Debating Privacy and ICT: Amsterdam January 17, 2002

aber auch dem einzelnen touristischen Angebot zugute kommen und wichtigen Umweltzielen dienen. Die jeweiligen Startphasen werden vom deutschen Umweltbundesamt bzw. Bundesumweltministerium und vom LIFE UMWELT Programm der Europäischen Union mitfinanziert.

»

Debating Privacy and ICT

Amsterdam, January 17, 2002

Conference report by Rinie van Est and Dirk van Harten, Rathenau Institute, the Netherlands

The Western world is facing the arrival of the information society, enabled by the rapid progress in information and communication technologies (ICT). Generating, processing and transmitting information are the information society's main sources of economic productivity, cultural change and political power. Internet and wireless technologies have made this all a cross border practice: the information society is not defined by state borders but by the World Wide Web, by satellites and the availability of these technologies.

Besides promising applications, ICT provide ample opportunities for misuse as well. ICT enable new forms of classical crimes – like the spreading of child pornographic material and fraud – and new types of criminal behaviour – like hacking, identity theft and Denial of Service attacks. These crimes present a threat to privacy and personal freedom. Paradoxically, the methods we use to safeguard society from criminal activities may themselves become a threat to basic human rights as well.

In order to discuss privacy issues in relation to ICT developments, some 130 privacy experts and other interested parties gathered on January 17, 2002, in Amsterdam at the conference "Debating Privacy and ICT". The conference was organised by the Rathenau Institute, the Dutch national TA organisation. Participants came from throughout Europe and Northern America and even from countries as far as Ghana. Their backgrounds varied from scientists to policy makers; from representatives of consumer and civil rights groups to representatives of industry and investigation agencies.

Eight speakers – from the US, the UK, the Netherlands, Canada and Austria – presented various privacy-related aspects of the commercial use of personal data and criminal investigations. The presentations focussed on the forces driving privacy law making in various countries, on international developments and on the consequences of the terrorist attacks of September 11, 2001, on the Pentagon and the World Trade Center. The Rathenau Institute, however, wanted to go beyond presenting the current state-of-affairs. In the afternoon the so-called "Declaration of Amsterdam: Trust in the Information Age – Securing Privacy and Safety" was handed out to the participants. The declaration contained policy recommendations and served as a discussion paper and a possible roadmap for a future approach.

The authors of this paper wrote the draft version of the declaration on the basis of all the conference papers. This draft was then sent out to the speakers for their commentaries. A day before the actual conference, the Rathenau Institute organised a preliminary workshop, at which speakers and a few other invited experts came together in order to streamline the declaration and to formulate a common series of policy recommendations that all speakers were willing to explain and defend during the conference.

The first recommendation immediately gave rise to heated debate. It was recommended to implement the EU Data Protection Directive in all EU member states and to support attempts to enforce an 'adequate' level of privacy protection in non-EU states. Objections from the audience were that this proposal ignores the controversies surrounding the directive and the fact that it already needs a thorough revision. The recommendation, however, was prompted by the fact that – despite all its flaws – the directive remains the most important international agreement and has become the standard even outside the EU. Furthermore, the directive is binding, which makes it far more useful than, for example, the guidelines laid down by the OECD.

Due to its general character, the second point of the declaration on public and private sectors, accountability and transparency hardly caused any controversy at all. But emotions were running high again when the third paragraph, on surveillance, was presented. This paragraph pleads to find a proper balance between the social costs and benefits of surveillance systems. The aftermath of September 11th has shown that current discussions and decision making are strongly fed by emotional arguments. Consequently, the safety argument tends to be dominant and the privacy argument tends to be neglected. It should be acknowledged, however, that the social costs of surveillance can go far beyond a mere invasion of privacy. Surveillance – as shown in the former communist countries – can lead to the imposition of 'normality' and standardised behaviour, and thus limit individual choice.

To actually establish mechanisms for balancing safety and privacy objectives may – as one of the speakers put it – very well be one of the greatest challenges the information society has to face up to. In its second policy recommendation, the declaration, therefore, presents a step-by-step approach on the basis of precautionary principles that may serve as a starting point for taking up that challenge. Some of the participants, however, complained about the vagueness of the principles and there were also pleas to be heard for more surveillance.

A recommendation on the "empowering of a technological citizenship" was found to be desirable, but a discussion came up on how to achieve this. It was argued that the right of the data subject to access his data – guaranteed by the EU Directive – could play an important role in this and, therefore, should be brought to the attention of the data user more strongly. Others held that in practice people do not use this right until problems occur that mostly have little to do with the issue of privacy. Still others claimed that a difference should be made between identification and authentication. After all, there are many situations in which a person does not really need to identify him or her self, but in which mere authentication would suffice. Lawmakers, in particular, should be more aware of this.

The last two paragraphs of the declaration – on the responsibility of the data user and on research – passed without many debates. Partly because both speakers and audience were growing weary by the end of the day, and partly due to the general character of the recommendations, claiming a strong legal framework and setting up scientific research programs in order to gather empirical and verifiable data.

Finally, it was questioned which status the "Declaration of Amsterdam" was to receive and to whom it was to be addressed. Some were afraid that being at the conference would imply backing the declaration. It was explained that that was absolutely not the case. Under its own authority, the Rathenau Institute will present the "Declaration of Amsterdam" to the Dutch parliament.

