Peace Institute
Institute for Contemporary Social and Political Studies

Matej Kovačič

PRIVACY ON THE INTERNET

Matej Kovačič
PRIVACY ON THE INTERNET

Translation: Olga Vuković
Proof-reading: Michelle Gadpaille
Drawing on the front cover: A. Stewart and R. Mendez, RSA Crypto-Sardine
Drawing inside the front cover: J. Bentham, Panopticon (1791) and V. Ćosić,
Internet war map of Yugoslavia
Design: Irena Wölle
Print: Stane Peklaj

Reviewers: Goran Klemenčič, Anton Kramberger, Franc Trček

The publishing of this book was made possible by the Open Society Institute

Book Series Politike POLITIKE

Publisher: Peace Institute
Institute for Contemporary Social and Political Studies
Metelkova 6
SI-1000 Ljubljana
E: info@mirovni-institut.si
www.mirovni-institut.si

Editor: Aldo Milohnić

Contents

9 FOREWORD

11 PRIVACY, SURVEILLANCE AND TECHNOLOGY

19 SURVEILLANCE SOCIETY
24 Surveillance in the workplace and surveillance of consumers
26 Surveillance and information technology
29 Electronic panopticon
31 Surveillance and privacy
34 Protection of privacy

39 PRIVACY IN CYBERSPACE
42 Collecting information about computers in a network
43 Electronic traces left with Internet providers
44 Electronic traces at content providers
49 Linking and gathering of distributed data
51 Intercepting data in a network
52 Intercepting electronic messages
54 Intrusions into computer systems
57 Intercepting data and information in the immediate environment of the system

59 THE PROTECTION OF PRIVACY IN CYBERSPACE
60 Anonymization
62 Protection against data interception
65 Protection against intrusion and stealing of data
67 Deleting electronic traces
68 Protection against TEMPEST attacks
69 Cryptography and the movement for electronic privacy

75 SLOVENE LEGISLATION AND PRACTICE
75 Territorial privacy
76 Privacy of communications
80 Privacy of information

87 CONCLUSIONS

89 BIBLIOGRAPHY

99 GLOSSARY

I would like to express special thanks to Slavko Splichal, PhD, from the Faculty of Social Sciences, University of Ljubljana, for his tutorial which made this book possible. I am also indebted to Matjaž Robinšak, Gorazd Kovačič, several memebers of Slo-Tech and Jernej from aufbix.org who suported my work on this book. I am also grateful to Jože Bogataj, MA and Jožef Šantavec, MA of the Inspectorate for Personal Data Protection, Marko Bonač, MA, director of ARNES (Academic and Research Network of Slovenia), Gorazd Božič, head of security centre SI-CERT, Tone Kramberger, PhD and Franc Trček, PhD from the Faculty of Social Sciences, Ljubljana and Vuk Ćosić; they have kindly provided critical comments on the first version of the manuscript. For critical reading and many very useful guidelines I would like to thank Goran Klemenčič, MA from the Councel of Europe.

FOREWORD

In 1976 the magazine *IEEE Transactions on Information Theory* featured a ten-page article by mathematicians Whitfield Diffie and Martin E. Hellman titled »New Directions in Cryptography«. The article described the protocol for the safe exchange of encryption keys via an unprotected medium, and the idea of an encryption system using public keys was born.

One night in April one year later, while laid up with a massive headache (Dupuis 1999), Ronald L. Rivest thought up a new coding algorithm that would be based on the system of public keys and would enable digital signatures. He wrote down the algorithm and sent it to his colleagues Adi Shamir and Leonard M. Adleman. The three authors, who at the time were newcomers to the area of cryptography, described the problem in a scientific article and submitted it for publication in *Scientific American*. The article was published in September 1977. The authors offered to send technical details of the algorithm free of charge to anyone submitting a self-addressed, stamped envelope. They received thousands of requests from all over the world. Another article by the same authors titled »A Method for Obtaining Digital Signatures and Public-Key Cryptosystems« appeared one year later in *Communications of the ACM*. It contained an explanation of the algorithm, which was named RSA after the initials of the authors (RSA Laboratories 2000, 12). The RSA algorithm proved to be an exceptionally powerful cryptographic system, meaning that the messages coded using this algorithm were extremely difficult to break.

Fourteen years later, in 1991, the computer programmer Philip R. Zimmermann wrote PGP (*Pretty Good Privacy*), a PC-based program for the coding of electronic messages and electronic files based on the RSA algorithm. The program was not only user friendly, according to the standards of the time, but also highly efficient. The year of its publication was the year in which the US Senate discussed a bill

envisaging heavy restrictions on the use of cryptography in civilian matters. In order to neutralize the impact of this law, should it be adopted, Zimmerman released his program as freeware, placing it on the Internet and allowing free copying. Within a relatively short time the program spread across the world.

