# Debating privacy and ICT

# Debating privacy and ICT

*By* Rinie van Est and Dirk van Harten

## Introduction

Mankind is facing the arrival of the information society. The information society is enabled by rapid progress in the field of Information and Communication Technologies (ICT) and has the Internet and wireless communication as its backbone. The generation, processing and transmission of information are the information society's basic sources of economic productivity, cultural change and political power. The information society is a global society. State borders do not define the reach of the information society. The World Wide Web, satellites and the availability of these technologies do.

Over the last decade business, governments and citizens alike have embraced the new possibilities of ICT. The mobile phone has entered the street scene. Citizens link up to the Internet in great numbers, in search for medical information or to chat. Trade and industry use ICT to integrate product chains and to increase the binding with their customers. Governments introduce the possibilities to electronically make one's tax return. In short, the rise of the information society has led and will continue to lead to new types of relationships between people, between business and consumer, between state and citizen. Society as a whole is only just beginning to experience these new sorts of 'virtual' relationships. The viability of these relationships and the success of concepts like e-commerce and e-government are crucially dependent on trust. The proper use of digital personal data, i.e. the issue of privacy, will play a crucial role in establishing and maintaining trust in the information society.

Besides promising applications, ICT also provide ample opportunities for misuse. The Internet not only enables new opportunities for 'classical' crimes, like fraud, spreading child pornographic material or stalking, but also leads to new kinds of criminal behaviour, such as hacking, spamming, identity theft, and spreading viruses. These recent phenomena give cause to great concern and are believed to lead to enormous societal losses. E.g., the (in) famous ILoveYou-virus is supposed to have cost international companies and government organisations billions of dollars already. Moreover, the September 11 attacks proved the notion of any kind of terrorism a realistic one, including cyber terrorism. These events help to illustrate the fact that the information age puts issues like crime, criminal investigations, law enforcement, warfare and security into a new perspective. Cyber crime and -terrorism can perhaps pull the rug out from under our economy and democracy. The issue of safety therefore relates to securing our subsistence and democratic rights and has to be addressed fully.

It is evident that the issue of ICT and safety has consequences for the issue of ICT and privacy. The coming of the information age urges the international community to develop a strategy that both secures and balances privacy and safety. In order to contribute to the

international debate on ICT, privacy and safety the Rathenau Institute has organised an international conference on “Privacy in the Information Society”.

**E-government, e-commerce and privacy**

Both in Europe and the United States privacy protection is increasingly being considered as an indispensable prerequisite for electronic commerce and government. A strong protection of privacy can get citizens and consumers to use the new electronic services. Privacy protection is thought to be crucial for the societal acceptance of these new services. However, there is a discontinuity between the lack of privacy rules in the United States and the comparatively strict standards in the European Union and Canada.

The European Union and Canada have opted for regulated self-regulation. Both have set up a clear legal framework (Privacy Directive 95/46/EC and PIPEDA, respectively) that tries to strike a pragmatic balance between privacy and economy. In contrast, the United States have chosen self-regulation as their basic strategy. America’s strategy seems to be based on the model of the well-informed, rational and self-protecting consumer. In this model privacy is considered a barrier for e-commerce, and accordingly a minimum level of protection is to be desired. The European Union and Canada use a different model in which the citizen needs protection. Moreover, this protection is considered as an economic stimulus in the long term.

The differences in conceptions and instruments of privacy protection between the United States and the European Union and Canada may lead to various problems. For example, the enforcement of Articles 25 and 26 of the EU Privacy Directive may disrupt the trade in goods and services from Europe to America. Moreover, the Internet has made the collection, storage, processing and exchange of personal data a cross-border practice. One of the consequences of the global character of the information society is that existing national legislative systems are no longer sufficient to protect the citizen from intrusions on his privacy. Although protected under EU Directive 95/46 within the European context of the Internet, the EU citizen has little idea of what will or can happen to his personal data when undertaking a transaction within the American context.

