

# Right need rules!

One cannot discuss the concept and creation of an Information Society without people and so any discussion involving people should incorporate their basic human rights.



Paul Maassen  
Hivos, The Netherlands  
p.maassen@hivos.nl

Rights that are valid in the real world are also valid in the 'virtual world'. The Information Society should be based on internationally agreed human rights. This is what Hivos voiced, in 2003, as a recommendation to the European Delegation to the World Summit on the Information Society (WSIS) in Geneva, Switzerland. This recommendation reflected and still reflects our point of view, that one cannot discuss the concept and creation of an Information Society without starting with the atoms of any society: people. As a result, any discussion involving these people should incorporate their basic human rights.

This seems an obvious statement, and many stakeholders also supported the idea of an inclusive Information Society based on human rights, rather than on pure bits and bytes as a focus of the summit. Nevertheless, grand political statements uttered in Geneva do not automatically transform themselves into a better world. Human rights often seem to be the ideal subject to applaud, but not to adhere to.

Internet strengthens the right to freedom of expression by providing individuals across the globe with new means of sharing and accessing information. Despite the continued exclusion of marginalised communities and many people in the developing world, everyone with access can voice his or her opinion and access decision-makers and local politicians through discussion forums, blogs or through e-mail. ICTs as a tool, have potential for enabling democratic participation and for open information sharing. However, it is precisely due to this enormous freedom, that Internet breeds fear. Foremost amongst those are some decision-makers.

Stakeholders, mostly governments, find many reasons to justify Internet regulation (or in some cases - monitoring, censorship or control). These reasons have in common that they are all based on the concept of fear. There is fear of government for its citizens, or fear of citizens for their own governments and other threats like terrorism.

As such, governments in dictatorial states often find ways to limit Internet access in order to prohibit opposing opinions. For example, the Chinese government fears Falung Gong and managed to cut off the tentacles of the Internet, blocking search machines and websites. Freedom of expression and thus information and communication technology pose a threat to repressive governments, undermining their control of 'acceptable' flows of information. As a result, whilst Falun Gong members once used e-mail and websites to successfully reach out, nowadays they prefer payphones, which are harder to trace.

## Privacy versus security

After 9/11, the USA has stepped up its homeland security. For instance, they requested the European Commission (EU) to provide online access to the Passenger Name Record (PNR) of all passengers on flight, from, to or through the USA. The PNR contains data such as name, date of birth, date of reservation, credit card number and phone number. Furthermore, the USA uses the Advanced Passenger Information System (APIS) of the airlines for additional information such as sex, passport number and nationality.

The transfer of this data is regulated and protected by the European privacy law. The Strasbourg Court is examining whether the European Commission, when making the deal, exceeded its powers and acted in breach of EU Data Protection legislation.

According to the report 'Transferring Privacy', the European Commission has 'not assured adequate protection requirements, clear purpose limitation, non-excessive data collection, limited data retention time, and insurance against further transfers beyond the Department of Homeland Security'.

Source: *European Digital Rights* ([www.edri.org/](http://www.edri.org/))

Hivos

Governments, companies and also parents try to filter unwanted content (pornography, racist websites, etc.) just like viruses. They reason that modern technology offers such a bewildering amount of information, that not all users are able to judge the content on its real value. This fear for harmful content has led to self-regulation by industry and to stronger juridical action by governments.

The fear for terrorism has led to massive tracking and registering of Internet behaviour by governments and, non-voluntarily, by Internet Service Providers (ISPs), both in the West and in 'rogue' states. Illustrating the consequences of this fear, Tunisia jailed 9 young Internet users for up to 26 years for just downloading files deemed as dangerous by the authorities. Preparing terrorist acts? Harmful content? Or, just curiosity?

Finally, for fear of their own government, citizens apply self-restriction in sending or finding opinions and information. In such cases, where governments can be perceived as threatening (such as Iran), self-censorship on the Internet is common. Through restricting this free flow of information, the biggest opportunities for an inclusive Information Society are lost.

