. It explains also the development of what we call the Web 2.0 multimedia applications like YouTube, Daily motion, etc.

Internet revolution - The Internet revolution might be described from different points of view. The global character of this network has a double meaning. It means not only the universal dimension of this infrastructure, implying the interoperability of technical norms². Internet also leads to the convergence of all networks, which were traditionally clearly separated like TV channels and mobile infrastructure and thus the possibility to cross match the data created by all these communication activities. That convergence is doubled by the convergence of the terminal. Our mobile devices and computers are achieving today activities like voice telephony services, TV or radio programmes reception, e-mails communications, etc. which 30 years ago were reserved to specific and dedicated terminals.

Ambient Intelligence - Ambient Intelligence³ is perhaps the more recent outcome of the ICT evolution. With the miniaturization of the terminals to a "smart dust" and their implantation in objects, clothes and even in our own bodies, it is now possible to conceive interaction among human beings and their environment, through this "Internet of Things". The technology is becoming ubiquitous covering all the events of our everyday life. We also speak of a "learning technology" insofar as it is able to adapt its functioning to the data obtained through its use. The networks created by the dialogue between things, among things or between things and people create a space progressively invested by ICTs. At the heart of these networks, the human being can become a "thing" itself inserted into a relation with other things which react to its or his/her presence.

Digital identities - "Digital identities" are increasingly linked to individuals or to be more precise with his or her bodies (biometric data) or with objects under their use (cookies or IP as regards the personal computer or the communication mean; tag number as regards RFID⁴

¹ For a more complete view on these trends, see Y. Pouillet – A.Rouvroy, "Introductory Remarks, General report, European Conference on Ethics and human rights in a Information Society organized by UNESCO and Council of Europe, Strasbourg, 13-14 Sept., 2007 available at the UNESCO website.

² An additional effort to coordinate infrastructure is being propelled by the European Organization for Nuclear Research (or "CERN", Europe's scientific consortium where the World Wide Web was born). CERN's Large Hadron Collider Computing Grid project includes a plan "to integrate thousands of computers worldwide into a global computing resource," or Grid. The project's most enthusiastic proponents contend: "*The Grid goes well beyond simple communication between computers and aims ultimately to turn the global network of computers into one vast computational resource.*".

³ "*The central idea of these networks is to create environments in which people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects. It is an environment that is capable of recognizing and responding to the presence and actions of different individuals in a seamless, unobtrusive and often, invisible way using several senses*".

⁴ RFID = Radio Frequency IDentifier.

enshrined in clothes or...) or simply with works or objects belonging to individuals or not⁵. One underlines the different roles of these “digital identities”. They firstly might be used as “authentication” tool, especially to permit the access to certain resources. Secondly they are essential for the reconstruction of an informational image about a person - identified or not - apart from pieces of information scattered in databases geographically dispersed through the network and that without any limit of borders. In other words they permit the traceability (the capacity to follow the movement of a person, a good or a message) and more the ability to establish links among different databases in order to retrieve the information concerning the same individual identified or not (e.g. cookies, RFID tag number, etc.)⁶. Digital identifiers (like IP address, RFID tag number) permit also to contact people by sending us appropriate messages. **That triple characteristic of digital identifiers, link ability, traceability and contact ability, explains why special attention must be given to that kind of data, which at first glance seem less sensitive than biographic data.** Finally, let us notice that biometric data precisely because there are directly linked with the body are available during the entire life of the individual and that traces revealing DNA might be found very easily (blood, hair, etc.).

1.2 Trends as regards applications

User Generated Content - User Generated Content’s applications definitively constitute, from the Internet user point of view, the most prominent new applications on the Web. About 60% of the content available on the web is coming from these new applications, like social networks, Wikipedia, online games or You Tube, generally grouped under the concept of Web 2.0 applications. These emerging applications radically transform the relationships among the actors. In the traditional scheme, the role of the information service provider on one side and the role of the Internet users on the other are quite distinguished and the regulation available is normally reserved only to professionals. What happens when the Internet users are, in the context of these new applications, playing a similar role as the traditional information providers by posting news on there blogs or on You Tube and becoming data controllers by putting information online about themselves and about third parties? Can we consider that the author of a blog is a journalist or an editor, subject to the same deontology and legal duties that the press companies? New risks and threats derive from the very sensitive nature of the data they are posting, the illicit or harmful information they are diffusing, etc. **The privacy risks created by the use of these data by third parties in the context of certain secondary uses are to be pinpointed.** We know that employers are often using data concerning their employees available at social networking sites and that companies are using this data to build up profiles and to take decisions on the basis of these profiles which can potentially discriminate the internet users.

Profiling techniques - Precisely the profiling techniques⁷ seem to be more and more used by companies or administrations. Profiling might be defined as a computerised method involving

⁵ See the Object Names System (ONS) put into place by GSI in the context of a large development of RFID and in a way quite similar to that chosen for the DNS operated by ICANN with the cooperation of Verisign. ONS will permit to trace a product to know exactly the producer, distributor, the ingredients, etc. Placed at a certain distance of a reader which might be the mobile, it permits a consumer to know exactly the product he or she is purchasing.

⁶ Digital identities might be considered as “matching identifiers”. “Matching identifier” refers to an item of information making it possible to identify the same individual in two data processing operations, each of which has a different file controller or a distinct purpose. Items of personal data include matching identifiers such as cookies which enable individuals to be recognised and their actions or movements to be tracked over time, whether in cyberspace or not.

⁷ R. Brownsword, ‘Knowing Me, Knowing You—Profiling, Privacy and the Public Interest’ in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen*, Dordrecht, Springer, 2008, pp. 362-382.

data mining from data warehouses, which may enable to place individuals, with a certain degree of probability, and hence with a certain induced error rate, in a particular category in order to take individual decisions relating to them. Taking the opportunity of the huge number of traces generated by the Internet users apart from their use of communications services and by the data collected just in time thanks to the technologies and coming from a large variety of sources, companies or administrations are defining profiles and apply these profiles to individuals in order to take decisions towards individuals identified or not. "Adaptive pricing" is often quoted in that context. According to the profile of the customer, the information service provider might decide to adapt the price of a service or a product. One to one marketing is largely based on that technique and more and more administrations are detecting presumed smugglers or terrorists using that method.