Speakers at the conference were Charles Raab (University of Edinburgh, United Kingdom), Colin Bennett (University of Victoria, Canada), Friso de Jong (Hoge van den Broek Advocaten, the Netherlands), Priscilla Regan (George Mason University, United States), Caspar Bowden (Foundation for Information Policy Research, United Kingdom), David Phillips (University of Texas, United States), Walter Peissl (Institut für Technikfolge-Abschätzung, Austria) and Barry Steinhardt (American Civil Liberties Union, United States). The conference was chaired by David Banisar from Privacy International and Harvard University, United States.

The full text of the Declaration of Amsterdam as presented at the conference can be found at the end of this article.

The full text of the Declaration of Amsterdam as presented at the conference can be found at the end of this article.

The conference papers, the Declaration of Amsterdam and the conference report can be obtained through the websites http://www.privacyconference.nl or http://www.rathenau.nl.

Contact

Dr. Rinie van Est
Drs. Dirk van Harten
Rathenau Instituut
Koninginnegracht 56, NL-2514 AE Den Haag, The Netherlands
Tel.: +31 (0) 70 34 21 542
Fax: +31 (0) 70 36 33 488
E-mail: q.vanest@rathenau.nl
E-mail: d.vanharten@rathenau.nl
Internet: http://www.rathenau.nl

The Declaration of Amsterdam: Trust in the Information Age – Securing Privacy and Safety

Presented at the conference: Debating Privacy and ICT
Amsterdam, January 17, 2002

International co-operation

International co-operation on privacy protection has a long history. The OECD, The Council of Europe, The European Union and others have addressed these issues. The most important international agreement remains the 1995 EU Data Protection Directive. The essential principles of privacy protection have been negotiated and agreed upon over the years. The tragedy of September 11th should not be allowed to interrupt the process of defining and harmonising international privacy principles.
Accordingly we suggest:

- That the EU Data Protection Directive be immediately implemented and effectively enforced in all EU Member States.
- To strongly support the attempt to enforce an "adequate" level of privacy protection in non-EU states.

The rapid development of ICT will continue to bring up new privacy protection and surveillance issues, especially when these new technologies will have a potential for security and law enforcement.
Accordingly we suggest:

- When addressing these developments in international agreements, privacy implications of these new technologies need to be considered in the very early stages of technology and standards development.
- To encourage the recent initiative by the Centre Européen de Normalisation (CEN) to develop a common international standard and quality assurance and a quality mark.

Public, commercial, and non-profit sectors

Over the last decades, the boundaries among public, commercial, and non-profit sectors have been eroding. Personal data that are collected, processed, stored and communicated by one sector are now increasingly exchanged across traditional boundaries. This development aggravates the problems of accountability and transparency and has consequences for public trust.
Accordingly we suggest:

- To address these problems by appropriate and effective instruments for the protection of personal data in all sectors.

Surveillance

The social cost of surveillance is not limited to the invasion of privacy. The collection, processing, storage and communication of personal data establishes norms of behaviour and standardises categories of social groups. This imposition of normality limits individual choice and restricts society's necessary potential for change. It also subjects individuals to discrimination.
Therefore:
We recognise that some surveillance systems may be justified in some circumstances to promote security or public safety. In order to legitimise any proposed surveillance and registration system, we propose a step by step analysis (precautionary principles):

1. Surveillance systems should only be implemented if they are effective, not easily circumvented, and will produce a real security benefit.

2. Surveillance systems should only be implemented if the benefits are worth the social costs, including the invasion of privacy, loss of autonomy, social discrimination, or imposition of conformity. (This means applying the principle of proportionality.)
3. If it will produce a security benefit that justifies the social costs, measures will have to be taken to minimise those costs.
4. Before any surveillance system is implemented, legal mechanisms of oversight and redress will have to be established.
5. The effects – both positive and negative – of the systems will have to be periodically reviewed by an independent publicly accountable body.

Empowering technological citizenship

Citizens have to be empowered through information and education that will give them the awareness, skills, and tools to participate in the decision making process and to protect themselves from abuse.
Accordingly we suggest:

- To support development and use of privacy enhancing technologies in order to make citizens less vulnerable to misuses of their personal data.
- To empower a technological citizenship by raising awareness of threats to privacy and strengthening digital skills through information campaigns and education.
- To raise public awareness by making transparent how public and private organisations deal with their personal data.
- To improve decision makers' understanding of the public's needs and concerns. This could be accomplished through public consultations.

The responsibility of the data user

Privacy protection requires effective implementation of the privacy principles by all organisations that handle personal data. Many attempts at self-regulation have been merely symbolic, poorly implemented throughout the organisation and/or misleading for the individual. Too often the interests of the data user have prevailed over those of the individual.
Accordingly we suggest that effective implementation of privacy protection requires:

- A well-defined legal framework
- An organisational structure and culture that respects privacy at all levels.
- Procedures for verifying compliance, including independent and external audits.
- Privacy impact assessments for the introduction of new technologies and/or services with implications for privacy.
- Where appropriate, a chief privacy officer or other responsible manager to ensure compliance.

Research

Current discussions on privacy seriously lack substantial empirical support and are therefore prone to be driven by ideology and opportunism.
Accordingly we suggest:

- That national and international research programs be set up in order to gather and analyse reliable quantitative and qualitative data on issues such as organisational practices, technological applications and innovations, and public understanding of privacy.
- That these research results be incorporated within the process of decision making and implementation in all sectors.