IFIP

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING

Ethics and the Governance of the Internet

To Promote Discussion
Inside the IFIP National Societies

Jacques BERLEUR, Penny DUQUENOY and Diane WHITEHOUSE, Eds.

IFIP-SIG9.2.2
IFIP Framework for Ethics of Computing
September 1999

ISBN 3-901882-03-0
Event number 1303

This brochure may also be found on the SIG9.2.2 website:
http://www.info.fundp.ac.be/~jbl/IFIP/cadresIFIP.html
by clicking on SIG9.2.2 "Ethics and Internet Governance"

IFIP

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING

Ethics and the Governance of the Internet

To Promote Discussion
Inside the IFIP National Societies

Jacques BERLEUR, Penny DUQUENOY and Diane WHITEHOUSE, Eds.

IFIP-SIG9.2.2
IFIP Framework for Ethics of Computing
September 1999

Contents

IFIP

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING

Date: September 8th, 1999

Address reply to:
Jacques BERLEUR
IFIP-SIG9.2.2 Chair
Institut d'Informatique
Facultés Univ. N-D de la Paix
Rue Grandgagnage, 21
B. 5000 NAMUR (Belgium)
Email : jberleur@info.fundp.ac.be

To: IFIP Members
Subject: Ethics and the Governance of the Internet

Dear Colleagues,

You probably remember that IFIP Technical and General Assemblies created, at the 1994 Hamburg meetings, a Special Interest Group on Ethics. It was the follow up of the survey we conducted on the Codes of Ethics and Conduct of our different Member Societies (see pp. 21-22).

By our letter dated May 8, 1998, we again contacted you to update our information about our ethical concerns inside IFIP.

Today we have prepared a new brochure that we hope could inspire our common reflection. It is the result of our work during the last two years, and of the discussions during the IFIP-TC9 HCC-5 (Human Choice and Computers) International Conference in August 1998.

May we draw your attention to some specific questions on which we would be happy to have your participation:

- **SIG9.2.2 Recommendations, pp. 16-17**
- **Questions Raised to the IFIP Members, pp. 17-18**
- **Summary of Resolutions, pp. 25-26**

This brochure may also be found on the SIG9.2.2 website, by clicking on SIG9.2.2 "Ethics and Internet Governance": http://www.info.fundp.ac.be/~jbl/IFIP/cadresIFIP.html

Many thanks for your attention and consideration.
Yours sincerely

On behalf of SIG9.2.2
IFIP Framework for Ethics of Computing

Jacques BERLEUR
IFIP-SIG9.2.2 Chair & IFIP-TC9 Chair

SIG9.2.2 Members

Barroso Asenjo Porfirio, Spain
Berleur Jacques, Belgium - Chair
Cameron Julie, Australia
Dolezal Jaroslav, Czech Republic
d'Udekem-Gevers Marie, Belgium
Duquenoy Penny, UK
Duncan Karen, USA
Enslow Philip H. Jr., USA
Gotterbarn Don, USA
Gritzalis Dimitris, Greece
Holvast Jan, The Netherlands
Jones Matt, UK
Kizza Joseph M., USA
Laopodis Vassilios, Greece
Lee John A.N., USA
Martin C. Dianne, USA
Masduki Mohd. Salleh, Malaysia
Morris Andrew, South Africa
Rödiger Karl-Heinz, Germany
Sizer T.R.H., UK
Thimbleby Harold, UK
Van Dijk Arjan A., The Netherlands
Weckert John, Australian Rep,
Wenngren Gunnar, Sweden
Whiley Jean, Zibabwe
Whitehouse Diane, UK

List of Representatives

Australia, ACS: John Weckert
CEPIS: Van Dijk Arjan A
Czech Republic, CSCI: Jaroslav Dolezal (Provisional)
Greece, GCS: Vassilios Laopodis
ICCC: Philip Enslow
Malaysia, MNCC: Mohd. Salleh Masduki (Provisional)
The Netherlands, NGI: Arjan.A.Vandijk
United Kingdom, BCS: Dick Sizer
Zimbabwe, CZS: Jean Whiley
Sweden, SIPIS: Gunnar Wenngren

Ethics and the Governance of the Internet
Introduction and Recommendations of IFIP-SIG9.2.2

Jacques Berleur
IFIP-SIG9.2.2 Chair
IFIP Framework for Ethics of Computing
Email: jberleur@info.fundp.ac.be

This introductory paper is intended as an overview of the current debates surrounding use of the Internet and regulation of the communications possibilities that the net offers. The paper lists a number of topics that have an ethical content, and highlights some issues that are coming to the fore in the debate. Finally, it makes a series of three recommendations to the member societies of the International Federation for Information Processing (IFIP), urging those members to take these suggestions on board. It also encourages IFIP member societies to answer ten very specific questions about the work that they may be doing in the area of ethics and the Internet.

"Internet Governance"?

Lists of websites may quickly leave the impression that the words "Internet governance" are linked today to the environment of domain name administration. Search engines readily refer to the homepages of IANA (Internet Assigned Names Authority), its substitute ICANN (The Internet Corporation for Assigned Names and Numbers), or the new IANA Corporation (Internet Addressing and Naming Authority).[1]

But when the CPSR (Computer Professionals for Social Responsibility) launched its “One Planet, One Net: CPSR Campaign on Internet Governance” in December 1997, it was "undertaking a broader examination of the issues in standards development, content development and control, and access to the Internet." "The Principles for the Internet Era" cover a wider area than simply domain names and addresses. They are principles intended "to counter the political, economic, social, and technical forces that (...) threaten the promise of open communication on the Internet."[2]

The European Commission’s Information Society Project Office (ISPO) presents on its homepage the project of Internet Governance, and seems to come back to a narrower understanding. It mentions:

---

[1] See http://www.iana.org and http://www.icann.org For the discussion with the European authorities, see for instance: Internet Governance, Reply of the European Community and its Member States to the US Green Paper http://www.ispo.cec.be/eif/policy/govreply.html

[2] The 1997 text of CPSR is reprinted in Annex 3 of the P. Duquenoy and D. Whitehouse paper, in this brochure. It may be found with other documents of the CPSR campaign at: http://www.cpsr.org/program/nii/onenet.html The question "Why Internet Governance?" is treated again in the Spring 1998 issue of the *CPSR Newsletter*.

- Management of Internet Names and Addresses,
- International policy issues related to Internet Governance,
- Internet Governance reply of the EC and its Member States to the US Green Paper, and
- Domain Names.[3]

We adopt a more open position than the European Commission, considering the currently predominant DNS (Domain Naming System) question as just one example of a larger debate among different interested parties such as technical organisations, businesses or groups of businesses, higher education institutions, and governments. The current debate between the USA and Europe also points to controversies over control of the Internet.[4] Everybody knows the issues at stake regarding Internet self-regulation, or in other words, the place of official governments and national or international authorities in ruling cyberspace, democracy on the Internet, its multi-culturality, the place of the developing countries in the universal service, etc.[5] We think that all these kinds of questions fall under the scope of "Internet governance".

As it will appear in the report on the rolling workshops and the round table held during IFIP-TC9 HCC-5 Conference, our approach has been inspired by a paper of Joel Reidenberg and suggests a three-way Internet governance: technical, self-regulating and legal.[6]

Do We Need Internet Governance?

The Internet has grown for a long time without too much regulation. Defining protocols and standards had been for a long time the most developed regulatory activity. But as soon as business took its place, the requirements changed. People present at the closing session of the IFIP-WCC'94 in Hamburg surely remember those who spoke about creating a "second Internet" dedicated to business, if safer measures were not to be taken. Standards and routing administration, encryption, digital signature, Internet service providers licensing, property rights, tariffs, computer crime, etc. were questions raised as soon as commerce came to the forefront.[7]

---

3 http://www.ispo.cec.be

4 Communication of the European Commission to the Council, International Policy Issues Related to Internet Governance, 20 February 1998, http://www.ispo.cec.be/eif/policy/governance.html

5 One may be interested in consulting the categories of the "Quicklinks" of the European Legal Advisory Board to have an idea of the current topics in debate on 'Legal and *regulatory aspects of Internet* and the information society': Access to public sector information / IT in government, Competition, Computer crime, Consumer protection, Content regulation, Convergence of telecommunications, media and information technology, Copyright, trademarks and patents, Data Protection (privacy), Digital signatures, Domain names, Electronic commerce, Electronic democracy, Employment and social issues, Euro and millennium bug, Information society and Internet policy, Interception, Internet access and use, IT in education, Junk mail (Spam), Liability, jurisdiction and applicable law, Multilingual content and software, Multimedia content and tools, Protection of minors, Quality of service, Rating and filtering, Security and encryption, Self-regulation / codes of conduct, Standards, Taxation and tariffs, Universal service ('Links to news items about legal and regulatory aspects of Internet and the information society, particularly those relating to information content, and market and technology', edited by Richard Swetenham, EC, DGXIII, http://www.qlinks.net

6 Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 *Emory Law Journal*, 911 (1996), reprinted in: *Borders in Cyberspace*, Brian Kahin and Charles Nesson, eds., MIT Press, 1997.

7 A list of some twenty issues is given on the "Issues" page of the European Electronic Commerce Initiative, http://www.ispo.cec.be/ecommerce/issues.htm

In particular, the management of Internet names and addresses is considered as critical to the stability and inter-operability of the Internet. The allocation of domain names is of utmost significance for the organisations concerned, users and trademark owners.

The debate is now lively because the key issue is "What kind of regulation?" Rules by governments or self-regulation by business and users? Because of its history, some highly sensitive features surround the concept of governance of the Internet. The Blue Ribbon Campaign and similar anti-censorship manifestations hark back to the origins, when the Internet was mainly a tool for research and education, i.e., operating according to the principle of 'academic freedom.'

Is more regulation needed? Those who advocate more regulation feel that the Internet today is chaotic and unmanaged and also weakly self-regulated. Examples were given during the HCC-5 session devoted to self-regulation. New associations created in the meantime do not alter these views. Most of the "codes" are created "to curb government regulation of the Internet" - it is even sometimes proclaimed as such. Here are some recent private initiatives:

- the Global Business Dialogue on Electronic Commerce: an initiative of top executives "to prevent conflicting governmental regulations from obstructing business in cyberspace."[8]
- the Electronic Commerce Platform Netherlands (ECP-NL): a platform coordinating initiatives in electronic commerce that has drafted a code of conduct, currently submitted for comments to "all interested parties," and proposed for discussion at both the OECD level and at a conference to be held in the Netherlands in the presence of US Commerce Secretary William M. Daley.[9]
- Electronic Commerce Europe, which considers that codes of conduct are the structuring approach to Electronic Commerce.[10]
- the ICRA (Internet Content Rating Association)[11]: the Bertelsmann Foundation is organising (Munich, September 9-11, 1999) a "summit" (sic) on "Self-regulation of the Internet Content". "The Internet Content Summit is the first milestone in the implementation of an international self-regulatory system to deal with the protection of minors online. The conference is organised and funded by the Bertelsmann Foundation in cooperation with INCORE (Internet Content Rating for Europe)."

One may wonder if such declarations or codes of conduct are not purely instrumental, i.e., aimed at making e-commerce or any use of the Internet or ICT systems more acceptable to the public. Undoubtedly, commerce is -- and always has been -- the big affair of mankind. It mobilises all the devices of creativity, including the newest technology. The sometimes hidden intention is to create a free-trade global market without customs, tax systems, and rules from the State.[12] The question is to legitimate the operation: rhetoric and metaphors may help!

---

8 Amy Harmon, Titans race to do the policing for the electronic roadway, *New York Times*, Jan. 18, 1999, http://www.gbd.org/library/newyorktimes.htm

9 Code of Conduct for Electronic Commerce, Draft version 2.0, July 1999, http://www.ecp.nl/

10 http://www.e-betobe.com/code/code.html

11 The founding companies of ICRA include AOL Europe, Bertelsmann Foundation, British Telecommunications plc (BT), Cable & Wireless, Demon Internet (UK), EuroISPA, IBM, Internet Watch Foundation, Microsoft, Software & Information Industry Association, and T-Online Germany. http://www.stiftung.bertelsmann.de/internetcontent/english/frameset_home.htm

12 Bernard Cassen, Adieu au rêve libertaire d'Internet, in: *Révolution dans la Communication, Manière de voir, Le Monde Diplomatique*, n° 46, Juillet-Août 1999, pp. 94-95.

About the codes -- let us repeat -- where is the power of sanction?[13] Are there any enforcement means? People know how sensitive these questions are. The "ICRA Summit" has prepared a long document about this specific question of "law enforcement".[14] But as far as we can see, associations where every individual member has to commit him/herself to abide by the code seem very rare!

In a way, SIG9.2.2 regards the opposition between private and public regulation as something to be overcome, and recommends a deeper cooperation of both sectors in the domain of governance. Controversial questions such as the relationship between self-regulation and the law must be confronted. The actual *credo* of a "socio-liberal third way" could lead to "disappropriation from the State."[15] Others speak about a "Governance Debacle," buried by politics.[16] Some suggest a distinction between "governance" and "institutional framework," and promote the latter.[17] Self-regulation with conditions, or embedded in an appropriate legal framework, could be satisfactory. The pending dialogue between the USA and Europe about the transfer of personal data to third countries and the interpretation of articles 25 and 26 of the European Directive on the protection of individuals with regard to the processing of personal data will be a very interesting case study on "self-regulation and/or the law" when it is resolved. The Directive mentions the necessity of examining the "appropriate level of protection" of the parties, whereas the USA speaks about self-defined "safe harbour principles."[18]

Do We Need Internet Ethical Governance?

If we need Internet governance, the question may be raised: "Do we need ethical governance?" And therefore also: "What does it mean?"