It is self-evident that a global information society needs international privacy norms and internationally agreed on principles. The above shows that such a situation is still far away. Still, some positive signs can be noticed. First of all, a ‘Safe Harbour Agreement’ has been negotiated between the US and the EU. Another encouraging phenomenon is that the privacy debate in America is shifting from an ideological one to a practical one; from a normative discussion to a reflection on whether self-regulation actually works in practice. Such a more pragmatic discussion is likely to lead to a demand for more privacy protection and regulation. For example, in its May 2000 report the Federal Trade Commission concluded, by a narrow 3-2 vote, that industry self-regulatory efforts had not be shown to be effective alone in protecting privacy and recommended that legislation was necessary as well. Public opinion may form yet another force that will stimulate the coming about of international norms. Various comparative poll results show that

American, Canadian and European attitudes about privacy and how to protect it are strikingly similar. Another development that may strengthen the call for privacy protection within the private sector is the gradual erosion of the boundaries between the "public" and the "private" sectors. The argument is that if "private" organisations perform "public" tasks, privacy protection in the private sphere should be similar to that in the public sphere.

**Cybercrime, -terrorism and privacy**

Following the terrorist attacks of September 11th, new laws were passed throughout the Western world under the claim of realising a safer and more secure society. In the United States the Patriot Act was drawn up, broadening wiretapping and intelligence provisions. The Foreign Intelligence Surveillance Act – soon to be signed by President Bush – will increase the surveillance possibilities still further. The Canadian Bill C-36 contains a varied set of measures to enhance the government's ability to prevent and detect terrorist activity. The Council of Europe's Cyber Crime Convention has been ratified not only by the 41 member states, but also by the United States, Japan and South Africa. The fact that intelligence agencies did not foresee the September 11 attacks is used to justify broadening their authorities. A safer society is conveniently being equated with the Surveillance State.

The hasty and draconian character of a lot of these legislative initiatives gives rise to concerns, not only among human rights activists, but also in more conservative circles. In the United Kingdom the House of Lords protested strongly against an anti-terrorism package proposed by government, saying it would undermine both privacy and freedom by giving police too much unchecked investigative powers, and by including provisions that do not apply to terrorism. The setting up of military tribunals by the Bush administration, in order to trial suspected terrorists, alarms civil rights defenders in the United States. The tribunals not only deprive suspects of the protections offered under normal criminal justice but also undermine the separation of powers. The European Cyber Crime Convention, finally, clashes with both the European Convention on Human Rights and Directive 95/46/EC on data protection, and thus hollows out the right on privacy.

Besides these principal objections, many critics doubt on the whole whether more surveillance power, made possible by the anti-terrorism laws, will lead to more security. Comprehensive surveillance of communication networks, e.g., depends crucially on technology. Investigation systems have to be programmed to react on specific 'catchwords' that give away potential criminal or terrorist behaviour; they look for the abnormal. Most of the terrorists who planned and committed the attacks of September 11$^{th}$, however, led apparently 'normal' lives and therefore consciously managed to escape from being observed. Accordingly, the effectiveness of the new anti-terrorist laws is questionable in terms of security and critics fear the negative consequences these laws will have on the fundamental human right of privacy. They claim that the balance between societal security and personal freedom will be seriously distorted.

**The challenge of integrating the privacy and safety discourse**

This lack of attention for privacy in the current discussions on security, and the consequent divergence between different existing legal frames, may be explained from a lack of interaction between the privacy and safety discourse. For example, the preparations for the Cyber Crime Convention have been almost solely been carried out by police and investigation organisations. Similarly, in past debates on privacy and ICT human rights and economic interests prevailed, while surveillance and security issues hardly came to the fore. The time has come, therefore, to connect the privacy and safety discourse in order to find and establish a new balance between security, safety and human rights. Such a balance should secure economic and social prosperity and should enable a fight against crime and terrorism that strengthens our democracies, instead of threatening their underlying basic values and human rights. Privacy should not be perceived as an obstacle for protecting our society, but should in fact be seen as one of the main goals of protection measures.