New actors: the intermediaries - Before discussing the implications of these applications as regards our fundamental liberties, we would like to underline the increasing role of **intermediaries**. By intermediaries, we mean all the activities which render useful the usage of the applications. It might be platforms offering the Web 2.0 services, search engines or all communications services providers as well as operators intervening in support of these communication services like certification providers. These persons play a decisive role by providing added value services but at the same time might be considered as gatekeepers to the information provided by or to internet's users. They are ranking the information, facilitating the access to that information and in certain cases, selecting the information offered.

To what extent they might be held liable in case of diffusion of illicit or illegal messages by their platform? The question has recently been raised after the diffusion on You Tube of images provided by the future Finnish killer⁸. Two additional remarks: firstly, the economy of the functioning of these services is often quite obscure since they are using the information they collect for their own benefit or the benefit of a third party by developing marketing operations or other added value services; secondly, the law enforcement authorities might be tempted to cooperate with such services providers in order to find potential suspects in criminal affairs.

Privatization of cyberspace – By privatization of cyberspace we refer to a quadruple evolution present in cyberspace. The first one concerns the fact that more and more through technical means (Digital Rights Management systems, Tattooing⁹, etc.) the information might become the "property" of their producers or authors by restricting the access to third parties or controlling their uses. We will come back on that reality later (see point 2.2). The second point underlines the fact that entering into the cyberspace requires going through certain private gatekeepers who control the content and the access to the public space of information and discussion. The third point recognizes that technologies are blurring more and more the traditional distinction between public and private spaces. So, for instance, surfing the Internet from my home reveals outside of the four walls of my private domicile, my habits and my preferences better than if I were in the street or in public or professional spaces. Finally, it is quite clear that protocols' norms as well as terminals' ones which generate or regulate the data flows are no more fixed and regulated by public authorities but by private companies or standardisation bodies like IETF, W3C or ICANN¹⁰.

⁸ The 18 year old Pekka-Erik Auvinen in November 2007, see for instance timesonline, "Finish "YouTube Killer" was bullied at school", 8 November 2007.

⁹ Tattooing (or watermarking) is creating a permanent, indelible mark in the digital record, see Edward Barrow, "Rights clearance and technical protection in electronic environment", February 1996.

¹⁰ IETF = Internet Engineering Task Force; W3C = World Wide Web Consortium; ICANN = Internet Corporation for Assigned Names and Numbers.

2. LIBERTIES AND INFORMATION SOCIETY

How Democracy is at stake in our Information Societies? - Democracy is at the same time the condition for the autonomy of human individuals and conditioned by the effective exercise of this autonomy. Insofar as Privacy defined as self-determination is considered as ensuring our self development, it might appear as an intrinsic condition of our democracy and its vitality. Freedom of expression is the result of this free participation. It implies the right for everyone to be heard and to have access to pluralistic and diverse opinions.

2.1 Privacy and Information Society

*What does privacy or self-determination mean?*¹¹ - In 1983, the German Constitutional Court in the famous census case¹² has approached the privacy as the fundamental right to self-determination and have underlined, in a very prospective way, the risks incurred by our privacy in our modern Information Society. The Court said:

“The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals’ behavior by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behavior is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behavior. If he reckons that participation in an assembly or a citizens’ initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good (“Gemeinwohl”), because self-determination is an elementary functional condition of a free democratic society based on its citizen’s capacity to act and to cooperate.”

The Court’s assertions might be analyzed in three steps: first, the Court gives a broad definition of the right to privacy; second, it enumerates the new threats to privacy in our information society; finally, in the third step of its reasoning, the Court recognizes a clear link between privacy protection and democracy. What “self-determination” presupposes and what it allows in a given society (the “facets” of privacy) is unavoidably contingent on many evolving factors.

Besides the state of technological development – suggested by L. Lessig¹³ as the central, if not exclusive, reason to adapt our normative instruments –, the nature of prevailing institutional arrangements and socio-political structures is a critical factor to take into account in order to explain the chronological development of the diverse and interdependent facets of the right to privacy. To summarize, **we argue that privacy, as a legal right, should be conceived essentially as an instrument for fostering the specific yet changing *autonomic capabilities* of individuals that are, in a given society at a given time, necessary for sustaining a vivid democracy.**¹⁴ The Court anchors the privacy and the data protection

¹¹ On that topic, read A. Rouvroy- Y.Poullet, art cit.

¹² Constitutional Court, Dec. 15, 1983, EuGRZ, 1983,p ; 171 and ff.

¹³ L. Lessig, Code and other Laws in Cyberspace, New York, Basic Books, 1999.

¹⁴ See, in the same sense, R. Sunstein, *art. cit.*, p. 157.

legislation directly in two ethical values which undoubtedly are of universal nature: the right to dignity and to self-development.

Privacy as a “fundamentally fundamental right” - Our capacities for both reflexive autonomy and deliberative ability to participate within the societal discussion are threatened in a unprecedented manner by the intensification of surveillance and monitoring technologies such as CCTV, data mining and profiling, RFID and the “internet of things”, ubiquitous computing, and “ambient intelligence”.¹⁵ The German Court acknowledged that self-imposed restrictions on deviant behaviour, or on participation in an assembly or in a civil society initiative by fear that this behaviour and activities could be disclosed to others with adverse consequences ensuing put our democracies at risk since they hinder the free expression and the autonomy of the citizens, what is fully necessary in order to ensure a democratic discussion.

As expressed by Burkert¹⁶, privacy may be considered a “*fundamentally fundamental right*”. Privacy is not a freedom on the same rank with the others: essential to human dignity and individual autonomy, and translating these moral principles in the legal sphere, privacy is a necessary precondition to the enjoyment of most other fundamental rights and freedoms.

Privacy as a broad, twofold and evolving concept - The Court anchored their approach to the right to privacy in two distinct constitutional provisions reflecting the primacy, in the German constitutional order, of two fundamental values: human dignity on the one hand, and individual self development in a free society on the other hand. The combination of these values inspired the Court's acknowledgement that a “generic right to personhood” (“*An Allgemeine Persönlichkeitsrecht*”), existed as the core of the legal constitutional order of the German Republic. That right, transposed in the technological context of 1983, was to be understood as a right to informational self-determination that justified the adoption of the Data Protection Act. That anchorage of the right to data protection to human dignity and self-development must be underlined. **It implies that data protection legislation is definitively to be considered as a condition for ensuring the dignity of the person but in the same time it reveals that data protection legislation is not exhausting the right to dignity and that the privacy protection must be evaluated in certain cases directly by reference to this dignity principle.**

Chronologically, privacy has first been conceptualized as a right to 'seclusion' (opacity, or privacy as solitude) and, secondly, as individual informational control or empowerment (“the ability of an individual to control the terms under which his or her personal information is acquired and used”, formalised through fair information practices).

