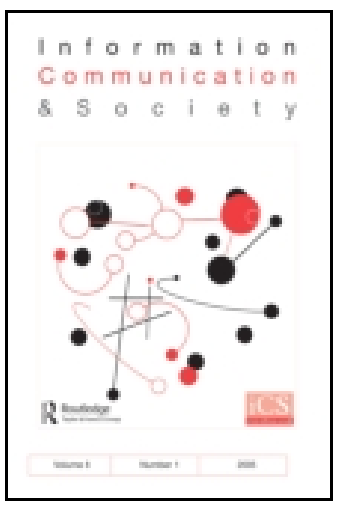
This article was downloaded by: [University of Cambridge]
On: 09 October 2014, At: 17:53
Publisher: Routledge
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Information, Communication & Society
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rics20

Privacy and security at risk in the global information society

Simone Fischer-Hübner [a]
[a] Faculty for Informatics , University of Hamburg , Vogt-Kölln-Str. 30, Hamburg, D-22527, Germany E-mail:
Published online: 25 Feb 2009.

To cite this article: Simone Fischer-Hübner (1998) Privacy and security at risk in the global information society, Information, Communication & Society, 1:4, 420-441, DOI: 10.1080/13691189809358981

To link to this article: http://dx.doi.org/10.1080/13691189809358981

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

PRIVACY AND SECURITY AT RISK IN THE GLOBAL INFORMATION SOCIETY

Simone Fischer-Hübner

University of Hamburg

Abstract

In the global information society, individual privacy is seriously endangered. An increasing amount of personal data is being transferred around the world, and communication data of users could be easily traced and used to create individual communication using new information infrastructures. With contemporary network technologies, it is difficult to protect personal data adequately. The Internet, as an important contemporary information highway, is missing essential features of reliability, functionality, confidentiality and integrity, and is threatened by various security attacks.

This paper discusses privacy and security risks in the global information society. It also compares and critically analyses the approaches to privacy protection of different information infrastructure programmes. The difficulties for a common harmonised legal approach to privacy protection, due to cultural differences, are analysed. Finally, possibilities for designing information infrastructures adequate under social and privacy requirements (in particular privacy-enhancing technologies) are discussed.

Keywords

global information society, information infrastructure programmes, privacy, privacy-enhancing technologies, security

Downloaded by [University of Cambridge] at 17:53 09 October 2014

INTRODUCTION

Since the Clinton government in the United States started the National Information Infrastructure Programme (US Government 1993), most other technologically developed countries have issued information infrastructure programmes for the further development of information highways and to strengthen the information and communication industry. A group of representatives, mainly from industry, under the chair of the vice-president of the European Union (EU) commission, Martin Bangemann, has elaborated a report and an action plan for the EU (Bangemann 1994) to carry Europe forward into the global information society.

The various national and global information infrastructure programmes promote different initiatives such as teleworking, distance teaching, health

networks and network access to all households with applications such as telebanking. They are motivated mainly by economic interests and hold great promises, such as the generation of new jobs, economic growth, better chances for people constrained by geography or disability, possibilities to overcome structural problems such as in traffic or in healthcare. On the other hand, the new information infrastructure will change our lives completely, and it bears different risks for society.

The Internet, as a contemporary data highway on which the global information society may be built, is known to have many security risks. Thus, the vast development of new information infrastructures will increase our dependability and might lead us to a vulnerable information society based on insecure technologies.

Besides, individual privacy is seriously endangered and is becoming increasingly an international problem. More and more sensitive personal data can be quickly transferred around the world. Moreover, an increasing amount of transactional data for network services will be available and can be collected at different sites around the world. This data can be used to generate consumer and communication profiles. Privacy as a fundamental civil right has to be protected in a democratic society.

The EU Directive is aimed at enforcing a relatively high standard of data protection and will probably not only be an instrument for harmonisation within Europe. It can also have a coercive effect on countries outside Europe to enact efficient data protection laws based on the EU Directive. Nevertheless, global international harmonisation of privacy legislation in addition to the EU Directive on data protection is hardly achievable due to cultural, political and historical differences. Thus, more privacy-enhancing technologies which can technically enforce legal privacy requirements have to be designed, implemented and used.

This paper discusses privacy and security risks in the global information society. It also compares and critically analyses the approaches to privacy protection of different information infrastructure programmes. The difficulties for a common harmonised legal approach to privacy protection, due to cultural differences, are analysed. Furthermore, privacy-enhancing technologies are discussed.

PRIVACY

An often used definition of privacy is the one by Alan Westin: 'Privacy is the claim of individuals, groups and institutions to determine for themselves,

Downloaded by [University of Cambridge] at 17:53 09 October 2014

when, how and to what extent information about them is communicated to others' (Westin 1967: 158).

In general, the concept of privacy can have three aspects (Rosenberg 1992; Holvast 1993):

- *territorial privacy* (by protecting the close physical area surrounding a person);
- *privacy of the person* (by protecting a person against undue interferences, such as physical searches or information violating his moral sense); and
- *informational privacy* (by controlling whether and how personal data can be gathered, stored, processed or selectively disseminated).

Data protection is the protection of personal data in order to guarantee privacy and is only a part of the concept of privacy.

