

"Ethical dimensions of the information society: Ethics and human rights in the information society"

Strasbourg, September 13 and 14, 2007

Dr. Jon Thorhallsson

President CECUA

Professor, University of Iceland (former)

Ladies and Gentlemen,

I would like to start by looking back in history.

In 1998 CECUA and its Partners held a conference in Brussels called "The Citizen and the Global Information Society"¹. This Conference focused on the opportunities and concerns as experienced or perceived by the citizens. CECUA and Partners had expected most of the Conference discussion to be devoted to opportunities. But as it turned out, the discussion focused on concerns instead.

A major finding of this conference was that above all, the Citizen lacks trust and feels vulnerable in the global information society, and that current legislation does not give the citizen sufficient security, privacy or protection when the Internet is used either for leisure or commercial purposes.

The discussion in the workgroups revealed that the Citizen's perception was that the concerns outweighed the opportunities offered by the Global Information Society. Technology was advancing at a bewildering pace and many citizens and SMEs did not have the resources to cope effectively with these changes. Further, there were a great confusion with "over featured" products which are not user friendly and become out of date quickly by "enforced" obsolescence. Similarly, there were a high level of mistrust by citizens and SMEs of information and service providers.

The Conference decided to explore the possibility of protecting Citizens' Rights by formulating a draft set of Articles, a Bill of Rights for the Citizens of the Information Society. There was a wide consensus on this with the hope that basic Rights will reduce the need for specific technically oriented legislation (which generally becomes out-of-date rapidly). The proposed Bill of Rights consists of a Preamble followed by 9 articles. Due to shortness of time I can only mention the article headings²:

1. DIGNITY, 2. FREEDOM of PERSONAL DEVELOPMENT, 3. FREEDOM of COMMUNICATION, 4. CULTURAL PRESERVATION, 5. RIGHT of ACCESS, 6. RIGHT for RELIABLE and FUNCTIONING SERVICES, 7. NETIQUETTE, 8 RIGHT for ACCURATE and UNDERSTANDABLE CHARGING, 9 RIGHT for REDRESS

The Bill of Rights has been presented and discussed widely at the level of the European Parliament, European Commission, the Committee of the Regions and at numerous conferences and seminars, e.g. Identity, trust and confidence, security in the digital world, Paris Conference, February 12, 2004, Foresight of the Internet, Castle of Namur International Conference, March 4, 2005, Internet Governance in the OSCE Region, Paris Workshop, December 15, 2006 and many many more.

It has also been used to test EU directives. Interestingly some Directives have failed the test.

Nine (9) years ago is by no means long time ago but let me remind you that in 1998 the Internet was in its infancy and relatively few people had access to it, mostly professional people who were informed users. They were using Windows 97 and Netscape. This was the beginning of the Internet bubble. And since then the bubble has expanded and expanded. But has anything really changed? CECUA's own research has shown that the citizens have the same concerns as before now 9 years later³.

Therefore, I am very grateful to the French Commission for UNESCO for organizing this conference and inviting me to participate in the discussions. To me this is a long awaited follow up of the 1998 conference in Brussels.

I will contribute to the discussions using the background of the 1998 Conference and what we have learned since.

This Conference's three main pillars are: (i) analysis of the opportunities offered by Information and Communication Technologies (ICTs); (ii) side-effects, negative impacts and possible conflicts of interest, and (iii) recommendations with the aim of contributing to Internet governance founded on the involvement of all stakeholders and the sharing of responsibilities and is indeed an appropriate follow up to the conference from 1998.

In 1998 the Internet was very new and a privilege of a few. Our Conference was looking toward the future without past experience to guide us. Now the situation is different. We have experience and it has developed rapidly. I come from a country, Iceland, where most people today have access to the Internet and there is a PC in almost every household. In 1998 the Internet was very much about technology. Today the Internet is firstly about people and secondly about technology. Advances in technology are moving at a racing speed. But people take their time to change. People want evolution, they do not want revolution.