One would expect that these apparently unimportant events occurring over a span of 15 years would be of interest only to a handful of mathematicians and computer experts. But developments took a different turn. In reality, this apparently inconsequential mathematical discovery proved to have much greater influence than anyone could have imagined at the end of the 1970s. This event, and in particular the implementation of the RSA algorithm, spurred into action the US judicial system as well as the inteligence services. And nothing was ever the same again.

PRIVACY, SURVEILLANCE AND TECHNOLOGY

We live in a society which, on the one hand, places stress on individuality and privacy, but on the other, we are also witnessing an increase in surveillance. Surveillance is frequently linked to the level of democracy or to the authoritarian character of a society. It undoubtedly affects privacy but is also connected with security and organization. Yet can one say that surveillance in itself is good or bad?

When studying privacy and surveillance, one necessarily encounters the paradox of its duality. Surveillance is both good and bad. Today surveillance of individuals is a means of social control and of ensuring social participation. Furthermore, we cannot overlook the close connection between surveillance and technology. Information technologies are intended for the collection and processing of all types of data and information – data and information about the society and environment in which we live, and about the individuals surrounding us. The information society *is* a surveillance society. It is not surprising then that contemporary information technologies have such a high significance for national security and that the issues of privacy are addressed with increasing frequency by political activists, civil society representatives and trade unions.

Any study of surveillance and privacy sooner or later brings us to the issue of technology. Technology as such is not good or bad either. The essential question is the purpose of its use – many technologies can be exploited for purposes that no one could have imagined at the time of their advent. This conclusion is applicable not merely to specialized technologies, but also to those that are already used, or will be soon used on a mass scale.

The caller ID service only became widely known in Slovenia with the introduction of GSM telephony and ISDN fixed telephony, although the technology was developed in 1987. The identification of

the caller's ID number has several obvious advantages. During a trial period in Canada in 1991, the police recorded a dramatic decrease in the number of obscene anonymous telephone calls and harassment by phone (Lyon 1994, 149). But in the US opinions were nevertheless divided, because the possibilities for abuse became obvious before long. Soon after the digitalization of the telephone networks in the US and the introduction of ISDN telephony in the 1990s, American companies began to exploit the caller ID facility for socio-economic and geo-demographic purposes. On receiving a telephone call, a company could now retrieve from its database consumer's profile and even his/her preferences. This triggered protests on the part of consumers, because, on the one hand, database information was in many cases either outdated or inaccurate, while on the other, this information was occasionally used to discriminate against specific types of consumers on the basis of their demographic profile, particularly race or residential location.

It is well known that the source of a radio signal can be located quite accurately using the triangulation method. This method is used for the detection of illegal radio stations, as well as in rescue actions e.g. of wrecked ships, by radio amateurs and so on. But it can also be used to locate mobile phone users, since mobile telephones transmit radio signals too. Roughly speaking, two methods are in use: a terminal-based (or a handset-based) solution, where the location is identified and transmitted to the network by the mobile device itself, and a networked-based solution where the location is determined by the network (Leskovšek 2001, 19). Terminal-based solutions are very accurate (with a range accuracy as low as 50 to 5 meters), but also rather costly. In addition, their implementation would be a long process since it would require the replacement of all mobile handsets with new ones that support the location identification option (e.g. using the GPS satellite navigation system). Much cheaper and more readily accessible, although less accurate (100 to 1100 meters), are network-based services; some are already in use (Leskovšek 2001, 20).

Mobile services constitute an important market niche for GSM operators. The identification of the user's location enables the localization of information services, tracking of users, provision of navigational services, management of geographically dispersed resour-

ces and the like (Leskovšek 2001, 21). For example, the US company Streetbeam already markets its products by sending SMS to mobile telephone users who approach their advertising points.[1] This type of advertising is undoubtedly bound to evolve towards interactive advertising billboards which will be capable of detecting and identifying the user and sending personalized advertisements. Of course, the identification and recording of the location may also have negative consequences for the user.

On November 4th, 1996 the *Resolution on the lawful interception of communications* was published in the Official Journal of the European Union (ref. C 329, pages 1–6). The first part of the resolution includes the statement that legally authorized interception of telecommunications is an important tool for the protection of national interest, in particular national security, and the investigation of serious crimes. The second part lists a series of detailed requirements that must be fulfilled by telecommunications companies. Among these is a requirement to supply on request information about the location of a mobile telephone user.[2] One problem in connection with this is the storage of data. Article 15 of EU Directive 2002/58 about the processing of personal data and privacy protection in e-communications allows the storage of traffic data for a limited period of time (Možina 2002, 4). Since this enables EU member states to prescribe the duration of data storage for telephone operators (among those is information about the location of the user), state authorities can trace every movement of virtually every individual. Some law experts have thus stressed that the privacy of location deserves legal protection equal to that accorded to communication content (Možina 2002, 5).