Some of the described threats are real, some are perceived and some are not more than happy excuses for paranoid governments to control. Either way, they illustrate two dimensions: human rights and fear. One thing is clear that to guarantee the human rights in a new virtual era, these issues cannot be dealt in the national level only. In a true Information Society, there is no national level, and there are no frontiers. Independent media and citizens, expressing opinions and ideas on the Internet, are subject to national law, which is in accordance with international law and agreements such as the Universal Declaration of Human Rights.

It is important not to adapt the principles guided by human rights just because the technology offers us the excuse to avoid

### Iran: cybercafés under surveillance

Owners of cybercafés in Iran, which are very popular with the young people, students and intellectuals, especially in the capital Tehran, ask customers to disconnect if they catch them looking at 'non-Islamic' sites.

The Iranian regime censors thousands of websites it considers "non-Islamic", officially to protect the public from immorality. They also harass and imprison online journalists. Internet filtering was increased in the run-up to the February 2004 parliamentary elections, at which the hardliners strengthened their grip on the country. Censorship has quickly spread to political content.

The OpenNet Initiative, a partnership of researchers from Harvard University, the University of Toronto and University of Cambridge, noted that Iran uses technology from the US company Secure Computing, calling the firm 'complicit' in the censorship. According to them, the thriving Internet censorship market spread like a virus from China to Iran to an increasing number of countries worldwide. It calls into question not only the trumpeted slogans of high-tech firms that the Internet represents 'freedom' and 'connectivity,' but simplistic divisions between 'us' and 'them' as well.

*Source: Reporters without borders (Internet under Surveillance 2004)/  
OpenNet Initiative*

### China: Microsoft censors blogs

Chinese bloggers posting their thoughts via Microsoft's net service face restrictions on what they can write. Weblog entries on some parts of Microsoft's MSN site in China using words such as 'freedom', 'democracy' and 'demonstration' are being blocked. Those using these banned words or any sensitive information get a pop-up warning that reads: 'This message contains a banned expression, please delete this expression.'

Chinese bloggers already face strict controls and must register their online journal with Chinese authorities. The regulations require the writer of a blog to identify themselves to the authorities. According to Reporters Without Borders, China is using a system called Night Crawler to patrol web journals and make sure that only registered blogs are published. Unregistered blogs will be shut down.

Microsoft said the company abide by the laws, regulations and norms of each country in which it operates. Yahoo and Google have also been criticised for similar activities and restricting what people can search for and read online.

*Source: news.bbc.co.uk*

them. In the limited number of cases where interference is indeed necessary, for example to fight child porn or to prevent acts of terrorism, we should act within the regular borders of a civilised, democratic state. This means that we need the following clear rules for accountability and transparency:

- Information collected should no longer be stored than what strictly needed;
- Information collected should not be used for any other purpose than the reason why it was collected in the first place;
- The proposed action should be within proportions;
- The people affected by actions that infringe their rights should be allowed to dispute the infringement;
- There should be at least one controlling mechanism or institution.

In view of these considerations, we advocate that governments and citizens follow procedures, norms and rules that are already common within the democracies of the 'real' world, and are slightly adapted to meet the specificities of the virtual world.

The anarchy and anonymity of the Internet fed the idea of some people that there are no limits of exercising their right to freedom of expression. But the debate in the Netherlands, following the murder of outspoken filmmaker and essayist Theo van Gogh, showed that the right to freedom of expression is not in fact limitless, nor should it be. Maybe, we can state that freedom of expression does not mean that you can always say everything to everyone, but rather that exercising your rights is limited by other people exercising theirs. And yes, some human rights are conflicting. But for those, there are laws, norms, values, and expected social conduct which provide guidelines on how to navigate these.

The virtual world of Internet and the real world are not that different. Both are merging with growing pains into what, we hope, will be an inclusive Information Society based on the principles of the 'old' world and adapted to the realities of the new one. ■