For most people Internet is a tool for getting information (surfing), communications (email) and shopping (eCommerce). To them Internet is like any other utility, water, electricity, television and telephone. People are concerned about ease of access, ease of use and safety of use and of course costs. And they carry their experiences with those "classical" utilities over to the Internet. People perceive the Internet as the merger of many utility services like the telephone, telegram, post and mail-order catalogue. And they expect the same safety of use as they have are used to. They expect evolution. But what are they getting? Revolution?

Yes, in a way they are getting a revolution and they are confused. Internet with its many possibilities has spurred many thinkers to see it as the incarnation of "Cyberspace", a term coined by William Gibson in his fantasy novel Neuromancer to describe the "world" of computers, and the society that gathers around them⁴. They feel that Gibson's fantasy of a world of connected computers has moved into a present reality in the form of the **Internet**. In cyberspace people "exist" in the ether--you meet them electronically, in disembodied, faceless form within this new form of social interaction. This is all very well. But to overwhelming majority of people this is nothing but sheer nonsense.

As a theoretician I am the last person to object to theoretical speculations in the hope that one day something practical will come out of it. However, those speculations and reflections have confused the Internet issue dramatically. Instead of facing and solving physical space real Internet problems people are exploring

Cyberspace. It is sort of like the "New brave World" some people are still waiting for. But in the meantime life goes on. We are all living in physical space, not in Cyberspace. Physical space has developed over thousands of years with its cultures, traditions, laws and regulations. We cannot simply abandon those and enter theoretical Cyberspace. All this has left many people confused and lost. People like to know where they stand. We live in physical space and we will continue living there and die there. And we will certainly not suddenly throw our cultures and rights overboard and climb aboard a fictitious Cyberspace that we do not really understand. But it is easier to talk about Cyberspace than to solve the problems of the physical space Internet?

Unfortunately my time is very limited and I will limit my discussion to a few issues starting with cultural and human rights issues and refer specifically to "Bill of Rights" Article 4, **CULTURAL PRESERVATION**

"The Citizen shall have the right to communicate in his native tongue, and to work and conduct official business in an Official language of the sovereign state of his residence."

What about the Internet? Does Internet offer this right to us? Unfortunately NO.

The Internet was conceived in the United States and is technologically brilliant. Its English language origins have been both a blessing but also a curse. Blessing because English has become the "common denominator" of world languages. But the Internet is only the backbone and most users see little of it. When people talk about the Internet what they really mean is the World Wide Web or short the web. People surf the web, use web email and do their shopping on the web. (Interestingly the web came originally from Europe (CERN) although most people perceive it as USA one.) The web content is multi national and multilingual. Originally most content was in English but more and more non English content is appearing. That is fine. No problem.

But to get to the web the user has to go through the Internet. Internet is so to speak the gatekeeper for the web. And as a good gatekeeper the Internet asks for identification. And that is where the English language curse begins. The identification has to be in English, English letters only or STAY OUT. The identification consists of 2 parts, a "domain" part and an "address part", both in English letters, NO EXCEPTION. To get his or her identification the user has to go through a process. At the very beginning the user has to select a so-called Internet service provider who provides the "domain" and "address" parts. Here is where the user first runs up against the English language dominated Internet. Internet domain names are in English letters **ONLY**. The domain part as such is not really a personal issue. But when it comes to the "address" part it becomes a real personal issue. The natural choice is to use the physical space name as Internet name also. We are given this name by our parents at an early age and it stays with us for the rest of our lives. And when it comes to selecting Internet name everybody likes to see his or her name and it only confuses family and friends if they have to remember two different names, one for physical space and one for the Internet. But to pass the gatekeeper, the user has to rewrite his name using English letters only. English may be fine in theoretical Cyberspace but in physical space we want language and cultural diversity. This is where the Internet fails badly to live up to Bill of Rights.