The initial interpretation of the right to privacy as understood by the 1950 Council of Europe Convention on Human Rights had much in common with the American “right to be left alone”, in the intimacy of one's private and family life, home and correspondence. The right to opacity means that each individual must have a physical place where to express him or her self and the possibility to exchange views or to reveal his intimate beliefs to others through private communications means without being observed from outside or by third parties.¹⁷ This

¹⁵ For further reflections on how the internet revolution and more recently the Ambient Intelligence technologies are metamorphosing the risks incurred by the individuals and their basic rights and call for new legislative actions reinforcing the different identified facets of the right to privacy, see Antoinette Rouvroy, ‘Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence’, *Studies in Law, Ethics and Technology* (forthcoming).

¹⁶ H.Burkert, ‘Dualities of Privacy -An Introduction to ‘Personal Data Protection and Fundamental Rights’’, in *Privacy- New visions*, M.V. Perez, A. Palazzi (eds), Cahier du Crid, to be published in 2008.

¹⁷ About the history of the privacy concept, read notably D.J. Solove, “*Conceptualizing Privacy*”, 90 *California Law Review*, 2002, 1085 and ff..

'right to seclusion' (in other words, the right to not participate within the Information Society) might well be even more vital today in our modern society than ever before, justifying the new legal tools put into place in order to protect 'opacity' against the new technological and socio-political challenges of the day. **What characterizes the present Internet world is precisely the unprecedented possibility that we will be constantly surveyed through the multiple traces we leave in the cyberspace and through the gradual invasion of our private sphere by terminals of multiple and ubiquitous nature (from personal computers, GPS, mobile phones, RFID, etc.), dissolving the traditional distinction between public and private spaces.**

The other facet is precisely the right when we are participating to the Information Society to have a certain master ship on the data flows concerning ourselves.

It implies and explains the fundamental principles of data protection (fair processing, performed for specific purpose, on the basis of the subject's consent or of other legitimate basis laid down by law, subjective rights of the data subject to access and rectify collected data) have been formalized in the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe,¹⁸ and restated in the fair information principles of the European directive on the protection of individuals with regard to the automatic processing of personal data¹⁹ and in the European directive concerning the processing of personal data and the protection of privacy in the electronic communication sector.²⁰ *"The ability of an individual to control the terms under which their personal information is acquired and used"*²¹ is often presented as the hallmark of data protection.

New risks in our Information Society - The rationale behind the data protection regimes relates to the risks to individual self-determination carried by the early development of the information technologies infrastructures. The use of information technologies have been considered, from the beginning, as worsening power asymmetries between data subjects (the individuals whose data are processed) and the data controllers (in charge of the collection, storage, processing, use and dissemination of data). Technological developments gradually create a situation where:

- a) there is virtually no limit to the amount of information that can be recorded,*
- b) there is virtually no limit to the scope of analysis that can be done-bounded only by human ingenuity, and*
- c) the information may be stored virtually forever.*²²

These developments had of course direct impact on the autonomy of the data subjects: vast collection and intensive processing of data enable data controllers such as governmental authorities or private companies to take decision about the individual on the basis of this collected and processed personal information without allowing for any possibility for the data subject to know exactly which data would be used, for which purposes, for which duration and overall without control of the necessity of this processing as regards the purposes pursued

¹⁸ Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS, N°108, Strasbourg, 28 January 1981.

¹⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L* 281, 23 November 1995.

²⁰ European Directive 2002/58/EC EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.

²¹ M.J. Culnan, « Protecting Privacy online: Is self-regulation working? », 19 *Journal of Public Policy Market*, 2000, 1, pp. 20 and ff.

²² H. Nissenbaum, « Protecting Privacy in an Information Age: the Problem of Privacy in Public Spaces », 17 *Law and Phil.*, 1998, pp. 576.

by the public or private bureaucracies. Data Protection regimes were thus designed (and, in some countries, translated into self-regulatory measures) in order to better balance 'informational power'.

This resulted in a widening of the protection previously limited and centred on intimate and sensitive data, which now includes all personal data defined as “information about identified or identifiable individuals”, and in the attribution of new rights to the data subjects, including an 'access right' allowing a better control over the uses and dissemination of personal data and, finally, the imposition of limitations to the permissible processing by data controllers, especially through the requirements that data processing will be fair, legitimate (another word for proportionate both as regards the existence of the processing and its content), and secure.²³

The relationships between data controller (D.C) and data subjects (D.S) in our information Society between KAFKA and ORWELL worlds –“Towards an Observation Society”- In a recent book, Solove describes the evolution of the relationships in our Information Society using two paradigms drawn down from two novels: “The Trial” of KAFKA and the “ 1984” or “BIG BROTHER” of Orwell. With the first, it denounces the radical and increasing opacity of the data capture and data flows permitted by the increasing use of ICTs and their ubiquitous character. This opacity leads to a certain anticipatory conformism in the sense that data subjects adopt the behaviour they believe is expected by the data controllers. The increasing asymmetry of informational powers is also due to the huge number of data, Data Controllers are collecting and processing which enables them to define profiles and to take the “appropriate” decisions on the basis of the data they are capturing about our behaviours, our movements, facial emotions, clicking habits: in other words on the basis of a lot of instantaneous slices of our lives we never expected they might be of a certain significance. One adds that Information systems might keep memory of all these events by storing that at long term. Information systems have a memory an individual has not.

This phenomenon comes together with the emergence of certain applications which are linked to the technologies of ubiquitous computing, inducing what we might call the “**Observation Society**” paradigm, Under this paradigm, the D.C. combines multimodal capture of data "extracted" from human bodies with an implicit understanding and interpretation of this data as valid and privileged source of "truth" about the persons, their preferences, intentions, etc., following the assumption that the ‘body does not lie’. Decisions are taken *a priori* on the basis of this data and profiles rather than on information by the data subjects. Since the Data subjects are not aware of this they are faced with decisions they are unable to understand and definitively to contest.

Do we need new legislation? – Transparency and proportionality as two key principles - Our privacy legislations are grounded on two main principles: transparency and proportionality. Undoubtedly, these two principles must be asserted again and in a certain extent enlarged.