The emphasis of this paper is on discussion of the informational privacy of individuals. Individual informational privacy has also been defined by the German Constitutional Court in its Census Decision of 1983 as the term 'right of informational self-determination', meaning the right of an individual to determine the disclosure and use of his personal data on principle at his discretion. In order to protect the right of informational self-determination, national privacy laws of many Western states, codes of ethics of different computer societies, as well as international privacy guidelines or directives (such as the EU Directive on Data Protection (EU Directive 1995)), require basic privacy principles to be guaranteed when personal data is collected or processed. These include:

- *purpose specification and purpose binding* (personal data must be obtained for specified and legitimate purposes and should not be used for other purposes) (see EU Directive, Article 6);
- *necessity of data collection and processing* (the collection and processing of personal data will only be allowed if it is necessary for the tasks falling within the responsibility of the data processing agency) (see EU Directive, Article 7);
- *the data subject's right to information and the right to correction, erasure or blocking of incorrect or illegally stored data* (see EU Directive, Articles 10–14);
- *control by an independent data protection authority* (also called supervisory authority, data protection commissioner, or ombudsman) (see EU Directive, Article 28); and
- *requirement of adequate technical and organisational security mechanisms* (to guarantee the confidentiality, integrity and availability of personal data) (see EU Directive, Articles 6 and 17).

Downloaded by [University of Cambridge] at 17:53 09 October 2014

The privacy-enhancing security criteria of *anonymity or pseudonymity* of a user is derived from the necessity principle. The privacy principle of necessity of data collecting and processing means that personal data should not be collected or used for identification purposes when not really necessary. Consequently, information systems should guarantee that, if possible, users can act anonymously. The best design strategy to enforce this requirement is the *avoidance of personal data*.

In general, privacy protection can be undertaken by:

- privacy and data protection laws promoted by government;
- self-regulation for fair information practices by codes of conduct promoted by businesses;
- privacy-enhancing technologies adopted by individuals; and
- privacy education of consumers and IT professionals.

THREATS TO PRIVACY IN THE GLOBAL NETWORKED SOCIETY

In the global information society, privacy is seriously endangered. A key problem is that the traffic on a global network (for example, on the Internet) crosses international boundaries and is not centrally managed. On the Internet, there is no overall responsibility assigned to a certain entity, and there is no international oversight mechanism to enforce legal obligations (especially data protection legislation), as far as they do exist (Budapest Draft 1996).

There are serious privacy risks, because personal data about the users or other data subjects is available and can be intercepted or traced at different sites around the world. Major risks are discussed in the following sub-sections.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

Privacy threats at application level

The Bangemann report (Bangemann 1994) and most other Information Infrastructure Programmes promote initiatives such as teleworking, distance teaching, research networks, telematic services for enterprises, road and air traffic management systems, healthcare networks, public administration networks, network accesses for all households through applications such as telebanking and video-on-demand. Meanwhile, the global information society is evolving rapidly and many new information highways and applications for the health sector, public administration, research, electronic commerce and private life are being developed. For these applications, there is a growing amount of personal data, such as sensitive medical data, business data and

private data that are collected, processed and communicated through networks across state borders.

For example, according to the Bangemann report, European healthcare networks for less costly and more effective healthcare systems for Europe's citizens are planned. A direct communication 'network of networks' based on common standards (e.g. standardised electronic patient case files) linking general practitioners, hospitals and social centres on a European scale will be developed. These healthcare networks will improve diagnosis through on-line access to European specialists, on-line reservation of analysis and hospital services by practitioners extended on a European scale, transplant matching, and so on. A complete electronic medical patient case file which can be shared between specialists and can be interchanged between hospitals and with GPs can help to diagnose diseases correctly, to avoid duplicative risky and expensive tests, and to design effective treatment plans.

Due to the development of new healthcare networks on a national and global scale, and the growing use of telemedicine and telecare, more and more sensitive medical data will be collected, electronically stored, shared between different healthcare professionals and transferred to different sites in the world. However, medical patient case files may contain some most sensitive information about topics such as abortions, emotional and psychiatric care, sexual behaviour, sexually transmitted diseases, HIV status, genetic predisposition to diseases. The privacy of medical data which is endangered has thus to be especially safeguarded.

Furthermore, there are serious privacy risks, since more and more sensitive personal data can easily be communicated to and is often routed via different countries, which do not necessarily have an appropriate privacy level. Messages transmitted in plain text could be intercepted or modified at each site of the communication path.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

Privacy threats at communication level

A side-effect of global communication is that connection data is available at different sites around the world, revealing details about communication partners, time of communication, services used, connections, and so on. This transactional data can reveal who communicated with whom, when, for how long, and who bought what for what price. Users leave an electronic trace which can be used to create consumer or communication profiles.

Every electronic message contains a header with information about the sender and recipient, as well as the routing and subject of the message. This

information could be intercepted at each site passed. There is normally no anonymity of communication, because the recipient of an electronic mail (even if the e-mail is encrypted) can determine the sender's identity through the sender's e-mail address which normally contains information about the user's name, background (for example, university or company), and location.

Besides, communication profiles could be created by the service provider to whom the user is connected (like Internet or mailbox providers). Service providers are storing personal user data about their subscribers (such as user name, login name, address, bank connection and status). Users are normally identified and authenticated by the service providers, and their communication behaviour (for example, accesses to news or World Wide Web (WWW) sites) could be easily traced and supervised by the providers. Normally, service providers record the use of services to create accounting data for billing purposes. Besides, the service provider has to collect connection data for operation of the cache.

Also, personal data about users can be recorded at remote servers. A recent study by the Electronic Privacy Information Center (EPIC) showed that none of the most frequently visited websites on the Internet meet basic standards for privacy protection (EPIC 1997). A WWW server can only record the Internet Protocol (IP) addresses of requesting users, which normally do not reveal the user's identity. Nevertheless, techniques, such as so-called 'cookies' or the proposed Open Profiling Standard (OPS), could be used by the remote WWW servers to monitor and track the user's accesses to web pages. Furthermore, a requesting user may be reidentified by the identi-protocol, which operates by looking up specific TCP/IP connections and returning the user name of the process owning the connection.