Responsible for Internet technical administration is a private company, ICANN, in California in USA. And ICANN does not really understand that people would like to use their mother tongue for identification. The past CEO of ICANN called the call for

national language support a “trumped up nationalism” and “anticompetitive”. The present ICANN administration has backed away from this stance but no solution is in sight. ICANN claims that there is a technical solution to the problem of multilingual domains and addresses. But that is all. No plan for implementation has seen light of the day. In the meantime users are forced to select domains and addresses using English letters only. That means killing off any special letters with which European languages are so rich. If users want to use their own names they have to be rewritten using English letters only. The names appear different or mutilated. Take my name as an example. In Icelandic it is Jón Þór Þórhallsson. After “transcribing” it into English it is Jon Thor Thorhallsson. It looks different and it sounds different. I do not feel that it is really my name. Similar situation is with French, Spanish and other languages.

European politicians talk about the European cultural diversity as a part of European richness. But when it comes to identification on the Internet the diversity and the richness ends. This is not only a cultural issue but also a human rights issue. **The user has the right to have his Internet identification in his or her own mother tongue. Any agreement, regulation or co-regulation on Internet Governance has to ensure that the user has this right.**

But there is more involved. The so called address is not a street address. It is the personal identification for the user like our name is. It is given to us by our parents when we are quite young and it stays with us for the rest of our lives. The name is our identification for the authorities, utilities, water, electricity, television and telephone. And it works well. Why should we have a different name in Cyberspace causing confusion to our family and friends who know us by our physical space name? Why reinvent the wheel? We should not reinvent it. Everybody should have the right to use the same name in both spaces, physical and Cyber. However, there is one big problem. While the name we have in physical space is chosen by our parents at their own discretion the names in Cyberspace are a commodity that can be bought and also sold. Many people like to use their physical space name also in Cyberspace. But there is no guaranty it is available. What he or she wants may not be available. Somebody else has got it first. But it may be available for sale? The price depends on the celebrity of the person involved. The more the celebrity the higher the price.

Every person should have the right to his or her first name and surname in Cyberspace. **This is a human rights issue.** The European Union missed a historic opportunity when it introduces dotEU, an opportunity to give every EU citizen the right to get his or her name in European Cyberspace. Instead EU opted for making dotEU a cheap copy of USA's dotCOM. The commodity business model again. This name issue needs to be addressed to bring the 2 spaces closer together, the physical space and Cyberspace, and make Cyberspace much more inviting for people to join the Internet crowd. Incidentally this is also a marketing issue. The more people who decide to go into Cyberspace the more business it brings.

In conclusion Internet does not live up to Bill of Rights Article 9.

In the final part of my presentation I will focus on legal issues including on-line shopping again refer to Bill of Rights.

Bill of Rights Art. 9 RIGHT FOR REDRESS

“The Citizen shall have the access to protection and redress for acts of fraud, corruption of personal data, loss of privacy, and consequential costs arising from errors, bugs or failures of internet services and facilities”.

Earlier I stated that people perceive the Internet as the merger of many utility services like the telephone, telegram, post and mail-order catalogue. On the Internet it goes faster and can all be done from home. But of course they expect the same safety of use as before. We have general laws and specific laws and regulations for each of those services. What about the Internet? We have no law or very limited law at best. But do we really need new laws? Maybe all we need is to amend the laws to adjust them to the new Internet environment? Probably we need both.

From 1998 the Internet criminality has grown exponentially and the legal system and law enforcement system have not been able to cope with it. Internet criminality has moved from being pranks by young people to become a part of organized crime.

What needs to be done? First we have to face it that we have a legal problem in Internet and physical space laws are not always up to par on Internet crime. Secondly we need to face the fact that Internet crime has become a part of organized crime. It is not any more some young people doing pranks on the Internet for fun. Those are professional criminals doing it for profit. And the threat is growing. After recent attacks on the Estonian Government websites Internet crime has entered the political sphere. The people or organizations perpetrating the crimes all live in physical space although they are plying their trade in Internet. They are violating physical space laws and have to be prosecuted under physical space laws.