There is no need to dwell on it, since the IFIP Ethics Handbook has already elaborated this issue. Jan Holvast reminds us that Julie Cameron et al. state it very simply: "We need IT ethics because:

- IT is a powerful and constantly evolving tool,
- IT permeates all aspects of our lives,
- IT dependency creates vulnerability on a large scale,
- IT evolution and usage outstrips the formulation and implementation of policy and legal instruments.'[19]

---

[13] See, f.i., J. Berleur and M. d'Udekem-Gevers, Codes of Conduct within IFIP and other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., A Handbook prepared by the IFIP Ethics Task Group, London: Chapman & Hall, 1996, pp. 7ff.

[14] Prof. Dr. Ulrich Sieber, University of Würzburg, Law Enforcement, 112 p. (downloadable from the site of the Bertelsmann Stiftung)

[15] Riccardo Petrella, La désappropriation de l'Etat, in: *Le Monde Diplomatique*, Août 1999, p. 3.

[16] Milton Mueller, The "Governance" Debacle: How the Ideal of Internetworking Got Buried by Politics, INET'98 Proceedings, http://www.isoc.org/inet98/proceedings/5a/5a_1.htm

[17] ibid.

[18] Department of Commerce, Elements of Effective Self Regulation for the Protection of Privacy and Questions related to Online Privacy, (http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm) Data Protection Working Party Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, DGXV D/5025/98 - WP12, 24 July 1998, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

[19] Julie Cameron et al. (1992), Ethics, Vulnerability and Information Technology. op. cit., p. 344. Quoted by Jan Holvast, Discussion paper, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, op. cit., p. 47.

We ourselves have welcomed "a revival of ethics" stressing the re-appropriation of our daily life in the field of ethics, a kind of "life-world ethics" ("le monde-vécu"), in the sense of Jürgen Habermas.[20]

There has been a relatively easy consensus that ethics is necessary on the net when speaking about protection of minors and human dignity. The "Action plan on promoting safer use of the Internet" is part of a coherent set of policies at the European Union level to deal with illegal and harmful content on the Internet.[21] Other international organisations such as UNESCO have also developed actions to meet this general preoccupation. But this is probably the emerging part of the iceberg.

There are also other topics that could similarly be considered as urgent ethical issues which require our attention and determine our priorities. However, this may depend upon different factors such as the culture, the place where we are living and acting, the practices at work, the motivation of people, the interests at stake, etc. SIG9.2.2 proposal is a first exercise whose result we present here. We have classified the different topics into two categories, the first one into two sub-categories. So, the first sub-category deals with issues related to the protection of the individual (citizen and consumer). The second, with more collective issues or with the organisation of society. The last category is dedicated to topics which we feel have a more ethical content: this is why we have not only listed them, but have also given a short explanation.

We must finally add that, in our opinion, the distinction between ethical and social issues is not always quite clear today; one cultural environment may call ethics what is considered 'social informatics' in another.[22] There is at least one trap we should not fall into: the distinction between ethical and social must not be considered as parallel to that between individual and collective. We leave that distinction between ethical and social issues open, and refer to the current literature.

SIG9.2.2 Proposal of Topics to be Considered

We propose ongoing discussions within the IFIP Members Societies about the subjects that follow. SIG9.2.2 also has various recommendations to make, and these then follow also.

Topics Already Under Discussion

Protection of the individual (citizen and consumer)

- questions related to risk, security, reliability, vulnerability, liability, ... (for instance in e-commerce),

---

[20] J. Berleur and M. d'Udekem-Gevers, Codes of Conduct within IFIP and other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, op. cit., p. 13, and J. Berleur, Ethics, Self-regulation and Democracy, *ibid*., pp. 241-256.

[21] European Parliament and Council, Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, http://www2.echo.lu/legal/en/iap/index.html

[22] See f.i. H. Tavani, 'The Tavani Bibliography of Computing, Ethics, and Social Responsibility', http://www.siu.edu/departments/coba/mgmt/iswnet/isethics/biblio/. The ImpactCS (Impact Computer and Society) Project was presented as addressing "social and ethical impact of computing", http://www.seas.gwu.edu/seas/impactcs/

- privacy, identification, authentication (consumer), confidentiality, encryption, key escrow, trusted third party, ...
- protection of competition / avoiding monopolistic practices,
- intellectual property rights, copyrights, rights on software, ...
- computer crime / misuse,
- advertisements on the Internet: providing the customer with legal, decent, honest and truthful (adequate, accurate, ...) information.

Other questions (collective organisation of society)

- infrastructure ownership / monopoly (see for instance the Microsoft trial[23]),
- technological dreams, utopias, computer metaphors ... and all questions linked to awareness and education,
- impact on work and organisations,
- democracy/ organisation of the civil society in accordance with the "common good"; role of governments, political aspects, public policies, telecommunication policies, democracy, public security and order, ...
- self-regulation.

Topics With a More Ethical Content

- equity in the right of access ("universal service"),

  The importance of making information universally accessible and affordable has been stressed since the first declaration on the US National Information Infrastructure. Access to information is crucial for education, public health, ...; its accessibility to all will be a sign of democracy. The current situation cannot be considered as equitable.
- questions linked to the respect of the dignity of the person (protection of minors and human dignity; illegal and harmful content on the Internet, paedophilia, racial hate, denial of crimes against humanity, incitement to murder, to drug trafficking, to riot, ...),

  Many national and international organisations are preoccupied by the deleterious influence that the Internet could have in such matters. The time has come to confront the different ethics and approaches to these issues and to harmonise the practices, and combat such scourges.
- justice and social exclusion (mainly North-South, but also work distribution, ...),

  Social exclusion is unfortunately a concept which is still fully relevant when speaking about the Information Highways: there, we observe discrimination and exclusion of the elderly, gender imbalance, ... What does it mean to have at one's disposal all the means for efficient work when this is accompanied by a 10 to 12% unemployment rate (or even more in certain regions of the world) or with precarious jobs, and what does an information society mean where participation in its construction is kept in the hands of a few? Most probably large minorities in the Northern countries are in danger to be excluded from the information society. But overall everybody has also to remember - as President Thabo Mbeki argued in his keynote address to a G-7 Information Society

[23] Computerwire's coverage of the Microsoft trial has been acknowledged as the most complete and insightful in the industry: http://www.computerwire.com/msoft/

Conference: "There are more telephone lines in Manhattan than in all of sub-Saharan Africa" and "half of humanity has never made a telephone call."[24]

- respect for the interests and the rights of the persons,

  The Universal Declaration of Human Rights includes rights which can have an application in the field of ICT: privacy (art. 12), freedom of thought (art. 18), free speech, freedom to seek, receive and impart information and ideas (art. 19), ... This makes sense when we know that there are still 45 countries where access to the Internet is more or less strictly controlled. This may also be called also "censorship" (see below). Today's research programs are also trying to develop concepts of cultural, economic, and social rights.[25] *There are also rights and interests of persons in commercial exchange, in daily life, etc. which may be affected by communications technology.*

- free speech / censorship,

  On the Internet, how to find a relevant balance between free speech and censorship (sensu lato, i.e., any kind of control)? What is the relationship between censorship and controlling the access to the Internet? Free speech and the First Amendment are arguments which are culturally located[26]*, and must be examined in other contexts. The freedom of the press is a possible approach. One cannot avoid confronting the freedom of speech with the concept of responsibility.*

- quality of life,

  The "whole person" - Does technology lead to an imbalance in mind, body, spirit? Quality is a subjective term, but refers to standards. Helpful questions for discussion might be: "What standard of life do we expect, and to what extent (if any) does ICT affect those standards?" and "In what ways might ICT enhance or diminish our self-worth?"

- right to information ("transparency"),

  The role of information in the relationship between the citizen and the administration as well as in an effective market requires that clear and sufficient information be given to the citizen or to the consumer. It implies, on the one side, easy access to government records. It also implies also, on the other -- in e-commerce for instance -- relevant promotional material, clear prices, terms and conditions brought to the attention of the customer, definition of complaints procedure, ... (See also above: "advertisement on the Internet")

- personal qualities (honesty, competence, ...),

  All professional codes of conduct emphasise the personal qualities - conscientiousness, honesty and positive attitude, competence and efficiency - of the individuals involved in that occupation or profession.[27]

- non-abuse of power (appropriate use),

  While power generally involves the use of force (particularly physical force); authority may be used to influence others through charisma; heritage; or particular attributes or skills (Max Weber).[28] *In relation to the Internet, many different actors have technical influence over the way in which individuals communicate. The appropriate behaviour of*

---

[24] Information Society and Development Conference, 13-15 May 1996, Midrand, South Africa, Chair's Conclusions, http://www.ispo.cec.be/isad/isadconc.html

[25] Interdisciplinary Institute for Ethics and Human Rights, http://www.unifr.ch/iiedh/english/

[26] Among others: The Electronic Frontier Foundation and its Blue Ribbon Campaign for Online Free Speech (http://www.eff.org/), the Global Internet Liberty Campaign (http://www.gilc.org),...

[27] J. Berleur and M. d'Udekem-Gevers, Codes of Conduct within IFIP and other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, op. cit., pp. 28-31.

[28] Max Weber (1947*), The Theory of Social and Economic Organisation*, Free Press.

authorities can be explored at several levels: the roles of the various international and federal authorities, including the police and security forces; Internet service providers (ISPs); computer service providers in educational establishments and in commercial organisations; and the activities of Internet users themselves. Debate is to be encouraged about the appropriate activities of both individuals and services, and how all these parties should ideally act (lawfully, democratically, and in an egalitarian manner).

- respect for cultural differences,

  In the face of U.S. cultural supremacy in many domains (for instance in values conveyed by current filtering services), European, Asian, Latin American, and African countries must be encouraged to make respect for cultural differences a major concern.

- freedom of choice in the use or non-use of the Internet,

  Neo-Luddism?[29] *Could we exist without communications media that employ the highest of high technology? Most of us would certainly agree that there is much to criticise in many manifestations of modern technology. The sorting out of what works from what doesn't - and why, and if it is needed - is the kind of public dialogue about technology that we need. Technology is thought, action, information, invention - it exists for human beings.*

- grounding "virtual" life in the physical realm.

  Many people are concerned that the increasing importance of 'virtual life' will have serious psychological and social implications. Proposals have been made to encourage the use of computing to support rather than supplant real life. For example, 'community nets' are geographically based networks that help enhance real participation within a specific locality (e.g. neighbourhood, village).

Recommendations

1. SIG9.2.2 recommends to IFIP members, and mainly its national or regional Societies, to represent an ethical approach when involved at the national or regional level on Internet governance policies, where key ethical issues will be defined by the specific concerns of particular nations. Some of the issues that may be of concern are those set out and classified above under the title "Topics with a more ethical content". SIG9.2.2 offers its services to act as a rapporteur, and to share with other IFIP members what has been done by IFIP Members Societies and others, and what is still to be done (see the list of "Questions Raised to the IFIP Members" below).

2. SIG9.2.2 endorses the recommendations proposed during the HCC-5 Round Table. They are listed hereafter in the "Summary of resolutions" of the Report of P. Duquenoy and D. Whitehouse. Let us already mention some of them here.
   Let IFIP:
   - act to mitigate unequal access to the Internet,
   - use the Internet to develop a cross-cultural approach to the search for peace on earth,
   - focus on children and families and their need to access the Internet to further their learning experiences. Promote netmaking, rather than networking, with kids.
   - organise an active debate with North America on some more controversial questions relating to the ethics of the Internet,

[29] http://www.luddites.com/

- develop a channel or open forum for the expression of an Asian/Confucian ethics of computing.

3. SIG9.2.2 highly recommends that IFIP members (individuals, full member Societies, associates, affiliates, corresponding, ...) be present in the different constituencies where ICT (Information and Communication Technology) uses are discussed and where ethical principles would have to be considered in order to promote these principles.
   As examples of constituencies, SIG9.2.2 suggests among others UNESCO and its World Commission on the Ethics of Scientific Knowledge and Technology,[30] the European Commission and especially its Information Society Project Office, the different associations where issues are discussed (see the above mentioned Internet Content Rating Association, the Electronic Commerce Platform Netherlands, the Global Business Dialogue, ...; but also associations such as the Internet Society, the Electronic Frontier Foundation, the Computer Professional for Social Responsibilities, Privacy International, etc.)
   As far as ethical principles are concerned, SIG9.2.2 names the issues at stake, among others, in the above mentioned Action Plan of the European Commission on promoting safer use of the Internet or in Electronic commerce,[31] or in property rights (e.g. plagiarism would be a specific ethical issue), etc. Other issues may be found in our list of topics. The CPSR "One Net principles" that we already mentioned and which are reprinted below could be also considered as deontological principles.

Questions Raised to the IFIP Members

Let us conclude this introductory paper by raising some questions that we would like to see examined by IFIP Member Societies. Faithful to its creed of creating spaces for discussion locally and internationally, SIG9.2.2 will be happy to report on the answers it receives on the following questions:

1. Is there a specific ethical Committee in your Society?
2. If your Society has no specific Ethics Committee, does it have a particular group in charge of handling ethical questions?
3. Do you intend to work on the recommendations of this brochure? How?
4. Has your Society already taken action on any of these recommendations?
5. On what specific topics related to ethical matters has your Society been working in the last two years? As an international body, SIG9.2.2 would be happy to compare which are the specific ethical issues related to the governance of the Internet, as they are perceived by different cultures or in different countries.
6. Is there any written document resulting from your work? Is it available, and where? Could you put it at the disposal of SIG9.2.2, and specify if it is public, and can be circulated?