- i. So, we do consider that ***transparency*** should encompass in our information society the right to a mastered and transparent functioning of the terminals equipment including RFID or other sensors embedded in our daily environment. Our computers are functioning to a large extent without possibility for us to know exactly what they are exchanging, receiving and processing. **The transparency of the processing means also the right to be informed about the data flows generated and the D.C. involved in these networks (Who has access? For which purposes? ...). As regards the profiling, special attention must be given to an access to their**

²³ Security is envisaged in its broadest sense, meaning integrity, confidentiality, accountability and availability.

existence and logic. The possibility for refusing the profiling application and blocking certain automated data flows has to be granted to the individuals.

- ii. The *proportionality* principle has to be recalled at a moment where data capture is so easy and data processing capacities have grown to an unexpected level and that data even when they concern instantaneous slices of my life might be kept for an unlimited period. Economic efficiency including in the interest of the consumers or the citizens (see the e-government efficiency myth) and private or public security nowadays are presented as justifying the processing. We have to resist to the temptation that since data is getting easier to capture and to process, its use to promote efficient services making more rentable the activities of companies or ensuring a better public service or control of the respect of the public regulations must be *a priori* permitted.

A societal control measuring the impact of the ICT applications on the individuals' autonomy is needed. That means that the balance between better efficiency and public interests has to be analysed extensively and from a social, psychological and ethical point of view too.

Proportionality and the debate between public security and privacy – Societal evaluation is crucial as regards applications developed by law enforcement agencies and intelligent services in the name of public security interests. Considering certain of these applications,

“one can safely assert that the mental privacy, the most intimate sphere, is being threatened, violating person's most secluded dimension. After 9/11, “privacy in the age of terror” would appear to be doomed. Not only is privacy no longer regarded as a fundamental right; in fact, it is too often considered a hindrance to security, and overridden by emergency legislation”²⁴.

The debate between security and privacy is too often presented as a conflict between two fundamental rights placed on the same footing; sometimes it is argued that the right to security is more fundamental than the right to privacy. Against this argument, we totally agree with the European Data Protection Supervisor when he asserts:

«a message such as: "No right to privacy until life and security are guaranteed" is developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford. [...] the Home Secretary of the United Kingdom, Dr John Reid, called for human rights law to be rewritten, stating that "The right to security, to the protection of life and liberty, is and should be the basic right on which all others are based". [...] This position could be potentially dangerous and may produce more problems than it seeks to solve... There should be no doubt that effective anti-terror measures can be framed within the boundaries of fundamental rights. It is these rights that need to be protected under all circumstances in a democratic society. In the past examples can be found in different parts of Europe where the failure to protect fundamental rights has served as source of continued unrest rather than ensure safety and stability ».²⁵

Need to reinforce Data Protection authority – Both the trend to evacuate more and more the proportionality judgment and the more and more opaque ICT environment have to be counterbalanced by granting more and more powers of investigation to DPA. The role of the DPA is definitively to ensure that the main principles of the Data Protection legislation are effectively respected and in case where a societal assessment is needed to create the possibility of a public debate and to stimulate it. **We are convinced that this debate due to**

²⁴ S. Rodota, “Data Protection as fundamental Right”, in *Reinventing Data Protection*, S. Gutwirth et alii, Springer Verlag, 2008 (to be published).

²⁵ CEPD, « Letters to the incoming presidency: fundamental rights are not captives of security”, 11 June 2007, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf.

the global character of the technology and their promoters has to be led at the European level, notably thanks to the Article 29 Working Party²⁶ by giving to this Group a real autonomy including financial, personal and managerial means.

Need to focus on terminal and information systems – Our traditional data protection legislation is considering only the relationship between data controllers and data subjects. Telecommunications protocols and the functioning of the terminals do not include data protection as a key requirement but as an option generally left to the discretion of manufacturers of the hardware and software that incorporates these standards. The Article 29 Working Group has argued that the principle enacted by Recital 2 under the Data Protection Directive which clearly asserts that technology must be at the benefit of the individuals and the society, might be considered as a justification for imposing on manufacturers of terminal equipment (including software elements incorporated into the terminal) certain obligations aimed at the transparency of their operation and preventing the unfair or illicit use of personal data associated with the connecting to and communicating with the network. It should be noted that these manufacturers are not covered as such by the present directive since they are not controllers of a file. **However, as the design of the equipment influences many processing operations, certain security responsibilities should be imposed on them so as to prevent operations to be carried out in unfair or illicit manner by third parties, They should be required to ensure transparency since the user of the equipment must be able to exercise a certain amount of control over the data flows generated by their use.**

2.2 Freedom of Expression and Information Society

Positive preliminary statement and from privacy to freedom of expression - The development of the Information Society increases the chances not only for individuals but also for communities to freely express opinions in cyberspace and receive information necessary for the exercise of their rights as citizens, as a community, as a state. Blogs, Web 2.0 services have recently contributed to the increase of that capacity for everybody to participate fully to the democratic discussion within the public space of the Internet. Traditionally, the Internet has been viewed as the ideal forum for individuals to express themselves and to enter into contact with others and have access to their expression. **The recognition of Privacy has to be considered as a preliminary requirement for the exercise of the freedom of expression.** Would I dare to sign a petition in favour of a worthy cause if I know that tomorrow a powerful search engine would offer a potential employer, the means to stigmatise me for my standpoint?

Two other preliminary conditions for the freedom of expression have to be underlined:

- i. The first one refers to the ***right of each citizen to an education which renders him or her capable of expressing him or herself in cyberspace.*** Definitely this first condition refers to the values of solidarity and social justice which justify the various components of the universal service. Universal service²⁷ means not only a non discriminatory and accessible access to an infrastructure of quality including the development of “public access points” like libraries, schools and administration but also the right to be educated how to use Internet services, what we call the “computer

²⁶ The Working Party was established by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in short: the Data Protection Directive). Its tasks are laid down in Article 30 of Directive 95/46/EC and in article 15 of directive 2002/58/EC.

²⁷ Please note that the author is referring to universal service as a generic term, and not to the concept of USO as defined in the regulatory framework.

literacy". "Computer literacy" has to be understood broadly as asserted by the Council of Europe not only as the computational aspects of the use of internet services but overall as an critical and ethical education in the use of these new services by a better understanding of the societal impact of the Internet services.