Cookies are blocks of ASCII text that a server can store and later retrieve from the local WWW browser of the user. Cookies, which were introduced by Netscape to allow user-side customisation of Web information, are a mechanism that allows a website to record users' comings and goings, usually without their knowledge or consent. If a user is identified by the server as having ordered goods or registered for software, the cookies of this user revealing their interest in particular web pages can be matched to his name or e-mail address by the server. Netscape soon modified its browsers so that cookies from one site could not be given to another site. However, web developers and Internet advertising companies (namely Double Click Network) soon found a way to use cookies to correlate user's activities between many different websites to track the user's usage history and preferences. This could be done

Downloaded by [University of Cambridge] at 17:53 09 October 2014

by adding cookies to GIF images that were served by third-party sites (see Garfinkel and Spafford 1997).

The current cookie usage is violating the provisions of the EU Directive on data protection and other national data protection legislation (see also Mayer-Schönberger 1997): first of all, because of their expiration date option, cookies may violate the 'accuracy' and 'timeliness' principles of Article 6 of the Directive. Furthermore, the average user is unaware of cookie storage and access. However, to meet Article 7 of the Directive, a user has to give informed consent to a cookie transfer, since the other alternative conditions of Article 7 (a legal obligation, vital interests and/or contractual arrangements) cannot be assumed. Browsers need to be specifically configured to disallow cookies or to display a cryptic warning that a cookie is going to be stored. The average user has not the technical knowledge to configure his system accordingly or to view or delete the cookie file and can hardly make an informed decision based on such cryptic warnings. Consequently, there is no informed consent by the user and cookie technology is therefore violating Article 7 of the Directive. Besides, the extensive information and access rights granted to the user by Articles 10–12 of the EU Data Protection Directive are violated.

In May 1997, the American companies Netscape, Firefly Networks and Verisign announced the 'Open Profiling Standard' (OPS) which is defined by Netscape as 'a standard that enables personalisation of Internet services while protecting user's privacy' (Netscape 1997). In contrast to cookies, OPS specifies the structure of Personal Profiles, so that the same information can be used by many different websites. To enhance an individual's privacy, OPS will give users control over their Personal Profiles and the ability to manage which information is disclosed or withheld from a particular website. Personal Profiles can contain information of any sort, such as a unique identifier for the profile, unique identifiers to each service visited, demographic information (e.g. country, zip code, age, gender), contact information (e.g. name, address, phone and fax numbers, e-mail address), commerce information (e.g. credit card number) or user-side specific information (e.g. detailed personal preferences, favourite books or magazines).

Although, OPS can enforce the principle of informed consent by giving users the ability to selectively release or withhold information in their Profiles, OPS could severely endanger the individual's privacy. In contrast to cookies, OPS uses standardised Personal Profiles, which can be shared by different sites and can contain user-identifying data and many more personal attributes. Even if the user refuses to give consent for the disclosure of information in his profile, he could be forced in practice to do so. This could, for example, be the

Downloaded by [University of Cambridge] at 17:53 09 October 2014

case if users are relying on access to a service or to resources, and the access is only permitted to them if they provide access to information in their Personal Profile (Brunnstein *et al.* 1998).

According to the German multimedia legislation, the provider may not make the use of services conditional upon the consent of the user to the effect that his data may be processed or used for other purposes, if other access to these services is not or not reasonably provided to the user. However, since the Internet has no national boundaries and personal data used for multimedia services often crosses national borders, corresponding international privacy regulations for multimedia services are needed as well.

Transactional data can reveal sensitive information about the user's communication behaviour and interests. For example, the choice of a news-group or access to websites of a political magazine could reveal information about the political opinion of a user. Marketing companies usually have a strong interest in such transactional data revealing the user's preferences. Users have reason to be concerned over the distribution of their transactional data for financial gain, and the (mis-)use for purposes other than the purposes for which it was collected. A famous case in the United States is the recent example of America Online (AOL) selling its subscribers' contact information, financial information and Internet activities.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

SECURITY RISKS

A further problem of the global information society is whether the requirements of appropriate technical and organisational security mechanisms to protect personal data on the information highways and to provide network reliability can be guaranteed sufficiently.

Important security and safety aspects that have to be guaranteed are:

- *confidentiality* (prevention of unauthorised or improper disclosure of data);
- *integrity* (the goal of ensuring that data continues to be a proper physical and semantic representation of information, and that information processing resources continue to perform correct processing operations);
- *availability* (prevention of unauthorised withholding of data or resources);
- *functionality* (the system performs its functions always 'as required'); and
- *reliability* (all functions performed on a system are always equally performed under equal constraints).

The Internet, an important contemporary information highway that consists of several thousand computer networks with several million users, is known for

many critical security holes and is missing essential security features of reliability, functionality, confidentiality, integrity and availability (see Brunnstein and Schier 1997). Various security attack techniques have demonstrated the insecurity of Internet technology and of contemporary information infrastructures:

- *manual* (such as the KGB hack) or *automated hacking* attacks (there are various Internet sites which offer hacking tools and introductory or educational material on hacking techniques);
- *sniffing* attacks (which monitor and store other's electronic traffic);
- *spoofing* attacks (which forge and misuse electronic addresses);
- *malicious agents* (which can exploit features or weaknesses of Internet services. An agent can be started either by the user or automatically, and may distribute itself through the network. Agents work in a hidden manner, and it will be difficult or even impossible to control activities or consequences of such agents. Examples of early malicious agent technologies are 'worms' (the Internet worm experiment by Robert Morris resulted in the breakdown of several thousand Unix systems and caused severe damage) or 'chain letter attacks' (such as crismas.exe));
- *malicious documents/macro-viruses* (which can import malicious side-effects into local Internet stations. Macro-viruses are computer viruses written in the macro or formula language of word processing and spreadsheet application programs. Macro-viruses spread when infected documents are transferred. Macro-viruses are a significant threat, because they are platform independent, easier to write than 'traditional' file viruses written, for the most part, in assembly code, and because data files are exchanged far more frequently than executable files. Due to the increased use of e-mail with the ability to attach files, and mass access to the Internet and on-line services like AOL, macro-viruses are currently regarded as the most serious malicious code threat);
- *malicious web contents* (such as hostile Java applets or Active-X controls. A Java applet is a Java program that is loaded over the Web and run from inside a web browser. In general, Java applets are restricted to a 'sandbox' and are prevented from reading and writing files on the client file system, and from making network connections except to the originating host. However, these restrictions have not prevented hostile applets (such as 'Noisy.Bear' or 'Killer-java') from misusing system resources to perform denial service attacks and to exploit various implementation flaws (bugs) in the Java run-time system (see Brunnstein 1997). In contrast to Sun Microsystem's Java, Microsoft's Active-X does not take the sandbox approach. Active-X programs have full access to the user's file system and

Downloaded by [University of Cambridge] at 17:53 09 October 2014

> can cause severe damage. The user's privacy is especially endangered by technologies that use a downloaded code, such as Active-X controls or Plug-Ins. Malicious downloaded programs can, through security holes, scan the end-user's hard disk or network for important information and then smuggle the data to the outside world using the computer's network connection (see Garfinkel and Spafford 1997).

A major reason for Internet security problems is that security was not an important aspect when the Internet was initially designed, and, consequently, it is now virtually impossible to fix many security holes. Security and safety are design-inherent features (i.e. they must be specified in the design phase and enforced in implemented systems). Later security enhancements, such as Internet Protocol Version 6 (IPV.6), including authentication and encryption, or protocols such as S-HHTP or SSL, can only reduce security risks, but cannot cure past design faults. A further problem is the lack of overall responsibility for security on the Internet; each site is responsible for its own security.

PROBLEMS OF INTERNATIONAL HARMONISATION OF PRIVACY LEGISLATION

According to the Bangemann report:

> Without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society. Given the importance and sensitivity of the privacy issue, a fast decision from Member States is required on the Commission's proposed Directive setting out general principles of data protection.
>
> (Bangemann 1994: 20)

In the EU, privacy protection will be enforced by the EU Data Protection Directive.

EU Directive on Data Protection

The EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive 1995) was formally adopted in October 1995 by the European Council. Member states of the EU have to amend their respective national laws (where necessary) to conform with the Directive by October 1998. The main objective of the Directive is the protection of privacy as a fundamental right which is more and more endangered in the networked society. As well as the

Downloaded by [University of Cambridge] at 17:53 09 October 2014

privacy protection of individuals, another objective of the EU Directive is to require a uniform minimum standard of privacy protection to prevent restrictions on free flow of personal data between EU member states for reasons of privacy protection. The EU Directive makes no differentiation between rules applied in the public and in the private sector. It sets out general rules on the lawfulness of data processing which should also enforce the basic privacy principles mentioned above. It could be used to enforce a relatively good level of data protection in Europe. However, it has also been criticised on the basis that some rules (especially the criteria for making data processing legitimate – Article 7) are very general and allow a variety of specific implementations in national laws. These differences in interpretation could hinder the goal of reducing divergence between national laws.

The Directive contains a combination of concepts, which are enforced by the data protection legislation of different member states. For example, the concept of registration of processing operations (Article 18) is enforced in the British, French and Scandinavian data protection legislation (among others). The concept of a data protection official inside an organisation (Articles 18 and 20) was taken from the German Federal data protection act and the concept of special protection of special categories of data (Article 8) was taken from the French, Irish and Scandinavian legislation. Rules for industrial self-regulation of personal data systems (codes of conduct, Article 27) were taken from the Dutch system.

The EU Directive also contains provisions for the transfer of personal data to third countries outside the EU. According to Article 25, the export of personal data to third countries, which do not provide an adequate level of protection, is prohibited. However, in open and free networks, such as the Internet, with no central agency of control, it is technically difficult to enforce this requirement (Koch 1995). It has also been criticised because many rules of the EU Directive include exceptions that are mandatory and may hinder states in providing a stricter standard of privacy protection (Greenleaf 1995).

Even if the EU Directive can help to enforce a relatively high standard of data protection in Europe, it will not be able to protect privacy sufficiently in the global information society. As discussed above, personal data can easily be transferred or routed across state boundaries to countries without any data protection legislation, where its information content or communication data can be intercepted. Privacy is therefore an international problem, and international harmonisation of privacy regulations is needed. However, a hope is that the EU Directive will not only be an instrument for harmonisation within Europe. It can also for the following reasons have a coercive effect on

Downloaded by [University of Cambridge] at 17:53 09 October 2014

countries outside Europe to enact efficient data protection laws based on the EU Directive. The Directive represents the 'most modern international consensus on the desirable content of data protection rights' and 'it may be a valuable model for countries currently without data protection laws' (Greenleaf 1995). Also, due to the restrictions of Article 25 on the data transfer to third countries, there is economic pressure on non-EU countries to enact efficient data protection acts. For these reasons, some states have already issued new data protection acts. For example, the 1993 Quebec Data Protection Law (the first North American legislation to enact private sector data protection) was based on the earlier EC Directive Draft and was drafted explicitly to protect business from the possible blockage of data transfer from Europe. Another example is Hungary, which is seeking EU membership, and has in 1996 become the first country in Eastern Europe to pass data protection legislation and establish a data protection commissioner. Countries outside the EU will increasingly use the EU Data Protection Directive as a model in devising or updating their legislation (see also Bennett 1997).