---

[30] http://www.unesco.org/ethics/uk/connaissances/

[31] Electronic Commerce is often considered today as one of the "killer applications" of the Information Highway. For the USA, see the official site of the Department of Commerce, United States Government Electronic Commerce Policy, http://www.ecommerce.gov For Europe, Electronic Commerce and the European Union, http://www.ispo.cec.be/ecommerce/. But there are lots of other sites, by country, such as for France, Mission commerce électronique, http://www.finances.gouv.fr/mission_commerce_electronique/, without forgetting the G8 pilot project 'A Global Marketplace for the SMEs', http://www.ispo.cec.be/Ecommerce/g7init.htm

7. In which national or regional organisations or groups is your Society present and active on ethical matters?
8. Can you describe, for the benefit of other IFIP members, some of the results of your activities?
9. Has your Society a Code of Conduct/Ethics? What was its date of publication? Is it on your website, and could you give us the exact URL? Is it translated, and available on the Internet in English? (Enclosed is the list of IFIP Member Societies codes at our disposal, with the latest dates of publication or revision.[32])
10. Does your Society intend or feel a need to update its Code of Conduct/Ethics according to the new uses to which the new technology can be put (Internet, e-commerce, tele-medicine, etc.)? In case your Society has already completed this work, can you provide SIG9.2.2 with the updated version?

[32] Some of them are available or referred to on the site of J.A.N Lee at Virginia Tech, or at the Centre for Computing and Social Responsibility, De Montfort University, Leicester, UK, http://ei.cs.vt.edu/~cs3604/lib/WorldCodes/WorldCodes.html http://www.ccsr.cms.dmu.ac.uk/resources/professionalism/codes.

IFIP Computer Societies and their Codes

1. IFIP National Member Societies

- ACM (Association for Computing Machinery, USA): ACM Code of Ethics and Professional Conduct (1992)
- ACS (Australian Computer Society, Australia): ACS Code of Ethics (Received 1993)
- AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico, Italy): Codice di Condotta Professionale dei Soci Ordinari AICA (Engl. transl. 1993)
- BCS (British Computer Society, UK): BCS Code of Conduct: Rules of Professional Conduct (1992), BCS Code of Practice (1978)
- CIPS (Canadian Information Processing Society, Canada): CIPS Code of Ethics and Standards of Conduct (1985)
- CSI (Computer Society of India, India): CSI Code of Ethics (1993)
- CSSA (Computer Society of South Africa, South Africa): CSSA Code of Conduct (1988)
- CSZ (Computer Society of Zimbabwe, Zimbabwe): The CSZ Code of Ethics for Institutional Members (1992), The CSZ Code of Ethics for all Individual Members (1992), The CSZ Code of Professional Conduct for Individual Corporate Members (1992), The CSZ Code of Professional Conduct for Registered Consultants (1992), The CSZ Training Accreditation Code of Practice (1992)
- FIPA (Finnish Information Processing Association): Code of Ethics (1999)
- GI (Gesellschaft für Informatik, Germany): Ethical Guidelines of the GI (1994)
- ICS (Irish Computer Society, Ireland): ICS Code of Professional Conduct (1994)
- IEEE (The Institute of Electrical and Electronics Engineers, Inc., USA): IEEE Code of Ethics (1990)
- IPSJ (Information Processing Society of Japan, Code of Ethics) (1996)
- NZCS (New Zealand Computer Society, Inc., New Zealand): NZCS Code of Ethics and Professional Conduct (1978)
- SCS (Singapore Computer Society, Singapore): SCS Professional Code of Conduct (1990)
- SIPIS (Swedish Information Processing Society - Dataföreningen i Sverige): Acceptable Use Policy of SUNET, and Ethical Rules for SUNET (1995)

2. IFIP Affiliate Member Societies

- CEPIS (Council of European Professional Informatics Societies, Europe): CEPIS Code of Professional Conduct (1992)
- SEARCC (South East Asia Regional Computer Confederation, South East Asia): SEARCC Code of Ethics, and SEARCC General Guidelines for the Preparation of Codes of Ethics for Members 1993)

Governance of the Internet: An Ethical Point of View
Report on a series of rolling workshops at the IFIP-TC9 Fifth World Conference HCC-5 (Human Choice and Computers)

Penny Duquenoy
Email: p.duquenoy@mdx.ac.uk
with the help of Diane Whitehouse
Email: Diane.Whitehouse@bxl.dg13.cec.be

Preface

The International Federation of Information Processing (IFIP)'s Special Interest Group on a Framework for Ethics of Computing (SIG9.2.2) exists as a result of an Ethics Task Group set up by IFIP's General Assembly in September 1992.

In the early nineteen nineties, a debate took place in IFIP about the possibility of establishing an IFIP Code of Ethics. Initially, an Ethics Task Group was set up to explore this possibility. In order to complete its task, the Task Group undertook to survey the codes of ethics of the various IFIP member societies.

As a result of this assignment, the Ethics Task Group published an in-depth analysis of thirty-one codes of ethics/conduct (Berleur & Brunnstein, 1996). This handbook contains specific recommendations that were adopted by the IFIP General Assembly in Hamburg in 1994. Those recommendations led to the foundation of the Special Interest Group on a Framework for Ethics of Computing (SIG9.2.2) and its various activities.

The handbook provides a wide range of material necessary for IFIP's member societies to consider when introducing or revising a code of ethics (or a code of conduct, or guidelines). It includes over thirty computer societies' codes and their analysis; comments on the most important codes; the philosophical background of cultural diversity; and papers on some more sensitive questions.

It is not IFIP's intention to provide its member societies with precise guidelines for particular codes. Rather, it advises them to consider its recommendations when writing or updating their own. IFIP does not actually state what 'ethics' the national societies should espouse when designing or adopting a code. It outlines that there are certain principles that all the national societies might wish to bear in mind.

In accordance with the diversity of histories, cultures, social and political backgrounds of IFIP member societies, IFIP regards it as essential that, when wanted or needed, codes should always be developed and adopted within the member societies themselves. IFIP offers its expertise in assisting these developments, collecting and disseminating material about established codes, and organising international debates on further developments.

Creating Spaces for Discussion

One of the special interest group's main activities is to create spaces for discussions. This is done in various ways (Berleur & Brunnstein, 1996: 263):

- submitting, for example, through the IFIP Newsletter, specific ethics case studies, and encouraging members to submit their own responses;
- making available all the up-to-date codes of IFIP national societies, with related pointers to existing documentation for further research;
- publishing, as foreseen in the European Directive, "the codes which have been the subject of a favourable opinion ..." (Directive 95/46/EC);
- providing a Forum - under the Chairmanship of the IFIP President - where discussion can be raised about harmonising codes of societies, in order to prevent restrictions in one country being prejudicial to another;
- participating in international forums where similar questions are treated; and
- assisting in the resolution of conflicts which could arise between national codes that are completely different.

On behalf of IFIP, the special interest group collects, compares and disseminates knowledge on developments in the national societies.

The special interest group's most recent initiative was to develop a series of workshops on the ethics of computing as its contribution to IFIP's 5th World Conference on Human Choice and Computers (HCC5). This conference, which took place in Geneva, Switzerland in August 1998, had as its main focus human choice in the age of globalisation in relation to computers and networks.

Governance of the Internet - Ethical Point Of View

Round Table on Rolling Workshop - Chair: Prof. Jacques Berleur

At the conference, a series of three workshops focused on issues related to the governance of the Internet. Three main forms of Internet governance were presented: technical controls, self regulation (that is, norms regulated by professional or trade associations), and legal controls.

The week of workshops culminated in a round table. The aim of this round table was to have discussion on the ethical issues and ideas arising from the previous three workshops. The round table's main points of discussion, and its ensuing resolutions, are described in detail here. Supporting materials from the workshops are contained in the appendices.

Attendees approached Penny Duquenoy the rapporteur) throughout the first two days of the conference to express their ideas and willingness to take the floor, and to give short, individual presentations to the audience at the round table. The presentations were as follows:

Prof. Colin Beardon (Plymouth University, UK)

Prof. Beardon was concerned that the impression in the first session on filtering/blocking software presented a rather 'negative' aspect of ethics: i.e. the workshop appeared to advocate

blocking or suppressing free speech and freedom of choice; thereby, encouraging a culture where values were attributed by third parties rather than by individuals. He wanted to see a different approach from censorship taken, and he cited the analogy of ethical investment by proposing the idea of "ethical gateways". In the same way that an investor can choose to invest in companies that pursue an ethical policy (from information given by an investment adviser), an individual could choose to support ethical practices on the Internet (via an ethical gateway). This type of approach re-establishes ethical responsibility with the user, engaging the user in ethical choices. To take an active ethical position sometimes requires 'hard choices'. For example, Greenpeace is promoted as an ethical organisation and is very action-oriented. As far as professional ethics (and associated codes of conduct) are concerned, there is a choice between a 'third party' approach (that is, when behaviour is monitored or controlled by a third party) and a more individually 'engaged' position.

Mr. Gunnar Wenngren (Linköping University, Sweden)

Mr. Wenngren's question also arose from the first workshop on filtering/blocking software. He pointed out that there were ethical issues in the evaluation of the criteria used to filter or to block in filtering/blocking software. The advisory groups for the various organisations and providers of software pronounce themselves representative of the Internet community. This announcement in itself is questionable. As far as the evaluation of the Internet is concerned (and the groups involved in the evaluations), several questions are raised: "who are the groups?", "what is their culture?", "are they a minority?", "what are their values? ", and "do they even exist?". The answers to these questions are relevant in an assessment of their authority and credibility. Further research would be useful. Values are very different between cultures. For example, in Switzerland prostitution is legal and regarded as a service whereas a prostitute in Afghanistan would be executed.

Although the groups undertaking the rating describe themselves as "advisory", there must be someone who makes the final decisions. Who are these people? Also, if a small subsection of a site is filtered, is the whole site filtered? In addition, it seems that some vendors choose to filter simply because they do not like a certain page or organisation. It is therefore right to ask the question "what sites are on the banned list?". This information should be publicly available.

Finally, filtering software can be automatically included in off-the-shelf products. These decisions are in the hands of a very few people.

Prof. Leif Bloch Rasmussen (Copenhagen Business School, Denmark)

Codes of ethics often enter the scene when a professional association is in crisis - that is, after the particular event causing the problem has occurred. For example, in the United States currently, the medical profession is assessing its behaviour at the very moment that it has become publicly known that syphilis research on black Americans was undertaken earlier in this century without the knowledge of the persons involved. Within communities, ethics and morality have been variously described by philosophers. The Danish philosopher K. E. Løgstryp talks about spontaneity, sovereignty, and a life of caring and helping when people are in need, and Pierre Bobillier suggests that morality is with mother and child. To bring these themes together, Prof. Rasmussen proposed that IFIP should concentrate on an initiative that examines the role of children and their families in relation to information and communi-

cation technologies. They should be viewed as learning entities which need access to the Internet. Let IFIP become the first ethical community!

Drs. Marc van Lieshout (Dept. of Informatics, University of Nijmegen, The Netherlands)

In the last presentation of the round table session, Drs. van Lieshout expressed his doubts regarding self regulation. His view is that the development of technology provides a choice between Faust and Frankenstein (a means to entertainment and amusement, but with a debt to pay). Although not a particular advocate of regulation/legislation, he foresees the alternative of self regulation as leading to a development of norms and values that are imposed on users by, for example, software companies, leaving the user with no free choice. Society is developing a view of people that is based on fun and entertainment - should this view set the foundation of ethical behaviour? For these reasons, it may be impossible to resist the power or the pressure to regulate in a more formal way. To return to philosophy, Drs. van Lieshout reminded the audience that, according to Emmanuel Lévinas, our conscience lies in the face of the 'other', and that we perhaps need that tension in order to ground our ethics.

*
* *

Discussion during this session was then open to the floor. Two general issues were raised that have previously been of concern to the special interest group on ethics (Berleur & Brunnstein, 1996: 241-56):

- were all the items for discussion within the series of workshops (and within the special interest group more generally) (such as intellectual property rights, security, and reliability) actually ethical issues?
- are ethics relative or fundamental? How possible is it to arrive at a universal set of ethics that is appropriate to all individuals? Alternatively, are there different sets of ethics relative to various broad cultural areas of the globe, such as the Far East, Europe, and North America?

It should be noted that the IFIP General Assembly has already given its pronouncement on these questions. It favours the discussion of ethics in all countries rather than promoting the idea of one code (Berleur & Brunnstein, 1996: 257).

An important suggestion was to think in terms of what we could strive for. Could there be a common starting point - for example, cross cultural values such as non-aggression, and peace? (Professor Gunilla Bradley) This proposal was supported. It was suggested that we question the underlying assumption of the Internet as an infinite resource, which it is not (e.g. unequal access), and that we look at the issues arising from a finite resource.

Finally, there were some comments from the floor regarding the document "One Planet, One Net : Principles for the Internet Era" drafted by Computer Professionals for Social Responsibility (CPSR). The remainder of the discussion was dedicated to a review of this document (see Appendix C).

Niklas Damiris, Visiting Scholar at Stanford University, Stanford, California, USA suggested that "There could be a re-thinking or a re-writing of the seven principles of the Computer Professionals for Social Responsibility charter".

Six very specific observations were made with regard to the document:

i) The CPSR document mentions rights but does not stress responsibilities enough. Rights should be linked with responsibilities.
ii) There is a need for debate with the United States US) regarding censorship. Americans' use of the First Amendment closes all avenues of discussion (i.e. freedom of speech takes priority over censorship).
iii) The document is written from an individual point of view, an individual who has free choice. The document presupposes we know what being socially responsible is.
iv) The word "freely" or "without restriction" should be added to item 3 of the document (Net users have the right to communicate). It is vital that freedom of speech should be upheld, notwithstanding the dangers that this brings with it.
v) As far as governance is concerned we have several models. However, because the US model is the first to emerge on the Internet we are in danger of adopting only North American rules rather than formulating rules from other cultures. This view of things will be unrepresentative; for example, the Asian view (if we take it from the perspective of a majority of the world's population) is important. We have a new opportunity to define a form of global government. Quite how this is to be achieved, we do not know.
vi) It was pointed out that, as an international federation, IFIP is well placed to obtain international views.