This ethical education is even much more necessary given that with Web 2.0 applications, each of us might become tomorrow a publisher, an author and a data controller. **We plead for the spreading at all levels (at the levels of internet communities, ISPs and intermediaries) of ethical codes discussed as possible with the different stakeholders).**

- ii. The second condition for the effectiveness of our freedom of speech relates to the *ambiguous relationship between IPR and freedom of expression*. It is quite obvious that IPR regimes have been created for stimulating the creativity and for supporting the action of dissemination of ideas and opinions. By asserting that, we re-emphasize that copyright finds its ultimate justification in the freedom of expression recognized by Article 10 of the 1950 Council of Europe Convention. At the same time the copyright regime guarantees the possibility -in case of prevalent general public interest- to have access to the works and deny the possibility to transform the copyright into a "property right", through adequate technological measures (like Digital Rights Management Systems or tattooing) and ever-lasting contractual provisions.

These measures reinforced by their legal enactment²⁸ contribute to limit *a priori* the access to certain works including despite legal exceptions (DRM) or/and acknowledge the presence of the work in any of its fragment without any discussion about the subsistence of the conditions of the legal protection in all these fragments (Tattooing). They permit a reinforcement of the control of any reuse of each element of the work. And, in the same sense, the use of filtering and contractual provisions might be imposed without respect to the copyright regulation requirements. The chilling effect on creativity might be feared. **That is why we do recommend to analyze deeply the impact of all the new technical and contractual tools on the traditional balance enshrined in the copyright legislation. Furthermore, we do encourage states to provide an electronic universal access to economic, legal, social, cultural information held by the public sector like the Archives, the public libraries, the museums, etc. (as suggested by WSIS)²⁹.**

Network Neutrality: an emerging but crucial debate - The concept refers to a policy principle which implies a non discriminatory treatment as regards access to online content services. It means for networks' operators the prohibition of blocking or degrading, the

²⁸ See on that issue, the Geneva Declaration on the future of WIPO: "As an intergovernmental organization, however, WIPO embraced a culture of creating and expanding monopoly privileges, often without regard to consequences. The continuous expansion of these privileges and their enforcement mechanisms has led to grave social and economic costs, and has hampered and threatened other important systems of creativity and innovation. WIPO needs to enable its members to understand the real economic and social consequences of excessive intellectual property protections and the importance of striking a balance between the public domain and competition on the one hand and the realm of property rights on the other."

²⁹ This idea of a 'Public Domain Content' has been clearly promoted by the UNESCO. See, Point 15 of the 'Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace', adopted by the UNESCO General Conference at its 32nd session (Oct. 2003): 'Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.'

submission to unreasonable and discriminatory conditions and even the prioritisation between the online services providers providing similar service.

This principle prohibits any control of the data flow and imposes an equal treatment to each data flow. It meets the initial so-called “Internet end-to-end principle” which was enacted for ensuring a maximum efficiency of the transmission to minimize the cost of the network and in case of insufficient network capacities to impose the “first-come, first-served” rule. That rule creates problem while dealing with delay sensitive internet application such as notably Voice on the Internet services, streaming videos, etc.. Engineers have developed technologies which permit apart from now “traffic prioritisation” and thus solve the “Quality of Service” (QoS) problem raised by these “time sensitive applications”. At the same time, it introduces the possibility for a network operator to prioritise and shape traffic at the router level by automated recognition of the identities of the sender/receiver of a data flow and/or of its content. This can potentially lead to anticompetitive measures being taken by mobile or cable infrastructure operators such as blocking e.g. the VoIP³⁰ and peer to peer systems by giving priority to certain service providers affiliated to them. Beyond that, it introduces the possibility of a “two tier” Internet, an Internet with high performance and great capacities of transmission for certain information providers and/or rich customers and another one with degraded performance accessible to the others. **This possibility imposes certain legislative actions beyond the application of competition law in order to ensure the transparency of the usage and purposes of the technology of prioritisation and perhaps to ensure that all internet users are provided a minimum quality of services what implies a re-evaluation of the Universal Service³¹.**

Minimal regulation for content - Freedom of expression, off line and online is a basic inalienable right of the citizens. If certain limitations are provided for by the text which enunciates these principles, we must resist to the temptation of regulating *a priori* the freedom of expression on the Internet. The temptation is great since certain recent events attempt the governments to justify interference by public authorities. The technology might help by creating solutions which were not possible in the offline world, notably by screening all messages in order to detect expressions or images considered as shocking, offending or disturbing. On that point, one have to recall the practice of the European Court of Human Rights (ECHR) which asserts that the democratic debate imposes the existence of a variety of opinions even if they might be considered as offending or disturbing people. We must learn to live with that risk and to concentrate our efforts only on certain precise regulations focussing on manifestly illicit (e.g. racism or pedo-pornography) or seriously harmful contents and trust the powers of freedom of expression reinforced by the Internet and its capacity to allow each citizen to react, discuss, and protest against certain practices or content. In our opinion, more speech might be the best way to solve the problem instead of developing filters, blocking measures or sanctions.

In that context, an ‘open’ and transparent self-regulation (versus the confiscation by certain intermediaries of this self-regulation) conceived as the participation of all stakeholders in the regulation of the content on the Internet is an appropriate way to maintain the Internet as a public discussion place and forum to acceptable limits. The next point is precisely dedicated to this issue.

³⁰ As it was decided in the US Madison River and Comcast Corporation cases (about these case and more generally on the “Network neutrality” debate, read, P.Vaelcke, “Network Neutrality: legal Answers from a EU Perspective”, *RDTI*, Sept.2008, p. 323 and ff.

³¹ See the OECD report, « Internet Traffic Prioritization: An Overview », Note by TIPS, (2007), DSTI/ICCP/TIPS(2006).

The “Death of Public Forum in Cyberspace”³² - The horizontal effect of the 1950’ European Convention of Human Rights imposes that the same freedom of expression principle and its limits are available also towards the intermediaries like search engines and Web 2.0 platforms. **Since they are becoming the private gatekeepers of the public discussion space, it is important that their policies as regards the control of the Internet content would be clear and transparent to the public.** Until now, these policies are quite unclear. The fear of an “over-censorship” by these private authorities calls for a control over their practice. Otherwise, as stated by Nunziante, the Internet will become transformed by this privatization of the public space “*into a collection of largely privately owned and privately regulated places*” without judiciary control. My opinion is that the countries have a positive duty to impose the respect of the freedom of expression to all actors and to recreate public places (i.e. public forums in cyberspace).