Nevertheless, the critical question remains whether a common harmonised approach to privacy will be possible due to cultural, historical and political differences. Anthropologists have stated that, on a low level, privacy (especially privacy of the person and of the close surroundings) is a human physiological need. But, on higher organisational levels, privacy is basically a cultural construct and there are considerable cultural variations in privacy needs and interests (Lundheim and Sindre 1993). In addition, the experiences from World War II, especially the practice of the Nazi government in amassing and misusing great amounts of personal details about the population, have created a greater sensitivity to privacy in Western European states (Madsen 1992). Another problem can be seen in non-democratic societies, where individual privacy is normally not protected by legislation. On the contrary, in these countries privacy is often invaded by the state.

In the following sections, the privacy approaches of technologically developed states that have set up information infrastructure programmes are compared with the EU approach. Thereby, considerable differences in the different national approaches to privacy protection are shown. Furthermore, all the approaches are critically analysed to determine the insufficiencies of privacy legislation (see also Fischer-Hübner 1997).

Singapore

Singapore was one of the first countries in the world to issue a national infor-

Downloaded by [University of Cambridge] at 17:53 09 October 2014

mation infrastructure programme. The information infrastructure plan *IT2000 – A Vision of an Intelligent Island* was formulated by the Singapore government in August 1991 (NCB 1991). By 2000, Singapore, the Intelligent Island, should be among the first countries with an advanced information infrastructure that will link government, business and people. Singapore ONE (One Network for Everyone) is a national initiative to deliver a new level of interactive, multimedia applications and services to all homes, businesses and schools throughout Singapore. So far, Singapore has worldwide the highest rate of Internet connections per household. However, Singapore, like most other Asian states, does not as yet have any privacy protection laws. On the contrary, privacy does not seem to be a topic at all. Intensive surveillance by security services is justified by Singapore's Internal Security Act. While promoting the use of the SINGNET (Singapore's Internet sub-network), the government is trying to control the content of the information transmitted over the Net at the same time (Madsen 1995).

Downloaded by [University of Cambridge] at 17:53 09 October 2014

Japan

In June 1993, the Information Industry Committee of the Industrial Council in Japan issued a report stating the need for the government to promote information technology. In May 1994, the Ministry of International Trade and Industry (MITI) published a *Programme for Advanced Information Infrastructure*. In this programme, under the topic 'Improvement of Environment for Realising Advanced Information Society', only security measures, and not privacy issues, are discussed (MITI 1994).

Japan, on the other hand, is one of the very few Asian countries to have implemented a data protection act. The awareness of privacy in Japan has resulted more from economic self-interest than from any long-standing tradition of ensuring individual privacy (Madsen 1992). The Japanese Act for Protection of Computer Processed Personal Data was made official in December 1988. In addition, cities, towns and villages have also enacted local privacy regulations. However, the Japanese data protection act only applies to national government organisations. Moreover, it does not set up an independent data protection authority to control data processing. In 1989, MITI issued formal guidelines entitled *Protection of Personal Data Processed by Computers in the Private Sector* to encourage self-regulation in the private sector on privacy, information integrity and information quality. However, these guidelines for privacy in the private sector as a means of self-regulation are not mandatory and can only be adopted internally by private companies.

United States of America

In 1993, the Clinton/Gore government presented the *National Information Infrastructure (NII) Programme – Agenda for Action* (US Government 1993). So far, the US have been criticised for being the first in technology but the last in data protection (Madsen 1992). The US Privacy Act of 1974 only covers the federal public sector. Besides the Privacy Act, there is only a non-uniform patchwork of various privacy and computer security legislation. The US does not have a data protection authority to oversee privacy protection and to act if there are complaints from data subjects about unfair or illegal use of their personal data. Consequently, the only way for data subjects to fight against data misuse is through the courts.

It has been realised that the NII does not only promise many benefits, but is also increasing risks to privacy. Therefore, the Information Infrastructure Task Forces (IITF) Working Group on Privacy has developed privacy principles with the goal of providing guidance to all participants in the National Information Infrastructure (IITF 1995). They are intended to be applied to governmental and private sectors, and are based on the idea that all participants (information providers, collectors, users and data subjects) of the NII have a shared responsibility for the proper use of personal information.

'General Principles for All Participants' require that all NII participants should ensure and respect information privacy, information integrity and information quality. 'Principles for Users of Personal Information' require information users to assess the impact on privacy of current or planned activities and to use personal information only for these activities or for compatible uses. Data subjects will be informed by the data collector about the reason and purpose of data collection and about their rights. Information users should use appropriate security mechanisms to protect the confidentiality and integrity of personal data. Information users should not use information in ways that are incompatible with an individual's understanding. Furthermore, they should educate themselves about how privacy can be maintained.

According to the 'Principles for Individuals who Provide Personal Information', individuals should obtain information about what data is being collected and for what reason, and how it will be protected. Individuals will have a responsibility to understand the consequences of providing personal data to others and will make intelligent choices on whether or not to provide their personal data. Individuals will be able to safeguard their own privacy by having the means to obtain their data, to correct them, to use appropriate technical safeguards (for example, encryption), and to remain anonymous

Downloaded by [University of Cambridge] at 17:53 09 October 2014

when appropriate. Furthermore, data subjects will have means of redress, if harmed by an improper disclosure or use of personal data.