Another comment was that, since the Internet is international, then we should look to international law. However, it was pointed out that the basic principle of international government is sovereignty of countries. The Internet is one overriding entity - are we able to regulate it?

Summary of Resolutions

A number of proposals for action by IFIP emerged from the discussions in the final session. These included suggestions for activities at various different levels of the federation (whether within its special interest group on ethics or through its series of conferences on Human Choice and Computers).

No definitive decision was made at the conference on which of the following proposals would be adopted. That decision-making forms the next stage of the special interest group on ethics' activities.

Broadly, the philosophy underlying any such efforts - shall we call it a pro-active philosophy? - was encapsulated in the ideas voiced by Professors Colin Beardon, Gunilla Bradley, and Leif Bloch Rasmussen. Let IFIP:

- act to mitigate unequal access to the Internet (Colin Beardon).
- use the Internet to develop a cross-cultural approach to a search for peace on earth (Gunilla Bradley).
- focus on children and families and their need to access the Internet to further their learning experiences. Promote netmaking, rather than networking, with kids (Leif Bloch Rasmussen).

Three specific areas of research to be undertaken by the special interest group on ethics were proposed from the floor:

- what are the principles underlying the internationalisation of any laws on the use of the Internet? (Andrew Sloane)
- can what has been learned from the United Nations' experience of developing a Universal Declaration of Human Rights (and its application over fifty years) be applied to IFIP? (Ruud Van Gael)
- a study of filtering software to illustrate ethical behaviour. (Richard Sizer)

Finally, the following proposal was made:

As part of its mandate, IFIP must act to promote public discussion about the ethics of computing. These discussions could take place on relevant topics. In such a forum, IFIP might:

- organise an active debate with North America on some more controversial questions relating to the ethics of the Internet (Jacques Berleur).
- develop a channel or open forum for the expression of an Asian/Confucian ethics of computing (Bill Bishop).
- formulate its own guidelines for a charter on rights and responsibilities in the age of the Internet (Richard Sizer).

Overview

The series of workshops provided an ethical focus or theme for the conference as a whole. The discussion served as a reminder that computer scientists' involvement with information technology, and specifically with the Internet, brings certain professional responsibilities.

The format of the workshops was considered to have worked well. The factual giving of information, with time allotted for discussion and deliberation among participants and between sessions, allowed a more informed and conscious debate in the final round table.

The success of the workshop series means that this is likely to be a format that the special interest group will use again in the future.

The proposals that were made enable the special interest group to move ahead in its work. It must now decide on its next activities, bearing in mind the input, feedback, and suggestions that it has received from a wider audience. Several stimulating, concrete, and positive suggestions were made which fit well with IFIP's basic premise of creating forums for discussion on the ethics of computing rather than laying down a mandate for the behaviour of each of its societal members.

The ethical challenges posed to all members of society by the increasingly global use of information technology (and particularly by the Internet) are considerable, and will require much further careful thought as we move into the next century, and indeed the next millennium.

For Further Information

SIG9.2.2 welcomes the continued participation of a wider audience to its initiatives. Anyone wishing to learn more about this special interest group and its activities, should visit the group's website at:
http://www.info.fundp.ac.be/~jbl/IFIP/sig922

or should contact:

Professor Jacques Berleur
Institut d'Informatique
Facultés Universitaires Notre-Dame de la Paix
Rue Grandgagnage, 21
B - 5000 Namur
Belgium
Phone: +32-81-7249-76 (Secr.-64)
Fax: +32-81-7249 67
Email: jberleur@info.fundp.ac.be

References

Berleur, J. & Brunnstein, Kl. (editors) (1996), *Ethics of Computing: Codes, Spaces for Discussion and Law*. Andover, Hants: Chapman and Hall.

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, Brussels, *Official Journal of the European Communities*, 23.11.95, No L/281/31-50.

'Timothy R. McVeigh vs. The US Navy'
http://dont.stanford.edu/cases/mcveigh/mcveigh.htm
http://www.wiredstrategies.com/mcveigh.html
http://www.lambda.org/McVeigh.htm
http://www.hrc.org/mcveigh/

'EU considers draft US "safe harbor" principles'
http://europa.eu.int/comm/dg15/en/media/dataprot/news/harbor.htm

'Joint Report on Data Protection Dialogue to the EU/US Summit, 21 June 1999'
http://europa.eu.int/comm/dg15/en/media/dataprot/news/summit.htm

APPENDIX A

A1. Background to the Workshops

At HCC5, SIG9.2.2 organised a series of rolling workshops and a round table with a focus on 'ethical governance of the internet'.

The format of the workshops and round table was somewhat in the nature of an experiment. Rather than simply host the round table and present conference delegates with topics for discussion, the emphasis was placed on active audience participation. The rolling workshops were specifically designed to introduce topics relating to regulation of the Internet to the participants. Although the topics covered were considered to contain an ethical perspective, the papers presented were deliberately devoid of ethical opinion. The intention was to offer the audience 'straight facts' so that they could assess the ethical dimensions of the questions for themselves. The idea behind this experiment was to provide conference delegates with concrete information so that they could give these matters some thought in advance of the round table session. They would then be able to participate more fully, and fruitfully, in the round table. It was planned that the structure of the round table session would evolve from comments collected from the delegates following the presentations, and that some members of the audience would become the presenters at that session.

To create a sense of continuum and participation, a member of the special interest group (Penny Duquenoy) was elected as rapporteur or 'collector of ideas' from the audience. Her remit was to provide a summary of the previous workshops at the beginning of each workshop session. She was also asked to collate any opinions on ethical matters expressed to her by members of the audience during the week.

A2. The Workshops

There were four workshops of approximately one hour each, arranged at intervals during days 1 and 2 of the Conference. The round table was held on the final day of the Conference.

The main theme of the series of workshops was the governance of the Internet. The workshops explored three main forms of governance: technical controls; self regulation (that is, norms regulated by professional or trade associations); and legal controls.

Rolling Workshop - Introduction
Chair: Prof. Jacques Berleur (Chair SIG 9.2.2)

The first of the workshops was an introductory one. It was chaired by Prof. Jacques Berleur, who explained the nature and theme of the workshops to the audience. The audience was made aware of the participatory nature of the events, and Prof. Berleur introduced Penny Duquenoy as the contact person for their views on ethics. The audience was requested to refrain from discussions about ethics until the round table, but any questions to clarify the content of any presentation were answered at the time of the workshop.

As an aide-memoire to the ethical focus of the series of presentations, the members of the audience were asked to bear the following questions in mind :

What are the main ethical issues?

i) Should the Internet be regulated?
ii) By whom?
iii) How (including cost effectiveness)?

In addition, the Computer Professionals for Social Responsibility (CPSR) document "One Planet, One Net: Principles for the Internet Era" was put forward as a discussion document. It was intended that comments and observations could be relayed back to the CPSR.

Technical Means to regulate the Internet
Chair: Eur. Ing. Richard Sizer (Member SIG 9.2.2)

The second workshop was the first in a series of presentation sessions. Two papers were presented, one on technical controls of the Internet and the other on filtering software.

"Internet Convergence and Technical Control" Prof. Joseph Kizza (University of Tennessee, Chattanooga, USA)

This paper presented the Internet as a combination of three media: communications, computer services, and broadcast. Each medium has its own problems in terms of governance and control. Within the communications area, there are ethical issues which may be a function of the level of security of the information held on databases at servers or the security of the data during transmission. With electronic commerce "predicted to be one of the fastest and largest components of the Internet within the coming couple of years", the security controls (involving both hardware and software controls) are related to server security, server access, and transmission. Technical security controls currently in use include firewalls (protection of the server) and cryptography (protection during transmission).

In the Computer Services medium, the loopholes in security are evident. Complex operating systems are exposed to risk in a variety of ways, such as hacking, fraud, and safety critical software. Again, security is the main issue.

From the point of view of the Internet as a broadcast medium, several issues (already well known in this medium) arise. These are issues of free speech, access, intellectual property, child pornography, harassment, and security. One of the technical methods of control is the Platform for Internet Content Selection (PICS), which provides standard of labelling web pages according to their content. This technology can be adopted by groups or individuals to set their own criteria for rating and accepting or rejecting web pages, leading to the development of filtering or blocking software.

"What can be regulated on the Internet by control/filtering software?" Dr. Marie d'Udekem-Gevers (Cellule Interfacultaire de Technology Assessment, Facultés Universitaires Notre-Dame de la Paix, Namur, Belgium)

This paper outlined a description and criticism of control/filtering software. It set out the social and ethical implications of the processes involved in control/filtering (for example, setting labelling vocabulary and assigning labels). The approaches taken to control content

vary from suggesting appropriate sites, searching, informing, monitoring, and warning to blocking. Control can relate to topics (taking place at the entry point to an address and based either on ratings or “not/black list”, or at the level of the content itself) or to time. PICS introduces a separation between labelling and filtering : consumers can choose their filtering software and label sources independently. However, questions arise such as :

i) Who has set labelling vocabulary and criteria for assigning labels?
ii) Who is in charge of assigning labels?
iii) What are the possibilities for customising the filtering software?

In a sample of ten ratings analysed by the author, nine are in English (one was written in Italian) and six use criteria defined in the US, the remaining four comprise Canada (2), the United Kingdom (1) and Italy (1). The most frequent categories in the sample are 'sex' and 'violence'.

Following these two presentations, the questions and concerns from the audience were:

"Is it possible to see which sites are on any filtering “not/black list”? Concern was expressed that certain sites could be arbitrarily black-listed (for example the suppliers of a filtering system could pre-set the system to exclude a competitor's web page). If black-lists are used, and the list is withheld from public view, any third party rating service has the power to dictate accessibility (i.e. inclusion or exclusion).

"To what extent is it possible to have a system of technical controls?" The point was made that as technical controls are introduced, technical 'antidotes' are also found. (For example, the introduction of filtering software has also brought bypass-filtering techniques.)

Self-regulation of the Internet
Chair: Penny Duquenoy (Member SIG 9.2.2)

This third workshop presented delegates with an overview of various means of self-regulation (through codes of conduct or charters). One paper was presented which is summarised below.

"Governance and Self regulation" Prof. Jacques Berleur, (Cellule Interfacultaire de Technology Assessment, Facultés Universitaires Notre-Dame de la Paix, Namur, Belgium)

As far as governance of the Internet is concerned there is now a call for self regulation. This presentation identified what is meant by self regulation (voluntary acceptance of rules of behaviour by a group), and showed the methods employed by Internet users to establish some system of self regulation (e.g. codes of conduct).

The methods classified under self regulation are diverse. They range from a variant of the "Ten Commandments", through to Netiquette, virtual communities' rules, charters, codes of ethics, and codes of Internet Service Providers (ISPs). Of course, with such a diversity of groups (and diversity of motivation) the priorities, and nature, of issues and principles differed. For example, the first item on the list of topics of the French Internet Charter Proposition aims to protect what they see as a "new space" (i.e. Cyberspace) of free expression and liberty, whereas the first item on the list of service providers refers to the legality of material. However, some generally agreed principles emerge (although the wording of the particular

charters or codes differs). Some common principles advocate fairness, respect, honesty, sincerity, privacy, intellectual property rights, free speech, and seek to discourage computer crime and illegal, dubious, or harmful material.

Although self regulation is effective in several areas, in matters that specifically concern ethics, a number of issues still need to be addressed including: questions of participation; 'places' (physical or virtual) where self regulation is applicable; and enforcement. To be effective, regulations of codes or charters must be seen to be applied. Even where some sort of complaints or feedback procedure is in place, it is unlikely that any organisation will advertise its shortcomings, or inform the general public of weaknesses in its security. This poses some difficulties in evaluating the success/effectiveness of self regulatory procedures. It also seems that, in some instances, codes of conduct or charters are little more than "propaganda statements" or self-defence provisions.

Following this presentation, some comments from the audience included :

Items mentioned in some codes of ethics/charters (e.g. fraud) are criminal offences. To focus a fruitful debate on 'ethically grey' areas, it might be helpful to distinguish between 'illegal' and 'unethical' activities.

The Internet - The Role of the Law
Chair: Prof. Joseph Kizza (Member SIG9.2.2)

This session offered delegates information on the legal issues currently under discussion with respect to the Internet. One presentation was made, as below.

"The Role of the Law" Laetitia Rolin (Centre de Recherches Informatique et Droit, Namur, Belgium)

This presentation focused on two issues of current concern to users of the Internet:

i) privacy,
ii) protection of copyright.

The debate concerning privacy began with the question, "Is privacy a matter of ethics or economy?". First the position held by the United States was outlined, followed by the position held by the European Union.

In the United States, the trend (although there are strong opponents) is for the private sector to lead the way. The government recognises the unique qualities of the Internet and is keen to avoid placing undue restrictions on its use. Electronic commerce is to be facilitated.

Statistics in the United States show that Internet users are concerned about their privacy, and the use of their private data. They also show that more people would use the Internet if their privacy were protected in some way. The implications are, therefore, that the use of the Internet for commercial purposes is not realising its potential, and the future expansion of the Internet is at risk.

The United States government believes that trust and confidence in the Internet must be restored in order to maximise its commercial benefits. An example of one mechanism to build trust comes from a private-sector initiative called TRUSTe, a standards-setting organisation that provides web pages with a recognised seal of approval. However, confidence is not being restored as fast as the Federal Trade Commission would like, and the Commission has demanded that effective self regulatory measures should be implemented before early 1999. If this does not happen, additional government measures will be deemed necessary.