That assertion does not contradict with the self-regulatory or co-regulatory measures like quality labels, moderators’ intervention, rating systems, put into place by communities or information providers services themselves. These initiatives might be interesting to promote the confidence and awareness of the ethical aspects of what must be our behaviour on the Internet. As already said, instead of punishing and sanctioning, it would be better to achieve the same goal by education and through codes of ethics discussed or clearly accepted and by developing ways and tools for Internet users and Information services providers to internalize norms and values.

New editors, new journalists - With the new world of Internet, the concept of press has to be reassessed. Not only because the actors are no more linked to specific countries but are active throughout the world or a large part of the world but also because everywhere new actors are now contributing to the formation of the public opinion without having all the elements of the definition. For instance, can we consider that Google News with selecting press articles has to be qualified as a press institution? You Tube is diffusing opinions, records about what has happened around the world but its activity might not easily be considered as the one of an editor even if there is a certain selection of information and images and definitively a classification of them. The traditional press sector develops also new services online such as forums of discussion and journalist’s blogs which sometimes are clearly outside the control of the editorial board.

The role of search engine has to be assessed in the same context. To what extent is democracy concerned by their activities? Even if we certainly agree that search engines provide a major input to the democratic debate thanks to the possibility given to everyone to retrieve and access, from any country - including not only developed countries - all adequate information on a topic, we, nevertheless, would like to put into question this progress. The equity of chance to exist and to be consulted on the WEB scene is far from being obvious when we do consider the “link popularity” metric applied in most of the engines. The lack of transparency thus is the major issue raised in this context. Most of the users do ignore how the ranking is done and often consider it as the true response and vision of the world of their queries.

Even if it is normal that the logics governing the functioning of the search engine are greatly dictated by economic and efficiency concerns, it remains that the method of selection has to be clear to everybody and might not be operated in an unfair way for ideological, anticompetitive or other reasons.

³² D. Nunziante, “The Death of the Public Forum in Cyberspace”, *Berkeley Technology Law Journal*, 2005, p. 1115 and ff.

As regards the actors implied in Web 2.0 services, everybody might become journalist, commenting through his or her blog the day to day events and his or her website can have a strong audience comparable to that of the newspapers. The concept of a journalist is not defined but it is commonly considered that his or her activity is to disseminate through the editors his or her independent opinion on events which are of public importance and due to their important contribution to the formation of the public opinion, are submitted to a deontology which ensures the public's confidence (duty to check the sources, duty to limit him or herself to the information published to what is needed for the formation of the public opinion, etc.). The respect of these obligations is, ensured by self-regulatory rules and organized by the peers themselves. To what extent this deontology might be applicable to citizens publishing their own opinions normally directed to a restricted public?

How to ensure the cultural diversity in a global environment? - Having asserted the absolute priority of the freedom of expression, EU has to recognize that certain values might be considered in a certain country differently than in the EU for religious, cultural or societal reasons. Nudity is accepted in some countries but is rejected and considered a threat to public morality in other. The French Yahoo case³³ concerning racist content illustrates the difference of approaches between US and EU as regards the prohibition of this kind of content. The adoption in 2005 of the UNESCO Convention on the diversity of cultural expression³⁴ is a clear recognition of this plurality of national perceptions of public order and moral. The abolition of physical frontiers in the context of the Internet might create difficulties for the countries to enforce in the context of the Internet their own perceptions of what might remain an attribute of their national sovereignty. This sovereignty is however recognized even by WTO Conventions since article XIV a) of the GATS permits a country to go against their market access commitments if taking measures is “necessary to protect public morals or to maintain public order”. The conciliation of public national sovereignty on one hand and of the global character of the Internet on the other hand is not easy to solve. On basis of the famous ANTIGUA vs. US case³⁵ about online gambling services, Rundle³⁶ observes that this kind of debate might not be correctly solved in the context of WTO, only on the basis of a balance between trade interests and public interests.

Another solution must be found at the international level in order to conciliate the freedom of expression principle and the right of each sovereign State to limit this fundamental liberty for prevalent public or general interest reasons. Perhaps an International Court of Justice created under the auspices of the UNESCO might be the appropriate solution. It implies the necessity that the infrastructure design gives the possibility for each nation to enforce the decision taken which might be difficult if the Internet configuration does not permit this enforcement. That refers to the delicate problem of the State sovereignty on the Net, a question we will address in our final statements.

³³ The first Court decision has been pronounced in 2000 by the Tribunal de Grande Instance de Paris, (decision available at:<http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm> with a lot of comments). This decision has been followed by numerous decisions in contradictory senses both in US and in France.

³⁴ Convention on protection and promotion of the diversity of cultural expression, adopted by the UNESCO General Assembly, Paris, 20 October 2005.

³⁵ WTO, Appellate Body Report, Measures Affecting the Cross-Border Supplies of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005, see www.wto.org/english/tratop_e/dispu_e/285arb_13_e.doc. On that issue, read, M.V. Perez Asinari, “Internet Gambling and betting services: When the GATS’ rules are not applied due to morals/public order exception. What lessons can be learnt?”, CL&SR, 2006, 1 and ff.

³⁶ M. Rundle, “Beyond Internet Governance: the emerging International Framework for Governing the Networked World”, Research Publication N° 2005-16, Fall 2005, <http://cyber.law.harvard.edu/publications>.

3. FINAL STATEMENTS

3.1 ICT challenging or enhancing liberties? Towards a value sensitive design of the technologies

Technology is the risk, it might also be the solution - ICTs are a tool, more precisely a “social construct” since their design and use are not predetermined but contains enshrined logic and pursued by their users. If technology certainly offers to them new opportunities and means to realize their goals, it is quite obvious that choices are still possible. We should never forget that if technology creates the risk in the same time it might bring solutions. In short, the technology can make a contribution to humanity just as it can put in peril the liberties of citizens. As already quoted, the Article 29 Working Party on Data Protection and RFID noted, under the basis of the Data Protection Directive preamble: “*Technology must be at the service of the human being, his or her freedom and dignity*”.