The IITF privacy principles could raise the level of data protection in the US, especially if applied in the private sector. Unfortunately, the principles only offer guidelines for those who are drafting laws and regulations, but they do not have the force of law. Although the IITF privacy principles are intended to be consistent with international guidelines such as the Organization for Economic Cooperation and Development guidelines, they do not in some respect offer the same level of privacy protection as the EU Directive. In practice, the idea of shared responsibility of equal partners will not always work, because data subjects (such as employees) often depend on services provided by the data processing agencies (for example, employers), so that they hardly have the chance to enforce their rights themselves. Consequently, besides the right of redress, the control of an independent data protection authority is necessary to protect data subjects efficiently. In IITF 1997 it is argued that the establishment of a data protection authority could reduce the likelihood that unfair information practices are prosecuted. However, in practice it is normally more cumbersome and risky for a citizen to go to court than to appeal to a data protection authority, which acts as the citizen's lawyer. Besides, with a data protection authority that monitors and checks the observance of data protection regulations, it is much more likely that personal data abuses will be detected.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

Currently, the US and EU are discussing how the EU Directive might affect transatlantic data flow, and whether Article 25 will restrict the data flow from the EU to the US and will thus have consequences on the transborder electronic commerce. A main question in the discussion is whether 'adequacy' will be judged against the principles of the Directive or also against the methods of enforcement and oversight. The European side tends to demand the enforcement of clear requirements of legitimacy (especially purpose specification and binding) as well as an independent oversight authority, which can act on complaints of the data subjects. Currently, the American side is opposed to enact data protection legislation according to the European model and instead favours means of self-regulation for the private sector.

A recent comprehensive report, *Privacy and Self-Regulation in the Information Age*, by the US Department of Commerce (US Department of Commerce 1997) explores the benefits and challenges of self-regulatory privacy regimes. According to this report, effective self-regulation must involve substantive rules as well as means to ensure that consumers know the rules, that

companies actually do what they promise to do, and that consumers can have their complaints heard and resolved fairly.

In the USA, voluntary privacy codes have generally been developed in conformity with the OECD Guidelines, whereby some of these codes embody external mechanisms for complaints and oversight and others are merely statements of good intention (Bennett 1997). However, although several hundred USA companies signed the OECD Guidelines, few adopted their provisions in practice (Madsen 1992).

The United States argue that an omnibus privacy legislation is a feature of a continental legal system, and that the Anglo-American system based on common law dictates a less regulatory regime. According to the US tradition of self-help and judicial enforcement, more responsibility is placed on the individual to demonstrate damage and make a claim through the court. However, in contradiction to this argument, in the US there are several application-specific acts regulating privacy aspects in the private sector, such as the Fair Credit Reporting Act or the Video Rental Act. Moreover, there are other states with a English common law tradition that enforce or plan to enforce an omnibus data protection policy. For example, the United Kingdom has passed its data protection act covering the public and private sectors in 1984, and Canada is currently planning to expand its data protection legislation also to the private sector.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

Canada

In September 1995, the Canadian Information Highway Advisory Council presented their final report, *Connection Community Content: The Challenge of the Information Highway* (Canadian Information Highway Advisory Council 1995). In contrast to most other information infrastructure programmes, which were mainly influenced by input from representatives of the IT industry, the advisory council also included members from artistic, creative and educational communities, and from consumer and labour organisations. It was chaired by David Johnston, professor of law at McGill University's Centre for Medicine, Ethics and Law.

The Canadian Privacy Act of 1982 which, in contrast to the US legislation, established the Office of Privacy Commissioner, only applies to federal government bodies and agencies. Only the province of Quebec has enacted privacy legislation for the private sector. Voluntary privacy codes and standards have generally been the preferred approach of Canadian business and industry associations. The diversity of codes of practice in Canada was one reason for

the Canadian Standards Association (CSA) to negotiate a 'Model Code for the Protection of Personal Information' in the private sector with business, government and consumer groups. Also, the CSA was motivated by the EU Directive and by the fear of the possible blockage of personal data transfer from Europe.

Privacy protection and network security were one of five principles that were set up by the Information Highway Advisory Council. The council recommended that the government should continue to collaborate with the CSA, business and consumer organisations, and other levels of government in order to implement the CSA code and develop effective independent oversight and enforcement mechanisms and thereby 'legislate' the standard. This recommendation was accepted by the Federal government in May 1996. The Canadian Justice Minister has promised that such legislation will be in place by the year 2000.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

PRIVACY-ENHANCING TECHNOLOGIES

In a fully networked society, privacy is seriously endangered and cannot be sufficiently protected by privacy legislation or privacy codes of conduct alone. Data protection commissioners are therefore demanding that privacy requirements should also be technically enforced and that privacy should be a design criterion for information systems. The Dutch Data Protection Authority (the Registratiekamer) and the Information and Privacy Commissioner (IPC) for the Province of Ontario, Canada, have collaborated in the production of a report (Registratiekamer/IPC 1995) exploring privacy-enhancing technologies that safeguard personal privacy by minimising or eliminating the collection of identifiable data. The report on privacy-enhancing technologies by the Registratiekamer and IPC, and a previous study of the Registratiekamer on how to design and model privacy technologies (Registratiekamer 1995), mainly focus on privacy technologies that permit transactions to be conducted anonymously.

Extended security criteria for systems with high privacy requirements should cover a diversity of privacy-enhancing security aspects such as:

- *Anonymity, pseudonymity, unlinkability, unobservability of users*: The privacy principle of necessity of data collecting means that personal data should not be collected or used for identification purposes when not really necessary. Consequently, information systems should guarantee that, if possible, users can act anonymously.
- *Anonymity and pseudonymity of data subjects*: If storage is needed, personal data of data subjects should be anonymized or pseudonymized as soon as possible.