Non-governmental measures, such as market sanctions can be helpful for the effectiveness of self regulation. In the case of privacy, shares in the Internet Service Provider, Geocities fell heavily following public exposure of its practice of selling information from its database.

Where government measures do exist, for example the Electronic Communications Privacy Act, these measures are not necessarily effective. In the McVeigh case in the United States, information regarding McVeigh was gained illegally (by his employer the United States navy) and given illegally (by his service provider). The Electronic Communications Privacy Act states that information regarding a subscriber may not be given to a governmental entity without a warrant or court order. In this case, personal information regarding McVeigh was obtained by the navy and used in court as evidence of behaviour which would lead to his discharge from the service. [33]

The position taken by the European Union is expressed in its telecommunications directive which argues the confidentiality of personal data. The link between privacy, confidence and trust, and the influence of these issues on electronic commerce is also recognised. However, as far as legal sanctions are concerned, there are problems because of conflicts in definitions. For example, is personal information held by Internet Service Providers traffic and billing data or the collection of personal data? Different rules apply to these categories. There is a lack of clarity in definitions of roles and scope of the actors involved. [34]

On the question of copyright, there is a tension between the law and technique. Technical solutions for resolving privacy on the Internet focus on the mechanics (techniques) of production rather than on the content of the work. If this concept is followed, and content takes a secondary position (or is ultimately ignored), the nature of copyright will be altered, and we could see the "death of copyright". This would have serious ethical consequences as far as traditional notions of the ownership of ideas are concerned.

---

[33] 'Timothy R. McVeigh vs. The US Navy'; http://dont.stanford.edu/cases/mcveigh/mcveigh.htm, http://www.wiredstrategies.com/mcveigh.html, http://www.lambda.org/McVeigh.htm, http://www.hrc.org/mcveigh/)

[34] Regarding the current status of the discussion between the United States and European Union about art. 25 of the Directive, on "adequate protection", when there is a transfer to a third country of personal data, see: 'EU considers draft US "safe harbor" principles' http://europa.eu.int/comm/dg15/en/media/dataprot/news/harbor.htm
'Joint Report on Data Protection Dialogue to the EU/US Summit, 21 June 1999' http://europa.eu.int/comm/dg15/en/media/dataprot/news/summit.htm

APPENDIX B

B1. Internet Convergence and Technical Control

Joseph M. Kizza
University of Tennessee, Chattanooga, USA
Email: joseph-kizza@utc.edu

Introduction

By its very nature, the Internet medium is a convergence of three independent media. First it acts as a communication medium by its email facilities. Secondly it can be considered as computer services medium because it is a mega network of computer networks. And thirdly it acts as a broadcast service just like television, radio, and newspapers because of its capacity to carry news and information.

Each one of these three media presents problems that are unique. The value and utility of the Internet as a global medium then depends on what constituent medium one is in and the value of the content one gets out. This means that the perceptions, expectations and concerns are different in each constituent medium. However, the Internet carries all these things faster, better, more efficiently, cheaper, covers a lot more ground and it exhibits an unprecedented ease of access.

The Broadcast medium has the most problems with the general public because it is extremely difficult to please everyone in the diverse cultural, religious, linguistic, educational, and geographical global population. So our focus in this paper is going to be on the Internet as a communication medium and as a broadcast medium.

The Internet as a Communication Medium: Security and Control Mechanisms

As a communication medium, the Internet's fundamental problem is security of information in databases on the Internet servers and during transmission between servers. The Internet's ability to globally bring these databases to the reach of individual computers created a potential for any computer user to access any of these databases at will. The security of information does not only depend on the security of databases and communication media, it also depends on weaknesses in network software like Internet browsers, operating systems and every network application software stored on servers. Security controls to be considered, therefore, need to cover server security, server access, transmission protocols, and should involve both hardware and software.

Hardware System Security and Control

Hardware security controls are varied and involve access to hardware resources like memory and files, authentication routines for file access, password protection and the use of firewalls. These controls are divided into six areas, namely (1):

(i) Prevention to restrict access to information on the system by preventing access to a server on a network.
(ii) Protection to identify all security requirements of the system, evaluating them and coming up with the most suitable and most comprehensive techniques which are then deployed to protect the system.
(iii) Detection to provide early warning for early discovery of security bleaches that have by-passed both protection and prevention mechanisms.
(iv) Limitation intended to cut the losses suffered in case of failed security.
(v) Reaction to analyze the security and type of lapses, and the efforts to come up with remedies for a better security system based on the failures observed.
(vi) Recovery to recover what has been lost as efficiently as possible and update contingent recovery plans for the system in case of future failures.

Firewalls

Prevention and protection can be achieved through a *Firewall.* A firewall is a computer with two Ethernet cards connecting two networks, one network on one card being an internal and secure network and the other network on the second card being an un-secure external network. This computer then is set up to accept, deny or pass network traffic in both directions. Only authorized traffic is allowed to pass through these bottleneck security barriers. Firewalls have two benefits. First they allow the control and monitoring of network traffic by the network manager of the local network, and they simplify and localize the security problems of a local network on a single device, thus making security management easy.

Internet Transmission Security

Information security during transmission depends on a secure transmission protocol suite. Cryptography or secure writing, secures information in transition through the use of mathematical and logical functions which transform data into unintelligible forms, a process known as encryption, before transmission and back into intelligible forms, a process known as decryption, after the transmission.

In communication, specially modern digital communication, cryptography is a vital part in information security policy. It provides the needed lock and key to information handling on the Internet. The security provided by cryptography then enables individuals and businesses to protect their sensitive information during transition. Of late Internet commerce, or ecommerce, has been the fastest growing component of the Internet. This growth, and indeed the growth of the entire Internet, will depend on the security of sensitive information while on the Internet, hence on cryptography.

The Internet as a Computer Services Medium: Network and Software Security Controls

Beside the highly technical and network-based hardware security tools and controls discussed so far, there are also software tools displaying more local and individual controls of

the security of Internet information. With the Internet's reflection of the real world and its ability to transcend national barriers, comprehensive control tools are difficult, if not impossible, to globally apply due to the global mosaic of jurisdiction, culture, religion and political interests. So these tools with individual control initiatives are more appealing because they give each individual user personal control, and they are not so technical. Such tools include client and network operating systems, information management techniques, Internet server and browser software.

Network Operating System Software

A Network Operating System (NOS) is a set of core programs that together manage the resources of a computer system or network making the users aware of the multiplicity of machines in the network. The security of an operating system depends on the security of the kernel: the operating system part that is at the lowest level of functionality responsible for synchronization, interprocess communication, message passing and interrupt handling. And the security of information on a computer system or network highly depends on the operating system.

The security challenges presented by network operating systems include the need to be able to integrate and synchronize individual systems' security technologies such as authentication, access control, and cryptology.

Security Information Management

As operating systems uses increased and the number of different operating systems' technologies and the sizes and types of network increase, the security issues involved become more complex. Different security mechanisms and protocols are being developed every day, and keeping up with that stream of new techniques and methods is becoming increasingly very difficult especially in a network environment where each site may have customized and specialized techniques and protocols. So a management scheme is necessary to effectively synchronize these deferring mechanisms and protocols, and protect the system from unauthorized accesses by those taking advantages of weak points and loopholes resulting from the integration.

Server and browser software security

The problems of server and browser software security fall within the general problem area of software security. Like in general software, server and browser software errors result because of programming and data bugs which create holes and trapdoors in the software. Such Internet security trapdoors are not only limited to Internet browsers, but are also in Internet software especially server software like Fast Track from Netscape, Mail Server, Proxy Server, Enterprise Server, News Server and Catalog Server. Beside web browsers and server software, Internet security problems may also be found in Network technologies like ActiveX, a Microsoft Internet technology, and Java applets a Sun Microsystems technology.

The Internet as a Broadcast Medium: Security and Control Tools

Labeling and Rating Software

Internet software technology has developed to such an extent that easier and self-regulatory tools for personal control are already available and cheap. The crusade for voluntary self-regulating the Internet using rating and labeling software is led by industry giants , Microsoft and America Online (2). The rating and labeling standards are based on a PICS technology. PICS stands for "Platform for Internet Content Selection", a mechanism of labeling web pages according to their content based on a set of criteria developed by rating software firms. The labels attached to the web pages are then used by the filtering software when such a page is being accessed.

Rating of Internet content is very similar to rating of movies and videos and it follows a similar procedure resulting in an assigned label. There are a number of rating companies most of them supporting PICS technology and standards. The two most notable of these are:

(i) RASC
RASC or RSACi rating system is open and content-based providing blocking capabilities for entire sites, sections, or even individual pages or files within a site and through browsers. The RASC rating system has about twenty category restrictions grouped into four descriptors of Violence, Nudity, Sex, and Language, and four levels.

(ii) SafeSurf
SafeSurf is a rating, classification and filtering system using PICS technology and standards. SafeSurf's identification mark is the SS~~, called the wave, with close to 90 category restrictions in its rating repertoire grouped into ten SS-classification marks from SS~~000 to SS~~ 009 with each classification mark having close to nine levels.

A website is given a label either through self-rating, in which individuals place voluntary labels on their products or third-party rating in which a third party, like an independent labeling agency, is used to label the contents of the products.

Filtering/Blocking Software

Filtering software also known as blocking software rates documents and websites that have been rated and contain content designated on a filter's "black list". Filters are either client-based or server-based. Client-based filters are installed on a user computer and such filters are maintained by individuals and therefore less secure. Server-based filters on the other hand are installed centrally on a server and are maintained by a network administrator or an ISP. They are very effective throughout the entire local network and they offer better security because they are not easy to tamper with.

Even though filtering software, both browser-based and client-based, have recently become very popular, they still have serious problems and drawbacks like inaccuracies in labeling, restriction on unrated material, and just mere deliberate exclusion of certain websites by an individual or individuals. Inaccuracies have many sources. Some websites are blocked because they are near a file with some adult content; for example, if some materials are in the same directory as the file with adult content, the website with the file without adult content may be blocked. Sometimes websites are blocked because they contain words deemed to be distasteful. Such words sometimes are foreign words with completely different meanings but happen to have similar string names.

Conclusions

In this paper we have outlined and at times discussed tools in place to check on the activities on the Internet. The array of tools discussed so far is indicative of the nature of the debate concerning online content and what to do about it. While there are disagreements on what needs to be done about Internet content, there seems to be total agreement on some issues like security and privacy of that content. On those issues where there is agreement, the tools needed to be used are already in place although some need improvement as technology improves. However, on those other issues where there is no agreement, new and more varied tools need to be developed that give customers control of the Internet content so that those who feel that there is a need for censorship can use those tools like filters and blockers to censor this content to the degree they want, and those opposed to censorship and can live with the content can do so.

References

1. Joseph M. Kizza. *Civilizing the Internet: Global Concerns and Efforts Toward Regulation*, McFarland, Publishers, London, UK and Jefferson City, NC, 1998.
2. "Cyberspace attacks threaten national security, CIA chief says", CNN-Interactive, June 25, 1996. Also http://cnn.com/TECH/9606/25/comp.security/index.html

B2. Ethics and modes of governance of the Internet

Jacques BERLEUR (IFIP-SIG9.2.2 Chair),
Marie d'UDEKEM-GEVERS and Laetitia ROLIN
Facultés Universitaires Notre-Dame de la Paix, Namur, Belgique
Email: jberleur@info.fundp.ac.be; mgevers@info.fundp.ac.be;
laetitia.rolin@fundp.ac.be

Introduction[35]

It is now well recognized that the global network environment, and in particular, the Internet, defies traditional regulatory theories and governance practices. The main reasons are linked to the disintegration of the concepts of territory and sectors. It has therefore been suggested to approach the regulation of the Internet from different points of view, technical, self-regulating and legal, for instance.[36]

This paper is a first exploration of those challenging issues, but does not pretend to be more than an attempt to assess what is really happening in the different domains of technical mechanisms, self-regulation and the law. We are not looking at what could be done, but at what is done through those different instruments, trying to enlighten which are the ethical issues which are covered by those instruments and which are not. It is a kind of a first inventory.

In this short paper, we tried to summarize the approach we presented during a recent "rolling workshop and round-table" during the fifth IFIP-TC9 Human Choice and Computers international conference held in Geneva, last August.[37] This work is the fruit of an on-going working programme within the Special Interest group (SIG9.2.2) "IFIP Framework for Ethics" of the International Federation for Information Processing. We shall analyze the ethical issues, as they appear first when considering the technical means of labeling and filtering, second in a sample of self-regulation systems, and finally in two specific legal questions.

---

[35] This paper is a summary of three papers which were presented during the "rolling workshop" of the IFIP-TC9 HCC-5 conference (Geneva, August 1998). It has been presented, as a result of the IFIP-TC9 HCC-5 Conference at the UNESCO InfoEthics'98. It is reprinted here with the kind authorization of UNESCO. (See http://www.unesco.org/webworld/infoethics_2/index.htm)
The two first authors belong to the Cellule interfacultaire de Technology Assessment (CITA), the third to the Centre de Recherche Informatique et Droit (CRID), which are both sponsored by the Belgian Federal Office for Scientific, Technical and Cultural Affairs, in the Framework of its Programme "Interuniversity Poles of Attraction", Phase 4, Convention n° 31.

[36] Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 *Emory Law Journal* 911, 1996, reprinted in *Borders in Cyberspace*, Brian Kahin and Charles Nesson, eds., MIT Press, 1997.

[37] Ethics and the Governance of the Internet, Rolling Workshop and Round-Table at the 5th Human Choice and Computers IFIP-TC9 International Conference, *Computers and Networks in the Age of Globalization*, Preceedings, S. Munari, G. Krarup and Leif Bloch Rasmussen, Eds, Geneva 25-28 August 1998, Printed by the University of Lausanne, pp. 307-387.