It implies that from a very early stage, the research laboratories, the information system producers and the public or private standardization bodies have to take into account these concerns and follow a “human values sensitive design”. That means an enhanced integration of ‘moral and legal values’ from the very starting stage of technological design. In order to ensure this integration a societal assessment should be initiated both at the level of research laboratories and definitively at the level of standardisation bodies’. It presupposes that computer scientists would be more aware of the legal and societal environment and impact of their findings and that public discussion might be organized at different levels. **Correlatively, Terminal equipments’ producers and Information Systems designers will have to support liability in cases where their products or services permit their users to infringe Human Rights legislation.** In conclusion, it is at the roots of the Technology where we should find the solutions to the risks created by the use of that Technology.

3.2 Crucial role of the state

The role of the state in enforcing human liberties - According to the jurisprudence of the ECHR the state is not merely under the obligation to abstain from interfering with individuals’ privacy, but also to provide individuals with the material conditions needed to allow them to effectively implement their right to private and family life.³⁷

In other words, according to the theories of the “positive duties” of the state combined with that of the “horizontal effect” of the EHCR, states are under the obligation to take all appropriate measures to protect the fundamental rights of the individuals including against their infringement by other non-state parties. Our duty as European states is not limited to the defence of the fundamental liberties within the European Union but also implies a commitment to ensure that this protection will be ensured at a global level. As regards Privacy protection, the Council of Europe Convention N°108³⁸ might be considered as the necessary global privacy regulatory framework since it is opened to signature by third countries and is offering a minimal common and acceptable basis for all countries.

The need for a global dialog founded on certain basic ethical values - Zoning the Net³⁹ according to citizenship might seem at first glance a sensible way to maintain the modern

³⁷ The positive duty of the State to provide the means necessary in order to allow effective enjoyment of rights is not as such recognised in the United States, neither by the law, nor by the jurisprudence.

³⁸ Council of Europe Convention of the protection of individuals with regards to the automatic processing of personal data N°108.

³⁹ On the possible temptation of certain States to come back to a zoning of the Net, through the technical design of the infrastructure and definitively through the intervention of intermediaries like Internet access providers or

world's citizenship lines. However, such a practice will encounter problems, not the least of which will be citizens' dissatisfaction with differential treatment based on nationality. As in other areas of governance, a global approach is needed. It requires that each country seriously takes into account the various cultural approaches existing throughout the world, the refusal to impose on the others nations a unilateral view as regards the public order. **A regulatory framework based on human Rights implies a commitment to enter into a dialog founded on a mutual recognition of the cultural differences and on some ethical common values revealed in international documents (especially the UNESCO Convention on protection and promotion of the diversity of cultural expression and the UNESCO Declaration on Bioethics and Human Rights⁴⁰) and universally accepted. These common values could be enumerated as follows: 1) person's dignity and autonomy; 2) solidarity between men and peoples and social justices; 3) need for beneficent technologies and prevention of their damaging effects.**

If this dialog does not happen, one might fear that the internet will become a Tower of Babel where fear and hate of the others' speech will be the sad result and will have as a result the loss of this unique and unedited chance of cultural, intellectual, political and human enrichment of the global society.

The need for a societal assessment - Beyond that, it is the role of the state and thus of Your Parliament to require as it has been recommended by the Commission on the particular case of RFID⁴¹ that **societal assessment should be initiated with the participation of all stakeholders, empowering what we might call the "ordinary" voices, such as representatives of all groups of society in particular the vulnerable ones, but also civil liberties associations, trade union representatives or consumer groups. Perhaps a permanent working group, a sort of observatory, has to be set up at least at European level. Its role would be multiple: to give advice and recommendations to the European Institutions at their demand or on its own initiative, collect information and disseminate good practices, organize the public debate about the technological evolution and their societal impact.**

The application of the precautionary principle, that implies the duty of the society to impose a certain assessment before to decide the exploitation of an innovation, as well as the shared responsibility of the producers of technology given the risks created, principles clearly asserted in the environmental law, has to be applied as regards the ICT technology. The principles of transparency and deliberation ("multi-stakeholderism") affirmed notably by the Aarhus Convention⁴², will henceforth find an echo. This will enhance the active role of the citizens and their participation on the Internet.

The role of citizens: from adrift to active participation – In its UNESCO report on the Network Governance, Rundle speaks about the citizen's adrift⁴³ as the major problem of the

payment systems , read J. Reidenberg, "States and Internet Enforcement, 1 *Univ. of Ottawa Law and Techn. Journal*, Vol. 1, N° 213, 2004.

⁴⁰ Adopted by acclamation on October 2005 by the 33rd session of the General Conference of UNESCO.

⁴¹ See Commission Communication of March 15, 2007 on 'radio frequency identification (RFID) in Europe': Steps towards a policy framework', COM(2007)96 and the Study commissioned by the European Parliament, STOA on 'RFID and identity management in everyday life, June 2007.

⁴² The UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, usually known as the Aarhus Convention, was signed on June 25, 1998 in the Danish city of Aarhus. It entered into force on 30 October 2001.

⁴³ "As the above account tells, governments have responded quickly to meet challenges in cyberspace: They have set certain parameters for people's online dealings. They have kept the doors open for e-commerce. They have let an international trade court review national rules on Net content. They have pooled resources for infrastructure development. They have set up cybersecurity arrangements. They have even cooperated to

future Information Society. Technological evolution is far beyond their ability to understand. Definitely that evolution brings many advantages and might lead to a new democracy where everybody might learn from the others, confront his or her ideas and therefore might participate more actively to the “vouloir vivre ensemble”. But in order to be realised, this promise presupposes that citizens should be seen not as simple consumers of services, manipulated to an extent never reached. For ensuring this citizens’ master ship of the technological environment, privacy regulation aiming to ensure the preservation of the autonomy of the individuals is definitively the main concern.

That recognition and even - as already proposed - enhancement of our privacy regulation is not sufficient. The public voice must be heard. It refers not only to the societal debates which have to be organised at all levels including at the global level but also to the free debates the citizens must open and promote by discussing all the possibilities offered by the technology. We underline the importance of the citizens’ networks supported or not by civil associations in order to defend alternative ways to develop the Internet. “Creative Commons”, “Open Net movements”⁴⁴ are examples but many others examples developed by “peers to peers” networks might be quoted in the context of the use of Internet services, taking fully into account the benefits of the technological tools at their disposal.