- Security mechanisms, such as access control or encryption, are necessary to protect the *confidentiality and integrity of personal data*, if personal data has to be stored, processed or transmitted. Such security mechanisms can also be classified as data protection technologies. In particular the privacy requirements of *purpose binding and necessity of data processing of personal data of users and data subjects* can be technically enforced through an appropriate security policy and access control mechanisms (for example, see Fischer-Hübner 1994, for a formal privacy enforcing access control model).

None of the early security evaluation criteria, such as the American TCSEC (TCSEC 1985) or the European ITSEC (ITSEC 1991), really covers user and privacy friendly functionality, as their focus is biased towards the protection of system owners instead of users and data subjects. The harmonised Common Criteria (Common Criteria Editorial Board 1998) at least cover the functionality class *privacy* for the evaluation of the functionalities *anonymity, pseudonymity, unlinkability and unobservability* of users.

Examples of privacy technologies which protect the user's anonymity at application level are electronic payment systems based on anonymous prepaid cards (such as telephone cards) or David Chaum's *eCash* which is based on blind signatures (Chaum 1992). Further examples of systems, which can provide anonymity of communication, are Anomyzers for anonymous Web-accesses (Boyan 1997), anonymous re-mailers or communication Mixes (see Cottrell 1997, Chaum 1981).

Anonymous re-mailers should allow the anonymous use of e-mail. Simple anonymous re-mailers are intermediary computers, which secretly pass messages to a recipient. However, such a re-mailer cannot sufficiently protect privacy, because a mapping of anonymous identities to real addresses must be maintained by the re-mailer which, for that reason, can be a sensitive point of attack. The Finnish re-mailer service anon.penet.fi was recently closed down, after it had been raided by the Finnish police in cooperation with the FBI.

So-called cypherpunk re-mailers enable the user to chain encrypted messages through a series of re-mailers. The structure of messages is a nested set of encrypted messages, where each message is encrypted to a re-mailer. Cypherpunk re-mailers should ensure that only the first re-mailer in the chain knows the address of the sender, and only the last re-mailer knows the address of the receiver. However, cypherpunk re-mailers can be attacked as well (see Cottrell 1997). Messages could be traced, if incoming messages to a re-mailer are directly forwarded. Even if incoming messages are delayed or reordered, an attacker could send a batch of messages after your message arrives, so that

Downloaded by [University of Cambridge] at 17:53 09 October 2014

your message will be flushed back out of the re-mailer's message pool. Besides, messages could be tracked by their size (which decreases) or by the use of active replay attacks.

A re-mailer that can guarantee anonymity effectively is Mixmaster (Cottrell 1997) which is based on the concept of Mixes (Chaum 1981). Mixmaster uses constant-length messages, includes defences against replay attacks and offers improved message reordering code to stop passive correlation attacks based on timing coincidences. In EFGA 1998, a current list of re-mailer services for the Internet with an estimation of their reliability is offered.

CONCLUSIONS

In conclusion, the global information society is at risk. A key problem is that most of the information infrastructure programmes emphasise economic opportunities and neglect social impacts. Nevertheless, democratic participation by the public in the design and development of the information infrastructure should be encouraged. Social and legal impacts of the different initiatives have to be assessed in advance and have to be periodically reviewed. High standards for security and network reliability are required.

In addition to international privacy measures, protection should also be undertaken by implementing and adapting privacy-enhancing technologies. The report of the Registratiekamer and IPC (Registratiekamer/IPC 1995) concludes that, if privacy technologies are to play a more significant role, it will be necessary to create more public awareness as well as consumer demand for them. If there is a demand, providers will probably try to respond to market forces.

Furthermore, privacy education is important to raise the awareness of the users, the data subjects, the system designers, the IT professionals and of the management. Most privacy-enhancing technologies themselves are not necessarily an effective means to technically enforce privacy aspects, unless users or customers have sufficient technical knowledge to apply them. Thus, users and customers need information and education about their rights, about the value of their personal data, about privacy risks and the possibilities of self-protection by the use of privacy-enhancing technologies.

Simone Fischer-Hübner
University of Hamburg
Faculty for Informatics
Vogt-Kölln-Str. 30,
D-22527 Hamburg, Germany
fischer@informatik.uni-hamburg.de

Downloaded by [University of Cambridge] at 17:53 09 October 2014

NOTE

From July 1998 to June 1999 the author's address is: Stockholm University, Department of Computer and Systems Sciences, Electrum 230, S-16440 Kista.

REFERENCES

Bangemann, M. (1994) 'Europe and the Global Information Society, Recommendations to the European Council' (Bangemann Report), 26 May 1994, Brussels.

Bennett, C. (1997) 'Convergence Revisited: Toward a Global Policy for Protection of Personal Data?', in P. Agre and M. Rotenberg (eds), *Technology and Privacy: The New Landscape*, Cambridge, MA and London: MIT Press, pp. 99–124.

Boyan, J. (1997) 'The Anomyzer: Protecting User Privacy on the Web', *Computer-Mediated Communication Magazine*, http://www.december.com/cmc/mag/1997/mag/1997/boyan.html

Brunnstein, K. (1997) 'Analysis of JAVA Security and Hostile Applets', in L. Yngstrüm and J. Carlsen (eds) *Information Security in Research and Business – Proceedings of the IFIP TC-11 13th International Conference on Information Security (Sec' 97)*: 14–16 May 1997, Copenhagen, Denmark, London: Chapman & Hall, pp. 293–5.

Brunnstein, K. and Schier, K. (1997) 'Global Digital Commerce: Impacts and Risks for Developments of Global Information Societies', in J. Berleur and D. Whitehouse (eds) *An Ethical Global Information Society: Culture and Democracy Revisited – Proceedings of the IFIP WG 9.2 Corfu International Conference*, Corfu 8–10 May 1997, London: Chapman & Hall, pp. 75–82.