Ethical Issues and Questions with Filtering Software

Introduction

Filtering/control software is a technical means, located on a PC or a server or at the level of an Internet service provider, to restrict the distribution of certain kinds of material over the Internet.[38] In many cases, its goal is the protection of children against sex, violence, hate speech, etc. (see Table 1).

Labeling categories	Frequency in the sample
sex	7/10
violence	7/10
age	5/10
intolerance/hate speech	5/10
gambling	4/10
drugs	3/10
language	3/10
nudity	3/10
alcohol/tobacco	2/10
profanity	2/10
education content	2/10
gross depictions	1/10
satanic/cult	1/10
militant/extremist	1/10
quality	1/10
etc.	

Table 1 : Labeling categories and their frequency in a sample of 10 ratings[39]

This kind of software is promoted or supported by industry, Free Speech activists and some governments. Currently a lot of the available control software packages filter at the level of the entry point to an address on the basis only of their proprietary (and secret) list of URLs.[40]

But this could evolve thanks to PICS (Platform for Internet Content Selection). PICS is a set of technical standards which have been developed since summer 1995 by the MIT's World Wide Web Consortium. "The first and most important distinction that PICS introduced is a *separation between labeling and filtering*. A label describes the content of something.[41] A

---

[38] 'Control' and 'filtering' are considered here as synonymous.

[39] Cyber Patrol (4.0) (CyberNOTlist), evaluWEB, Net Shepherd's Rating, SurfWatch (for kids), Adequate.com, IT-RA, RSACi, Safe For Kids, SafeSurf's Internet Rating Standard, Vancouver Webpages Rating Service (see M. d'Udekem-Gevers, What can be regulated on the Internet by control/filtering software ?, in: *Computers and Networks in the Age of Globalization*, doc.cit., pp. 315-334).

[40] An URL (Uniform resource Locator) identifies the location of a document.

[41] « PICS labels can be attached or detached » (and stored on a separate server called a 'label bureau'), Paul Resnick, 1997 Filtering Information on the Internet, in: *Scientific American* 03-97.

filter makes the content inaccessible to some audience."[42] In other words, thanks to PICS, "Consumers choose their selection software and their label sources (called rating service) independently." [43] "More generally, there are six roles that could be filled by different entities", as explained in table 2.[44]

1. 'Set labeling vocabulary and criteria for assigning labels'
2. 'Assign labels' (= rate or classify)
3. 'Distribute labels'
4. 'Write filtering software'
5. 'Set filtering criteria' (= customize)
6. 'Install/run filtering software'

Table 2: The 6 roles implied by filtering software (according to Resnick 1998)[45]

Moreover, PICS standards facilitate "*self rating* (enable content providers to voluntarily label the content they create and distribute) *and third party rating* (enable multiple, independent labeling services to associate additional labels with content created and distributed by others. Services may devise their own labeling systems, and the same content may receive different labels from different services."[46]

PICS would become more and more important. Control software such as Cyber Patrol does not hesitate to become currently PICS compliant.[47] PICS approach, which separates clearly the different roles involved in filtering, helps to analyze issues and allows solutions which are interesting from an ethical point of view.

Ethical issues with filtering software will be discussed here from the breakdown of table 2. Let us first remark that to 'set labeling vocabulary and criteria for assigning labels' is not value-neutral and that to 'assign labels' and to 'set filtering criteria' imply moral judgements. Any ethical approach has thus to focus on these three roles.

Outside PICS

Outside PICS, it happens as a rule that several roles (particularly to 'set criteria for assigning labels' or for classifying, to 'assign labels', to 'distribute labels' and to 'write filtering software') are filled in the framework of one firm or even by one sole commercial entity.[48]

---

[42] Paul Resnick last revised 26-01-1998, PICS, Censorship & Intellectual Freedom FAQ, http://www.w3.org/PICS/PICS-FAQ-980126.html

[43] Resnick Paul and Miller James, 1996, PICS: Internet Access Controls without Censorship, in: *Communications of the ACM*, 39 (10), October 1996, p. 88.

[44] P. Resnick last revised 26 01 1998, PICS, Censorship & Intellectual Freedom FAQ.

[45] See http://www.w3.org/PICS/PICS-FAQ-980126.html

[46] See http://www.w3.org/PICS/principles.html

[47] According to several comparative reviews, Cyber Patrol is the best among the tested packages. (see Munro C., 1997, Internet Filtering Utilities, in: *PC Magazine*, April 8 1997, pp. 235-240.;Parental Control Software at a Glance, October 97 issue of *FamilyPC* http://www.zdnet.com/familypc/9709/noway/table.html ; Meeks Ch., 8 programs to porn-proof the Net, 4/3/96; updated 5/28/97 http://www.cnet.com/Contenu/Reviews/Compare/Safesurf)

[48] The role of 'assigning labels' is similar to the one of making a list of URLs to block.

Ethical issues are obvious with this kind of software: *users are linked to the subjective value judgements of this firm* ! Even to 'set filtering criteria' can be reduced by the firm to a nearly virtual role: the only choice available can be, for example, between 'filtered access' or 'not filtered access'.

Within PICS

Within PICS, as explained above, the six roles can be filled by different entities. This can obviously improve the situation from an ethical point of view but cannot delete any issue.

We suggest here a set of questions to be raised and which, of course, remain valid outside PICS.

Set Labeling Vocabulary and Criteria for Assigning Labels

To 'set labeling vocabulary and criteria for assigning labels' is a crucial role. First it influences automatically other steps of the filtering process ('assigning labels' and 'setting filtering criteria'). But moreover, as pointed out by CPSR (1997), "in general, the *use of a filtering product involves an implicit acceptance of the criteria used to generate the ratings involved.*"[49]

- Who is in charge of this role ? Is the identity of the person or the body responsible for this role clearly given in the documentation about the filtering software ? Would it be justified that a government fills this role ?
- Are the rating vocabulary and criteria clearly defined so as to allow the user (parents, ...) to judge if they are consistent with his/her own values ? Are they rich enough to allow a real choice at the level of the rating and at the level of the customization ?

Assign Labels

- Who is in charge of the very sensitive role of assigning labels ? Is the identity of the person or the body responsible for this role clearly given in the documentation about the filtering software ?
- Which of the two approaches (self-rating and third party rating) is the best ?
- When a third party rating service is involved, the next questions are to be raised : Who is effectively represented by this third party ? Is this party representative, for example, of a values-oriented organization or of a given population or culture? How are the ratings attributed?
- With self rating, the questions are : How to oblige or, at least, to incite people to self rate ? And on the basis of which principle ? How to solve the problem of mislabeled pages, and particularly of deliberately mislabeled pages ? As suggested by Cranor & Resnick, "The Internet community will need to co-operate in the creation of either vouching services, which vouch for authors who are honest in their self-labeling, or blacklisting services which keep track of authors whose labels are not reliable."[50]

---

[49] CPSR 1997, Filtering FAQ, Version 1.1, 12/25/97, written by Hochheiser H., http://quark.cprs.org/~harryh/faq.html

[50] Cranor Lorrie F. & Resnick Paul, Technology Inventory, 12 March 1998, http://www.research.att.com/~lorrie/pubs/tech4kids/t4k.html

- If people assign labels and if labeling is not compulsory all over the world, it is obvious that *many sites will stay unlabeled*. The question is then : What to do with unlabeled sites ? If the software allow unrated sites, then the global control will not be efficient but if it does not, then innocuous and very interesting sites will be not accessible (see the discussion of Weinberg on this subject).[51] And thus in this case, "blocking software could end up blocking access to a significant amount of the individual, idiosyncratic speech that makes the Internet a unique medium of mass communication. Filtering software, touted as a speech protective technology, may instead contribute to the flattening of speech on the Internet."[52]
- Can the person or body in charge of the rating use rating criteria in accordance with his/her own value judgements ?
- Are the ratings numerous and various enough to cope with the diversity of cultures and of opinions at the level of the customization ?

Set Filtering Criteria

- Which kind of customization ? In fact there is a dilemma : the more choices you give to the final users the more difficult it is to set ! A solution in the future could be, as suggested by Cranor & Resnick, "to allow users to download preconfigured setting from organizations they trust. Child advocacy organizations as well as various religious, political, and educational organizations might recommend configurations to parents. Parents could download these settings with a simple click of the mouse and have them installed into their child's software."[53]
- Who is in charge of this role? Initially this role was dedicated to parents to control their children. But filtering software are used also by libraries (in the USA), for instance to control adults, by schools and by firms. Is it ethically justified to give such a power of control to this kind of entity ? "A government could try to impose filtering criteria in several ways, including government-operated proxy servers (a national intranet), mandatory filtering by service providers or public institutions, ..."[54] Would it be ethically justified ?
- Can the person or body in charge of the customization find both criteria and a rating in accordance with his/her own value judgements ?

Governance and Self-regulation

Pierre Van Ommeslaghe defines self-regulation as "a legal technique according to which the legal rules or the rules of conduct are created by the persons to whom they are intended to be applied, - either those persons do it by themselves or they are represented to do it", but he does explicitly exclude some 'codes of conduct' which are enacted by international organizations, since the persons to which the code will be applied are not participating in the process.[55] In a way which is not very different, Pierre Trudel defined it as "the recourse to

---

[51] Weinberg J. 1997, Rating the Net, http://www.msen.com/~weinberg/rating.html
[52] ibid.
[53] Cranor L. F. & Resnick P., Technology Inventory, art. cit.
[54] See http://www.w3.org/PICS/PICS-FAQ-980126.html
[55] Pierre Van Ommeslaghe, L'autorégulation. Rapport de synthèse, in: *L'autorégulation*, Actes du Colloque organisé par l'A.D.Br. et le Centre de droit privé de l'Université libre de Bruxelles le 16 décembre 1992, Bruxelles, Ed. Buylant, 1995, pp. 233-274.

voluntary norms which are developed and accepted by those who participate in a determined (specific) activity."[56]

Our *Corpus* - Different Styles

We have gathered some 15 documents - codes or rules - which may be relatively well recognized as self-regulatory instruments of governance for the Internet to which we joined the 30 IFIP Codes that we had analyzed before.[57] Our collection shows the extreme diversity of the material which comes under the label 'self-regulation'. We tried to classify the documents according to the Van Ommeslaghe's classification but we were obliged to consider it as inapplicable.[58] The present list is more classified on themes or names.

The 'Ten Commandments' and the Netiquette rules

- The Ten Commandments of Computer Ethics, by the Computer Ethics Institute (CEI), Washington, D.C.; published in many places.[59]
- Suggestion of Netiquette - Core Rules of Netiquette, Virginia Shea.[60]
- The Net: User Guidelines and Netiquette, by Arlene H. Rinaldi.[61]
- Charter and Guidelines for news.admin.net-abuse.announce, Source: Newsgroups: news.admin.net-abuse.announce, 11 April 1995.
- One planet, One Net: Principles for the Internet Era, CPSR (Computer Professionals for Social Responsibility): still under discussion.[62] (not analyzed)

Charters

- Cyberspace and the American Dream: A Magna Carta for the Knowledge Age, 1994, published by the Progress and Freedom Foundation (PFF).[63]
- Online Magna Charta, Charta of Freedom for Information and Communication, 'The Wartburg Charta', 1997.[64]
- The Intergovernmental Information Technology Leadership Consortium (Council for Excellence in Government) - Draft - Consortium Charter, 1997.[65]

---

[56] Pierre Trudel, Les effets juridiques de l'autoréglementation, in: *Revue de Droit de l'Université de Sherbrooke*, 1989, vol. 19, nr. 2, p. 251, quoted by Olivier Hance, L'évolution de l'auto-réglementation dans les réseaux informatiques: Eléments pour la construction d'un modèle théorique, in: *Journal de Réflexion sur l'Informatique*, Namur, Août 1994, Nr. 31, pp. 25-31.

[57] J. Berleur and Marie d'Udekem-Gevers, Codes of Ethics Within IFIP and Other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., Chapman & Hall, 1996, pp. 3-41.

[58] Pierre Van Ommeslaghe, L'autorégulation. Rapport de synthèse, art. cit. pp. 251 ff.

[59] See for instance: http://www.fau.edu/rinaldi.net/index.htm (July 1998)

[60] Virginia Shea, *Netiquette*, San Francisco: Albion Books, 1994 (See: *EDUCOM Review*, Vol. 29, Nr. 5, September/October 1994, pp. 58-62). See also: http://www.educom.edu/web/pubs/review/reviewArticles/29558.html (July 1998)

[61] http://www.fau.edu/rinaldi.net/index.htm (July 1998)

[62] In: *CPSR Newsletter*, Volume 15, N°4, Fall 1997.
See also: http://www.cpsr.org/dox/program/nii/onenet.html (July 1998)

[63] http://www.pff.org/position.html (July 1998)

[64] http://www.lipsia.de/charta/ (July 1998)

[65] http://www.excelgov.org/techcon/charter.htm (July 1998)

Codes of Ethics and Conduct

- Codes (Standards/Guidelines) of Ethics (Practice/Conduct) of IFIP Computer Societies.[66]

ISPs', SPA's Codes, 'Virtual communities' rules and others
Codes of ISPs' (Internet Service Providers) Associations

- Internet Service Providers Association (ISPA-UK), Code of Practice, 1996.[67]
- Internet Service Providers Association (ISPA-Belgium), Code of Conduct, 1998.[68]
- Canadian Association of Internet Providers (CAIP), 1997.[69]
- La Charte française de l'Internet, Proposition de Charte de l'Internet, Règles et usages des acteurs de l'Internet en France, 1997.[70]
- La Charte de l'Internet proposée par la France à l'OCDE, Proposition française présentée à l'OCDE pour une Charte de coopération internationale sur Internet, 23 octobre 1996.[71] (not analyzed)

'Virtual Communities'

- JANET Acceptable Use Policy, 1995.[72]
- GeoCities Members Guidelines, and particularly GeoCities Page Content Guidelines and Member Terms of Service, 1998.[73]

Others

- US SPA's (Software Publishers Association) Guidelines for Copyright Protection (previously called 'ISP Code of Conduct'), 1997.[74]
- International Chamber of Commerce, Guidelines for ethical advertising on the Internet, 1998.[75]

Most of them are short, maximum 2 A4 pages; but some are shorter than others; 10 commandments, 10 rules of Netiquette, 7 principles for the Internet era. Symbolic figures! And sometimes one stresses that it must be a 'portable' regulation: CPSR doesn't hesitate to launch its idea 'One planet, one net' on a book marker! It seems that that the shortness is a characteristic of such kind of documents, except when they are 'codes of practice'. But this shortness has, at least, to be combined with the content density!