Thirdly, law is one thing, enforcement of the law is another thing. No use for Internet crime laws if they can not be enforced. To combine law making and enforcement needs international cooperation. Internet crime is a global issue and as long as one country does not sign on to such international cooperation it is no good. Non-signing countries will become the heaven of Internet criminals.

But we also have to do some work at home. We can crack down on local criminals and punish them. For that we need to look at the legal framework. EU member states have been beefing up their legislation also to cover Internet crimes. Those are real crimes costing private persons and companies billions of Euros each year. People are robbed of their savings by identity thieves. And businesses are robbed of billions of Euros each year. This has to be stopped. And persons and businesses have little or no hope of finding the perpetrators and have them prosecuted. This is definitely not satisfying Article 9 of Bill of Rights.

Take for example online shops. Experts⁵ warn of serious security gaps in online shops. They estimate that more than half of all e-business platforms are open to attacks and about 20% have security gaps which allow reading or manipulation of customer data. This is a national issue and must be stopped. Maybe online shops have to be licensed?

Many legal issues need to be clarified. What is the responsibility of Banks offering customers Internet banking and then leave them open to phishing attacks? What is the responsibility of online shops offering goods and services on the Internet and then the customers are robbed? There is a need for EU directive on Internet crime. EU also has to make sure there is no conflict between the Internet crime directive and other directives, e.g. the Data Protection directive. This is homework for the EU. But any EU crime directive can only apply to EU member states. Outside of EU other directives or no directive at all may apply. This is an international issue and in the end an UN issue. But we have to start somewhere and we can start at home.

Our law enforcement agencies are not well prepared for Internet investigations. Combating Internet crimes calls for a new generation of police officers with understanding of the Internet and its possibilities. This is very different from the officer patrolling his beat. Also the courts are ill equipped to deal with Internet cases. Lawyers and judges have to be upgraded also. This transformation will take time and the sooner we begin the better.

Bringing law and order to the Internet includes many stakeholders from users, internet service providers, banks, online shops, police, prosecutors to name some. Every one has to look at his own part and ask what do I have to do. This calls for cooperation between all parties. But I am not sure even with cooperation they can do it alone. Governments have to step in. The role of Government is to protect their citizens and no doubt whatsoever here we are talking about protecting citizens. A key issue is to raise the awareness of Governments to the fact that Internet criminality is a real criminality threatening their citizens and businesses and even Governments as recent example from Estonia shows. Here Internet Government services were attacked and paralyzed for political purposes. This can happen to any government. Governments have been too removed from the Internet criminal scene to really feel it. Now Internet criminality is on their doorstep. That could do it. Because in the end: Internet law and order is the responsibility of Governments. Nobody can take that burden from their shoulders. Governments have to provide the leadership for other stakeholders to follow. And they have to remember that Internet criminality is not a local issue. It is not even a national issue. **INTERNET CRIMINALITY IS A GLOBAL ISSUE.**

In conclusion the Internet is without law and order. It has a long way to go to give the private and corporate citizen the right for redress stated in the Bill of Rights.

CECUA would welcome any discussion on the Bill of Rights. It has served its purpose well in the past and will continue to do so.

¹ The Citizen and the Global Information Society, http://europa.eu.int/ISPO/topics/citizen/i_index.html

² Draft Bill of Rights, www.cecua.org

³ The users: Hostages of the Free Market?, www.cecuaacademy.org

⁴ Neuromancer, William Gibson, 1984

⁵ Integralis warns of security gaps in Online shops", Computerworld.de, 27.09.05

The author wishes to express his sincere thanks to the many CECUA colleagues who have contributed to this presentation, in particular Stuart Goold, CECUA Honorary President, Alain Moscowitz, CECUA Vice President and Friedrich Dittmer, CECUA Deputy Director.