Brunnstein, K., Fischer-Hübner, S. and Schaar, P. (1998) 'Verbraucherbefragung und Globale Informationsgesellschaft', in *Computer und Recht*, February 1998, Verlag Dr Otto Schmidt, pp. 125–6.

Budapest Draft (1996) 'Data Protection on the Internet: Report and Guidance', International Working Group on Data Protection in Telecommunications, http://jilt.law.strath.ac.uk/jilt/consult/iwgdp/default.htm

Canadian Information Highway Advisory Council (1995) *Connection Community Content: The Challenge of the Information Highway*, final report, September 1995.

Chaum, D. (1981) 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms', *Communications of the ACM* 24 (2): 84–8.

—— (1985) 'Security without Identification: Transaction Systems to Make Big Brother Obsolete', *Communications of the ACM* 28 (10):1030–44.

—— (1992) 'Achieving Electronic Privacy', *Scientific American* 8: 76–81.

Common Criteria (CC) Editorial Board (1998) 'Common Criteria for Information Technology Security Evaluation', Version 2.0, May 1998.

Cottrell, L. (1997) 'Mixmaster and Re-mailer Attacks', http://www.obscura.com/~loki/re-mailer/re-mailer-essay.html

EFGA (Electronic Frontiers Georgia) (1998) *Reliable Re-mailer List*, http://anon.efga.org/anon/rlist.html

Downloaded by [University of Cambridge] at 17:53 09 October 2014

EPIC (Electronic Privacy Information Center) (1997) 'Surfer Beware: Personal Privacy and the Internet', June 1997, http://www.epic.org/reports/surfer-beware.html

EU Directive (1995) 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, http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html

Fischer-Hübner, S. (1994) 'Towards a Privacy-Friendly Design and Use of IT-Security Mechanisms', *Proceedings of the 17th National Computer Security Conference*, October 1994, Baltimore, MD, pp. 142–52.

—— (1997) 'Privacy at Risk in the Global Information Society', in J. Berleur and D. Whitehouse (eds) *An Ethical Global Information Society: Culture and Democracy Revisited – Proceedings of the IFIP WG 9.2 Corfu International Conference*, Corfu 8–10 May 1997, London: Chapman & Hall, pp. 261–74.

Garfinkel, S. and Spafford, G. (1997) *Web Security and Commerce*, Cambridge, Köln, Paris, Sebastopol, Tokyo: O'Reilly and Associates.

Greenleaf, G. (1995) 'The 1995 EU Directive on Data Protection – An Overview', *The International Privacy Bulletin* 3 (2):10–21.

Holvast, J. (1993) 'Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?', in J. Berleur *et al.* (ed.) *Facing the Challenge of Risk and Vulnerability in an Information Society*, Proceedings of the IFIP-WG9.2 Conference, Namur, 20–22 May 1993, Amsterdam: Elsevier Science, pp. 267–79.

IITF (Information Infrastructure Task Force) – Privacy Working Group (1995) *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, final version, June 1995.

IITF (Information Infrastructure Task Force) – Information Policy Committee (1997) *Options for Promoting Privacy on the NII, Executive Summary*, April 1997.

ITSEC (Information Technology Security Evaluation Criteria) (1991) *Provisional Harmonised Criteria*.

Koch, F. (1995) 'European Data Protection – Against the Internet?', paper presented at Privacy International Conference on Advanced Surveillance Technologies, Copenhagen, September 1995.

Lundheim, R. and Sindre, G. (1993) 'Privacy and Computing: A Cultural Perspective', in R. Sizer *et al.* (ed.) *Security and Control of Information Technology in Society*, IFIP WG 9.6 Working Conference, St Petersburg, August 1993, Amsterdam: Elsevier Science, pp. 25–40.

Madsen, W. (1992) Handbook of Personal Data Protection, New York: Stockton Press.

—— (1995) 'Securing Access and Privacy on the Internet', in *Proceedings of the COMPSEC-Conference*, London, October 1995, Elsevier Science.

Mayer-Schönberger, V. (1997) 'The Internet and Privacy Legislation: Cookies for a Threat?', *West Virginia Journal of Law and Technology* 1, 1, http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm.

Downloaded by [University of Cambridge] at 17:53 09 October 2014

MITI (Ministry of International Trade and Industry) (1994) *Programme for Advanced Information Infrastructure*, Japan, May 1994.

NCB (National Computer Board) (1991) *IT2000 – A Vision of an Intelligent Island*, Singapore, August 1991.

Netscape (1997) 'The Open Profiling Standard (OPS)', http://developers.netscape.com/ops/ops.html

Registratiekamer (Dutch Data Protection Authority) (1995) *Privacy-Enhancing Technologies: The Path to Anonymity*, vol. 2, Achtergrondstudies en Verkenningen 5B, Rijswijk, The Netherlands.

Registratiekamer (Dutch Data Protection Authority)/IPC (Information and Privacy Commissioner/Ontario, Canada) (1995) *Privacy-Enhancing Technologies: The Path to Anonymity*, vol. 1, Achtergrondstudies en Verkenningen 5A, The Netherlands/Ontario, Canada.

Rosenberg, R. (1992) *The Social Impact of Computers*, Academic Press.

TCSEC (1985) *DoD Trusted Computer Systems Evaluation Criteria*, DoD 5200.28 STD, Washington, DC: Department of Defense.

US Department of Commerce (1997) *Privacy and Self-Regulation in the Information Age*, Washington DC, June 1997, http://www.ntia.doc.gov/reports/privacy/

US Government (1993) *The National Information Infrastructure: Agenda for Action*.

Westin, A. (1967) *Privacy and Freedom*, New York.

Downloaded by [University of Cambridge] at 17:53 09 October 2014