---

66 J. Berleur and Marie d'Udekem-Gevers, Codes of Ethics Within IFIP and Other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., op. cit.
67 http://www.ispa.org.uk/codenew.html (July 1998)
68 http://www.ispa.be (July 1998)
69 http://www.caip.ca/caipcode.htm (July 1998)
70 http://www.planete.net/code-internet/ (July 1998) (Translation "Proposition for an Internet charter, Rules and Courtesies of the Actors of the Internet in France, 1997", done by Dr. Victoria Steinberg, Foreign Languages Department, University of Tennessee, Chattanooga, USA).
71 http://www.telecom.gouv.fr/francais/activ/techno/charteint.htm (July 1998)
72 http://www.ja.net/documents/use.html (July 1998)
73 http://www.geocities.com/members/guidelines/ (July 1998)
74 http://www.eff.org/pub/Legal/Cases/SPA_cases/spa_revised_isp.code (July 1998)
75 http://www.iccwbo.org/Commissions/Marketing/Internet_Guidelines.html (July 1998)

A tentative analysis

The 'Ten Commandments' and the Netiquette rules

The first series of texts is a mix of prevention against what is called computer crime (for the *Ten Commandments*) and of kindness and fairness (for the *Netiquette* rules). Many of the rules governing Newsgroups, for instance the 'Charter for news.admin.net-abuse.announce', are worth being mentioned since they make explicit what is considered as "net-abuse", and which is spelled out, at least partially, in terms similar to those used in computer crime laws.[76]

The categories of computer crime which were adopted by the Council of Europe in 1990 may fix our attention and cover the majority of the topics here suggested.[77] The Council of Europe recommended to have a *Minimum List*, which includes computer related fraud, computer related forgery, damage to computer data or programmes, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer programme, unauthorized reproduction of a topography, and an *Optional List* covering alteration of computer data or programmes, computer espionage, unauthorized use of a computer, and unauthorized use of a protected computer programme.

The Charters

'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age' is a manifesto of the Progress and Freedom Foundation (PFF), in the spirit of the third wave of the Tofflers.[78] If we mention this 'Carta', it is only to notice the hot issues as they are seen by certain zealous propagandists: property rights necessary for the market, infrastructure ownership, dynamic competition on the Cyberspace marketplace and Schumpeter's 'creative destruction' with its winners and losers, customized and actionable knowledge for the Knowledge Age, hackers "vital for economic growth and trade leadership", ...

The 'Online Magna Charta, Charta of Freedom for Information and Communication, The Wartburg Charta' (1997), is no more than the previous one, a 'Charter'. It is a protesting reaction of Netizens when the US CompuServe provider blocked the access to 200 discussion fora under judiciary inquiry, in November 1995. It is a claim to the right to free speech and the freedom of opinion, information and communication, the right to 'a virtual home'.

The last 'charter' here mentioned is the 'Intergovernmental Information Technology Leadership Consortium Charter' which again does not fit into that category and is more a self-satisfactory statement promoting its own quality in the delivery of government services, in the economic growth, and in the citizen participation at all levels of the process of governance.

---

[76] I was told, in April 1998, by the former moderator, that this group does not exist anymore.

[77] Council of Europe, Computer-Related Crime, Recommendation N° R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg, 1990. See also : Jay Bloombecker, Simplifying the US State and Federal Computer Crime Law Maze, in: *Transnational Data and Communications Report*, September/October 1994, pp. 6-8.

[78] Alvin and Heidi Toffler, *Creating a new civilization. The politics of the third wave*, Foreword by Newt Gingrich, Turner Publishing, Inc., Atlanta, 1995.

Codes of Ethics and Conduct

Codes of Ethics and/or Conduct of many computer societies, such as in IFIP, are not specific to the Internet, but their content is rather frequent in such a kind of self-regulation and so worth noticing.

The 'fields of reference' which have been considered by at least one third of the 30 codes of the IFIP national member societies which we have examined are as follows :

- Respect for the interests or rights of the people involved, for the prestige of the profession, for the interests or rights of the public, for the welfare, health of the public, and for the quality of life;
- Conscientiousness and honesty, acceptance of responsibility and integrity, respect for requirements or contracts or agreements, conscientious work, professional development and training , competence, effectiveness and work quality;
- Confidentiality, privacy in general and respect for property rights;
- Flow of information to involved parties, and information to the public;
- Respect for the code, for the law, and for IT and professional standards.

ISPs', SPA's Codes, 'Virtual communities' rules and others

Our collection of self-regulatory documents still include 4 Codes of Internet service providers associations, 2 'virtual communities' rules, 1 Software publishers association Guidelines for Copyright protection, and 1 International Chamber of Commerce Guidelines for ethical advertising on the Internet.

Codes of ISPs' Associations

The 'French Proposal of an Internet Charter' must be included in the category of ISPs' codes, more than in the charters' category. On the opposite, the 'US SPA's Guidelines for Copyright protection', although it was called earlier 'ISP Code of conduct', will be mentioned in our last category 'Others'. The French proposal - still a draft - is the most complete one, and also the longest: it is more than 12 pages long whilst the others are generally 2 pages. It seems also that in Europe, at least among the 10 EuroISPA members, there are only 2 having presently a code.[79] So, our collection contains, first, 4 codes of ISPs' Association: two Europeans (UK and Belgium), one Canadian, and the French draft.

The comparison regarding the people concerned and the country does not reveal great mysteries: the members of the association and the country where it is located! Let us just mention the CAIP's Code which stipulates that "it will cooperate with international organizations and law enforcement authorities ..." Procedures for enforcement are not very strong, and the commitment for reporting is weak.

As the topics are concerned, at the risk to be regarded as nationalist, let us take the most recent code, from Belgium. Except the French draft, it is the most complete and it includes most of the items of the others. It includes general commercial clauses insisting on legality and sincerity (services, products or advertising material), honesty (with clients; inform them of this existing code), personal data protection, publicity, and right information on prices.

[79] http://www.euroispa.org/coc.html (July 1998) A recent update (August 1999) brought the number of codes to 6, for 11 members.

These commercial clauses are spelled out in similar terms in the UK and Canadian documents. There are also special clauses on crime in the Belgian code: pay special attention for fighting against 'illegal or dubious material', but no capacity for controlling everything; they will assist public authorities, have special email address for complaints, and inform hotline about every illegal or harmful transaction: sex, pornography, paedophilia, racism, xenophobia, genocide denial, provocation or encouragement to criminal act, criminal association, gambling and lottery, drugs ("list is not closed"), ...

What the draft French Internet Charter seems to bring new in the scope is the creation of what is called an 'Internet Council', "an independent and unique body for self-regulation and mediation." Its roles will include information and advice to actors and users, process of complaints, and participation in the international cooperation. The role is a bit larger than the ISPs associations. The Canadian association of Internet providers code resembles to the others, but one specific clause is worth mentioning: "CAIP members are committed to *public education* about Internet issues and technology (f.i. how to assign liability for content and network abuse, and help all Canadians understand the options available to all stakeholders).

'Virtual Communities'

JANET is the well known UK education and research community network. We do not have here a real document of 'self-regulation', but an 'acceptable use policy', as it is most of the time called in Anglo-Saxon world.[80] But it contains rules which are typical not only of such academic community, but of many others: privacy protection, no harmful material, no computer crime (unauthorized access, no defaming, no infringement of copyright, corrupting or destroying other users' data, disrupting the work of others, other misuse of JANET or networked resources, such as the introduction of 'viruses', etc.), and also some rules of usual Netiquette such as: "Do not use JANET for deliberate activities such as wasting staff effort or networked resources, (...) in a way that denies service to others, ...

JANET acceptable use policy is a very temperate and sober community code when compared to the GeoCities Guidelines. GeoCities could be classified among the ISP, but it looks also like a big community - 'more than 2 million GeoCitizens' from all the world, located in some 40 'Neighborhoods' - common interest communities.

Regarding the illegal or harmful material, the rules do not differ very much from what we have read until now. "Refrain from using free Personal Home Page or GeoCities Chat and Forum session for: material containing nudity or pornographic material; material grossly offensive to the online community, including blatant expressions of bigotry, prejudice, racism, hatred, or profanity; material that exploits children under 18 years of age; restricted or password-only access pages, or hidden pages or images (...)."

There are other interesting clauses. "Refrain from: instructional information about illegal activities, physical harm or injury against any group or individual, or any act of cruelty to animals; defaming any person or group; for commercial purposes (...); using page (or directory) as storage for remote loading or as a door or signpost to another home page."

The list includes a clause which is nearly the copy of one from the US SPA Guidelines for Copyright Protection, as we shall see: "refrain from using your home page for acts of

[80] See John W. Corliss, Policies of Acceptable Use at Educational and Research Institutions, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., op. cit. pp. 61-70.

copyright, trademark, patent, trade secret or other intellectual property infringement, including but not limited to offering pirated computer programs or links to such programs, information used to circumvent manufacturer-installed copy-protect devices, including serial or registration numbers for software programs, or any type of cracker utilities (this also includes files which are solely intended for game emulation)."

Then it goes on with: "Refrain from: violating Internet standards for the purpose of promoting your home page; hyperlinking to content not allowed in GeoCities; gathering personally identifiable information for commercial or unlawful purposes; posting or disclosing any personally identifiable information belonging to children. [Kids: For your safety, do not put your real name, address, phone number, e-mail or other information like that on your webpage or give it to strangers.]"

This rather long list is completed by an explicit sentence: "GeoCities does not actively monitor the content of Personal Home Pages but will investigate complaints of violation of these guidelines.

Others

We have finally collected two specific Guidelines, because they are 'sectoral' and linked to the Internet.

The first one, the Guidelines of the US SPA are in a way curious, because they have been developed by SPA for server operators who do not seem "to participate in the activity", to quote the definition of self-regulation by Pierre Trudel: the real actors on whom self-regulation is here imposed are the subscribers. The question was very controversial: SPA suited small ISPs, but the case was dropped.[81] Amusingly, when writing this paper, we found a 'Hotnews' 'Dutch ISPs Refuse to Squeal on Software Pirates': "Dutch Internet service providers World Access/Planet Internet, XS4All and Euronet have said they will not check their systems for advertisements by software pirates, even though the Business Software Alliance (BSA), an organization of software distributors, holds the providers responsible for the majority of software piracy over the Internet in the Netherlands."[82] The subject is surely hot and on the agenda of many organizations, as well as the general problem of intellectual property right.[83]

The Guidelines of ICC on Advertising and Marketing on the Internet are surely worth seeing, since we are here also in a very sensitive domain. The privacy protectors and the anti-spamming leagues will surely react to such guidelines. Problems which are here treated are: legality, honesty, social responsibility, clear information to the users, use of personal data (with a right to opt-out), right to access his/her own data, no unsolicited commercial message (when indicated), special clauses for advertising to children, and respect for potential audiences: pornography, violence, racism, sexism, ...

---

[81] Electronic Frontier Foundation (EFF), Software Publishers Association vs. ISPs - suits dropped, 'Code of Conduct' critiqued [Dec. 6, 1996], http://www.eff.org/pub/Censorship/HTML/hot.html#cda (July 1998)

[82] Dutch ISPs Refuse to Squeal on Software Pirates, http://www.best.be/hotnews.CFM?DPPRESS=743 (July 10, 1998).

[83] Robin Mansell and W. Edward Steinmueller, Intellectual Property Rights: Competing Interests on the Internet, in *Communications and Stragegies*, IDATE-Montpellier, n° 30, 2nd Quarter 1998, pp. 173-197.

Self-Regulation : First Results

What could be considered in some way as a tedious analysis reveals repetitions and a rather convergent final result. Some 'issues', if not 'categories', emerge:

- fairness and kindness: Netiquette, ISPs, ICC
- respect, honesty, competence, sincerity, right information, ...: Codes, ISPs, ICC
- privacy (and deriving rights such as right to know about his/her own data): nearly all
- computer crime: Ten Commandments, Net-abuse administration, Virtual communities, Janet, ICC
- intellectual property right, copyright, trademark, patent, ...: GeoCities, PFF Carta, US SPA
- free speech, right to information and communication: Wartburg, French Charta
- illegal, dubious, harmful material: ISPs, GeoCities, ICC
- etc.

We must say our disappointment about the other features of our analysis: people involved and concerned, places where self-regulation is applicable, rules for enforcement. It looks like the reign of vagueness.

About enforcement and procedures, without doubt, we are in a relatively recent situation: the texts we have examined do not go back further than 1994-1995. Moreover, as most often, organizations do not like to report on complaints which could reveal a weakness in their security system, for instance. This means that we shall have difficulties to evaluate the functioning of the procedures, when they exist. We can just regret that some organizations explicitly state that they cannot commit themselves in controlling what they have on their servers.

This means that, if the topics and issues appear relatively clearly, the main concern, in terms of governance, reveals that we have to make further decisive progress. We could also add that the real problem with such codes is not that they exist, but that in some pages they try to cover what the law needs many well crafted numerous articles for!