In order to promote participation, citizens’ education is a major issue, particularly as regards their awareness of the ethical issues and of the liability implied by their participation in the Information Society. That education is definitively needed at a moment where we are full actors on the Internet through the web 2.0 services. Internet increases tenfold the power of individuals who in a targeted or a dispersed way, in a conscious or unconscious manner, can with a simple message posted on the Internet destroy the reputation of the others, transmit a virus, send or receive pedo-pornographic contents and thus encouraging the enslavement of human beings. The Internet gives to our actions without a particular effort on our part a “global impact” which prompts us to question individual and collective responsibility. Perhaps this individual and collective commitment to play a critical and active role in the design and choices of our Information society constitutes a chance for our democracies.

safeguard the financial stability of the networked world. However, in letting the framework for Net governance evolve in an ad hoc way, policymakers have focused on surface problems, at the expense of deeper, more fundamental questions of democracy. Sooner or later, the networked world must confront an issue facing all societies: that is, the relationship between the state and its citizens. » (M. Rundle, “Beyond Internet Governance: The Emerging International Framework for Governing the Networked World”, Center for Internet and Society at Stanford Law School, Research Publication No. 2005-16, Fall 2005).

⁴⁴ The **OpenNet Initiative** is a joint project whose goal is to monitor and report on internet filtering and surveillance practices by nations. The project employs a number of technical means, as well as an international network of investigators, to determine the extent and nature of government-run internet filtering programs. Participating academic institutions include the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard Law School; the Oxford Internet Institute (OII) at University of Oxford and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge, (Wikipedia Encyclopedia).

BIBLIOGRAPHY

- Barrow, E (1996) Barrow, E (1996) "Rights clearance and technical protection in electronic environment", February 1996.
- Brownsword R. (2008) Brownsword, R., 'Knowing Me, Knowing You—Profiling, Privacy and the Public Interest' in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen*, Dordrecht, Springer, 2008, pp. 362-382.
- Burkert H. (2008) Burkert, H., "Dualities of Privacy -An Introduction to 'Personal Data Protection and Fundamental Rights'", in *Privacy- New visions*, M.V. Perez, A. Palazzi (eds), Cahier du Crid, to be published in 2008.
- Council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS, N°108, Strasbourg, 28 January 1981.
- Culnan M.J. (2000) Culnan, M.J., "Protecting Privacy online: Is self-regulation working?", 19 *Journal of Public Policy Market*, 2000, 1, pp. 20 and ff.
- Council of Europe 1950 Convention on Human Rights Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome, 4.XI.1950, ETS No 005 and protocol ETS No. 155.
- Council of Europe Convention N°108 Council of Europe Convention of the protection of individuals with regards to the automatic processing of personal data N°108, ETS N°108.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L* 281, 23 November 1995.
- Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.
- ETAG European Technology Assessment Group, Study commissioned by STOA for the European Parliament on "RFID and identity management in everyday life", June 2007.
- European Commission Communication of March 15, 2007 on 'radio frequency identification (RFID) in Europe': Steps towards a policy framework', COM(2007)96
- Geneva Declaration Declaration on the future of WIPO <http://www.cptech.org/ip/wipo/futureofwipodeclaration.pdf>
- Hustinx, Peter Data Protection Supervisor, letter to Minister of Justice Alberto Costa and Minister of State and Internal Administration Antonio Costa, "Presidency work programme and the protection of individuals with regards to the processing of personal data and the free movement of such data", 11 June 2007, see http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf
- Lessig L. (1999) Lessig, L., "Code and other Laws in Cyberspac", New York, Basic Books, 1999.
- Nissenbaum H. (1998) Nissenbaum, H., "Protecting Privacy in an Information Age: the Problem of Privacy in Public.Spaces", 17 *Law and Phil.*, 1998, pp. 576.
- Nunziante D. (2005) Nunziante, D., "The Death of the Public Forum in Cyberspace", *Berkeley Technology Law Journal*, 2005, p. 1115 and ff.
- OECD report (2007), "Internet Traffic Prioritization: An Overview", Note by TIPS, (2007), DSTI/ICCP/TIPS(2006).
- Perez Asinari MV. (2006) Perez Asinari, M.V., "Internet Gambling and betting services: When the GATS' rules are not applied due to morals/public order exception. What lessons can be learnt?", CL&SR, 2006, 1 and ff.
- Reidenberg J. (2004) Reidenberg, J., "States and Internet Enforcement, 1 Univ. of Ottawa Law and Techn. Journal, Vol. 1, n° 213, 2004.

Rodota S. (2008) Rodota, S., "Data Protection as fundamental Right", in *Reinventing Data Protection*, S. Gutwirth et alii, Springer Verlag, 2008 (to be published)

Rundle M. (2005) Rundle, M., "Beyond Internet Governance: the emerging International Framework for Governing the Networked World", Research Publication n°2005-16, Fall 2005 available at: <http://cyber.law.harvard.edu/publications>.

Rouvroy A. et al (2007) Rouvroy, A., and Poullet, Y., "Introductory Remarks, General report, European Conference on Ethics and human rights in a Information Society organized by UNESCO and Council of Europe", Strasbourg, 13-14 Sept., 2007 available at the UNESCO website.

Rouvroy A. et al (2008) Rouvroy, A., Poullet, Y., The right to informational self-determination and the value of self-development - Reassessing the importance of privacy for democracy, in *Reinventing Data Protection* Gutwirth, S., Poullet, Y, De Hert, P., de Terwangne, C., Koops, B.J., (ed.), Springer Verlag, 2008, to be published.

Rouvroy A. (X) Rouvroy, A., "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", *Studies in Law, Ethics and Technology* (forthcoming).

Sunstein R. (2003) Sunstein, R., *Why Societies Need Dissent*, Harvard University Press, 2003, pp. 157-158.

Solove D.J. (2002) Solove, D.J., "Conceptualizing Privacy", 90 *California Law Review*, 2002, 1085 and ff.

UNECE Convention (Aarhus Convention) The UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, signed on June 25, 1998, Aarhus. Entered into force on 30 October 2001.

UNESCO Convention UNESCO Convention on protection and promotion of the diversity of cultural expression, adopted by the UNESCO General Assembly, Paris, 20 October 2005.

UNESCO Declaration Declaration on Bioethics and Human Rights, Adopted by acclamation on October 2005 by the 33rd session of the General Conference of UNESCO.

UNESCO Recom. "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace", adopted by the UNESCO General Conference at its 32nd session (Oct. 2003).

Vaelcke P. (2008) Vaelcke, P., "Network Neutrality: legal Answers from a EU Perspective", *RDTI*, Sept.2008, p. 323 and ff.

WTO WTO, Appellate Body Report, Measures Affecting the Cross-Border Supplies of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005.