The Internet : The Role of the law. Two new legal issues

The problem of the regulation of the Internet could be solved in different ways. The law is one of them. But, because of the particular nature of this new medium, and especially the fact that it allows to exercise a lot of different fundamental freedoms (like the freedom of expression, the freedom of information, etc.) important ethical choices have to be made in order to conciliate all interests.

To give a better idea of these ethical choices, we will analyze the regulation chosen in two different topics: the protection of privacy and the protection of copyrights.

The Protection of Privacy

Different choices have been made in USA and in the European Union. These choices could be explained in an economical point of view. On the one hand, we have the United States of America whose economical tendency is liberalism, which means that the market

should be let free to solve as much issues as possible. On the other, the European Union which has chosen to regulate.

The Choice Made in the United States

In July 1997 the Clinton's Administration published a paper entitled : "Framework for global electronic commerce" in which different principles were developed from which three are relevant for our purpose.[84]

First of all "the private sector should lead" and consequently, the government will encourage industry self-regulation and the private sector participation in the making of standards or collective agreements. Secondly, "Governments should avoid undue restrictions on electronic commerce". Thirdly, "where governmental involvement is needed, its aim should be to support predictable, minimalist, consistent and simple legal environment for commerce" which means that the Governments plans to set up only decentralized or contractual model of law rather than a legal environment base "on top-down regulation".

The choice of the federal administration was clearly in favour of self-regulation. But in 1998, a poll taken by *Business Week* revealed that a lot of citizens refused to go online because of privacy concerns. The efforts of the companies to set up adequate privacy protection seemed not to be convincing. It is why in July 1998, the Federal Trade Commission made the following declaration : "Unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of the year, additional governmental authority would be appropriate and necessary."[85]

One month later, the Federal Trade Commission charged the company GeoCities, one of the most popular sites on the World Wide Web, of misrepresenting the purposes for which it was collecting personal identifying information from children and adults.[86] A few days later, the GeoCities' shares lost more than 20 percents. And that can be considered as a mirror of the growing awareness "that Internet privacy protection can have an enormous impact on a company's bottom line."[87]

The Choice Made in Europe

The legal policy in the European Union has clearly been a regulatory policy. A general directive was issued in 1995 and set up different rights such as the right of access or the right to object.[88]

The general directive speaks also about the self-regulation, and one article is really interesting to understand the place the self-regulation should take (mostly the Codes of Conduct). The article provides that: "The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account

---

84 http://www.ecommerce.gov/framewrk.htm

85 http://www.wired.com/news/news/politics/privacy/story/13895.html

86 http://www.ftc.gov/opa/1998/9808/geocitie.htm

87 Reuters 17/08/1998.

88 Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31 (hereinafter general directive). (Right of access: see article 12; right to object, see article 14)

of the specific features of the various sectors".[89] The Commission seemed to consider the Code of Conduct only as a supplement to the law, nothing more.

This article also creates the possibility for trade associations and other bodies representing other categories of controllers to submit the code they have drawn up to the opinion of the national authority. The Directive suggests that the Member States should make provision for this authority to ascertain whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to the Directive.[90]

But at this point of the debate we have only compared the choice made in the United States and in the European Union. It would be interesting to join them face to face. The first feature of this confrontation is the article 25 of the European Directive, which provides that : "the member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the directive, the third country in question ensures *an adequate level of protection*" the second paragraph of the article gives more details about the assessment of the level of protection saying that "particular considerations shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country" . At that moment the level of protection in the USA has been considered as inadequate. But the problem is that the Directive will have direct effect in October 1998. Therefore, US and EU officials are meeting to discuss ways of avoiding a potential impediment to electronic commerce trading between the two continents.

The problem is now: How to solve this conflict? Because both parties will stay on their positions. A solution could may be found in the article 26.2 of the European Directive which creates an exception where the controllers adduce adequate safeguards with respect for the protection of privacy specifying that such safeguards may in particular result from appropriate contractual clauses. So the solution could be the creation of standard contracts which would be used for each transborder data flows to third countries.

In 1997, the Commission issued a second Directive on privacy, particularly focused on the telecommunications.[91] This Directive gives several rights to the consumer with regards to the use of telecommunications, which can be made with a commercial purpose. For example, article 10 says that a subscriber must be provided, free of charges, with the possibility to stop automatic call forwarding by a third party to his or her terminal. These calling systems include the fax transmission, so doing; the Directive provides a solution to the problem of commercial harassment.

In conclusion, we can observe that the process used in the European Union is exactly the contrary to the one adopted in the USA. In a first step, the Clinton's Administration had given the priority to the self-regulation. But recently they have faced different abuses of the market due to the lack of regulation. They probably will come to the decision to write a law. But something remains surprising. It is the fact that the financial market has started to consider the

---

[89] Article 27 §1.
[90] Article 27 2 al. 2.
[91] Directive 97/66/EC of the European Parliament and of the Council of the 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ 1998 L24/1.

protection of Privacy as a criterion to evaluate a company carrying business in electronic commerce. Therefore it could be considered that a change of the way to regulate privacy in the USA would be the result of an economical choice more than of an ethical one.

On the opposite, the European union started directly with a directive whose purpose was, among others, to ensure a high level of protection to the right recognized in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[92] The choice of the Commission was to enforce that ethical value with a Directive but with a possibility to use self-regulation as a complement. It could be asked which of those two process is the most efficient. The answer could be none of them because they both try to stay between the over-regulation and the legal emptiness knowing that each of them is really close to the farthest utmost point.

The Protection of Copyrights, the Competition between Law and Technology

Opposite to the privacy domain, the field of copyright has been regulated strongly in the USA and in the European Union. The ethical choice has been done in favour of a real protection of the rightholders. But, new questions arise now with the coming out of technical systems of protection. These systems are capable of managing the access to the works.

Furthermore, a proposal for Directive on copyright and related rights in the information society would require Member States "to provide adequate legal protection against any activities, including the manufacture or distribution of devices or the performance of services, which would enable or facilitate the circumvention without authority of effective technological measures designed to protect copyrights and related rights."[93]

This position of the Commission is the starting point of different considerations. First of all, the danger is that such an Electronic Copyright Management System (ECMS) could manage the access to works, which are not protected anymore by copyrights. Which might, according to different authors, "result in appropriation of public domain, which has to remain freely accessible to the general public."[94]

Furthermore, the technology seems to offer a better protection than the copyrights themselves, and one could ask if that technology will not cause the "death of the copyrights" in the virtual world? This remark could be found excessive but something is certain, the spirit of the protection by the copyright is changing. Before the protection was an *a posteriori* one the copyright was invoked after the infringement. Now, to prevent the ECMS to violate the right of information of the public, it becomes necessary to decide *a priori* which works are protected and which are not.

It is interesting to note that the emergence of the new information technologies could be regulated by three different instruments : first of all the law which has the advantage to be effective and possibly enforced by a court order. But, the law has also weaknesses such as its

---

92 Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31, whereas (10).

93 http://europa.eu.int/comm/dg15/en/intprop/intprop/1100.htm (comments on article 6).

94 Severine Dusollier, "Legal aspects of Electronic Rights Management Systems (ERMS)", p.6. (to be published)

general character which does not help when practical details have to be solved. The second way to regulate is the self-regulation. This way is generally chosen in sectors where the connections between the actors are very strong like for example in the financial world. The self-regulation has an effectiveness when it is the commercial advantage of the actors to comply with. If it is not, it is really difficult to imagine that such a regulation could have any possibility to be enforced.

A third and new way to regulate is the technology which can integrate the requirements of the law and enforce them by technological ways. The danger resides in the following question: "Who is entitled to write the standards governing the machine?" Because if only an oligarchy decides of the rules to be implemented by the machine they give to the law their own interpretation and sometimes bypass completely the philosophy of the rule. If, like some authors said "the answer to the machine is the machine", the user has to remain the master and may not become the slave …

Conclusion

We may be short. Two main conclusions are obvious and could be considered at least as a provisional agreement and allow us to focus on newer issues.

First, there is a general agreement on the ethical issues as they are covered either by the technical means, or by self-regulation, and partially at least by the law. Privacy (and deriving rights such as right to know about his/her own data); computer crime; intellectual property right, copyright, trademark, patent; free speech, right to information and communication; fight against hatred speech, racism, and against sectarianism; pornographic, illegal, dubious or harmful material; etc. All these issues are rather frequently mentioned.

Second, within the ways those issues are solved, or at least approached, there are also ethical choices to be clarified. Who is setting the labeling vocabulary and the criteria for assigning labels, who is rating the web sites ? Who is establishing the filtering criteria ? Those questions that we have raised about the technical means show us that there are social and ethical choices. As we have seen there are also ethical and social choices in the ways privacy may, for instance, be protected. Or it may be that a technical choice deregulates the legal means - what is also an ethical and social choice!

Ethics is not out of scope in the governance of the Internet, and plays its role. Therefore, as it was suggested during the recent IFIP-TC9 international conference on Human Choice and computers, we must "care about the net" instead of fearing it, play a role in a more face-to-face way (E. Lévinas); in other words we must devote ourselves to "netmaking" more than to "networking" and we have to *create* an ethical community. Others were suggesting to strive to develop cross-cultural values to the service of great causes such as reducing violence and promoting peace. Or, to develop principles of governance which include social responsibility. Social dialogue, cultural dialogue, social responsibility are not only important words: they must be in the forefront of our action to create human networks in the age of globalization.

APPENDIX C

CPSR DOCUMENT - "One Planet, One Net: Principles for the Internet Era" (reprinted below)

http://www.cpsr.org/program/nii/onenet.html : August 1998 (Still the same in September 1999)

One Planet, One Net: Principles for the Internet Era

The emergence of the Internet presents enormous opportunities and challenges to humanity. If we work to preserve its openness and diversity, we can ensure that the Net will be used to change the human condition for the better, and can prevent or mitigate its less desirable consequences.

The Internet is more than wires, computers, software, modems, routers, standards, and the applications that use them. It even encompasses more than text and pictures, and the audio and video that are rapidly joining those media. The Net is also the collective knowledge and experience of countless communities, each with its own modes of interaction, languages of discourse, and forms of cultural expression.

Certain principles must be understood and respected as we consider the more detailed daily questions that arise in the administration or governance of the Net. We believe that among these principles are the following:

1. The Net links us all together.
2. The Net must be open and available to all.
3. Net users have the right to communicate.
4. Net users have the right to privacy.
5. People are the Net's stewards, not its owners.
6. Administration of the Net should be open and inclusive.
7. The Net should reflect human diversity, not homogenize it.

The continuing evolution of the Internet presents both opportunities and challenges. We must work to counter the political, economic, social, and technical forces that work against these principles and threaten the promise of open communication on the Internet. Failure to do so may lead to a future in which the Internet is homogenized, commercialized, and regulated to the extent that it fails to meet its fundamental mission - to serve as a medium for maximizing human potential through communication.

1. The Net links us all together

The nature of people and their use of networking technology provides a strong natural drive towards universal interconnection. Because the flow of information on the Net transcends national boundaries, any restrictions within a single country may act to limit the freedom of those in other countries as well.

The true value of the Internet is found in people, not in technology. Since each new user increases the value of the Net for all, the potential of the Net will only be reached when all who desire can openly and freely use the Net.

2. The Net must be open and available to all

The Net should be available to all who wish to use it, regardless of economic, social, political, linguistic, or cultural differences or abilities. We must work to ensure that all people have the access to the technology, education, and support necessary for constructive, active participation. People in all walks of life should have as much right to send and receive information as do the affluent and powerful.

3. Net users have the right to communicate

Every use of the Net is inherently an exercise of freedom of speech, to be restricted only at great peril to human liberty. The right to communicate includes the right to participate in communication through interacting, organizing, petitioning, mobilizing, assembling, collaborating, buying and selling, sharing, and publishing.

The Net offers great promise as a means of increasing global commerce and collaboration among businesses, but restrictions on information exchange would eviscerate that promise.

4. Net users have the right to privacy

Without assurances of appropriate privacy, users of the Net will not communicate and participate in a meaningful manner.

The right to privacy includes at least three forms:

- Individual Network users should control the collection, use, and dissemination of personal data about themselves, including financial and demographic information.
- Network users should be free to use any available technical measures to help ensure the privacy of all aspects of their communications.
- Individuals have the right to control who they communicate with, and how they conduct that communication. The privacy implied by the decision to not communicate must be respected.

5. People are the Net's stewards, not its owners

Those who want to reap the benefits of the shared global Net are obliged to respect the rights of others who may wish to use the Net in different ways. We must work to preserve the free and open nature of the current Internet as a fragile resource that must be enriched and passed on to our children.

Individual pieces of the Net, such as wires, routers, and servers, have owners whose economic rights and interests must be respected. However, just as the ecosystem in which we live cannot be owned, the Net itself is not owned by anyone.

6. Administration of the Net should be open and inclusive

The Net should be administered in an open, inclusive, and democratic manner for the betterment of humanity. The needs of all who are affected by the Internet - including current users, future users, and those who are unable to or choose not to be users - must be considered when making technical, social, political, and economic decisions regarding the operations of the Internet.

Although administration of the Net should aim to enhance its efficiency, availability, and security, it should not do so at the cost of discouraging use of the Net. Administration should facilitate and encourage greater use of the Net for communication, rather than inhibit it in any way.

7. The Net should reflect human diversity, not homogenize it

The Net has the potential to be as varied and multi-cultural as life itself. It can facilitate dialogue between communities and individuals that might previously not have encountered each other in a dozen lifetimes. However, the Net could also become a homogenizing force, working to suppress diversity in favor of a bland globalism.

Individuals and communities should not be forced to forego local cultures and traditions in order to participate in the Net. In order to preserve the vitality that comes with a diversity of viewpoints, we should work toward helping the whole world participate as equals.