Today it is almost impossible to imagine life without ID cards and smart cards which enable us to carry out everyday tasks such as shopping, or to access health services. However, the initial purpose of identification cards was to enforce the registration of enemies of the state (Banisar et al. 1999). Identification cards were first intro-

1 For more on this see http://www.streetbeam.com.

2 The same demand is found under item 6 of Article 4 of the proposal for the Rules about Software Applications and Interfaces for Lawful Interception of Communications, prepared by the Ministry of Information Society and submitted to public discussion on December 20th 2002.

duced in the Netherlands during the Nazi occupation, following a proposal by the Dutch statistician Jacobus Lambertus Lentz. These ID cards included a photograph, a fingerprint and a signature, but also information on whether a person was of Jewish nationality. Black maintains that ID cards were the first step towards the realization of the Holocaust in the Netherlands, since identification was followed by deportations (Black 2002, 388–389).

In addition to personal ID cards, various other cards such as bank or shopping cards which carry information on the user's identity may also be classified as identification cards. Unlike ordinary identification cards, which carry only pre-defined information, smart cards include a memory chip where data are stored in the process. The most important argument in support of smart cards is that they enable users to have better control over their personal data (Lyon 1994, 150). However, as Lyon pointed out, the use of smart cards also enables the merging of public (government) and commercial (private) databases. In Slovenia, for example, the idea of using health insurance cards for the identification of students has already been proposed some time ago. Even though no major technical obstacles stand in the way of such a solution, the legal restrictions would very likely be insurmountable. As Chaum has concluded, the use of such cards poses an increasing threat to privacy (Chaum 1996, 235).

Biometry is the process of collection, processing and storage of data about the physical characteristics of individuals for the purpose of their identification. The most popular forms of biometry are iris scan, hand geometry, fingerprint and thumb print scans, and voice and face recognition. Other systems are currently in the process of development, among them typing and pen usage pattern recognition (speed of writing, pressure of the pen etc.). The international airport Ben Gurion in Tel Aviv, where hand geometry scanning is already in use (Mesenbrink 2002), and Amsterdam's Schiphol airport, which uses iris scans (Amsterdam 2001), are proof that these technologies are not science fiction. After the September 11th attacks, airport security providers at several US airports began to consider the use of face-recognition systems. This system was already in use in Tampa, Florida, by January 2001, while in July 2001 a similar project that should facilitate the tracking down of criminals and missing children was launched in Virginia Beach (EPIC 2002).

An even more controversial biometric method is DNA identification. According to the Privacy and Human Rights Report, the police forces of several countries, among them the US, Germany and Canada, were establishing national databases of DNA samples (Banisar et al. 1999). There is no doubt that biometry opens new surveillance options, so it comes as no surprise that the ideas about the general use of biometry at airports were put forward soon after the terrorist attacks on New York on September 11, 2001 (Manjoo 2001).

Despite the fact that wiretapping and secret video taping in private facilities are prohibited, many countries – among them Slovenia – do not legally restrict the sale of audio bugs and secret video surveillance cameras. This equipment is relatively cheap and accessible to a broad segment of consumers. The Privacy & Human Rights Report includes an estimation made in 1996 that 200,000 bugs were sold each year in Britain, with this number being even greater in Asian countries (Banisar et al. 1999).

Similarly, CCTV systems (Closed Circuit Television System) are today massively used in public buildings and public spaces. According to an interim report on the technologies for political control by the STOA research team (Scientific and Technological Options Assessment of the European Parliament), the technology of visual surveillance has dramatically advanced recently. Its hardware components have been reduced to miniature proportions, while the use of state-of-the-art technologies and new algorithms enables comparison, storage and collation of recorded images. One such example is vehicle recognition systems that have been available on the market since 1994 (STOA 1998). Their basic purpose is the monitoring of traffic, but they can be used to identify the registration numbers and monitor the movement of vehicles.[3] The authors of the STOA study have concluded that »we are at the beginning of a revolution in 'algorithmic surveillance' – effectively data analysis via complex algorithms which enable automatic recognition and tracking« (STOA 1999). According to this report, these systems have even found their way into the capital of Tibet, even though

[3] The Canadian Ministry of Transportation web page includes interactive maps of three highways and images recorded by the cameras installed on these highways; http://www.mto.gov.on.ca/english/traveller/compass/.

the city has no difficulties whatsoever with traffic. The Chinese government used a similar system during the 1989 student protests at Tiananmen square for the identification of protest leaders (STOA 1999).

The power of video surveillance in combination with other technologies such as movement detection, enlargement techniques and infrared cameras, can be augmented still further. Another method of implementing visual control is by means of satellites. Satellite images are already used for various purposes, for example, in reports from crisis spots, to assess the scope of damage caused by environmental disasters, and even to detect unlawful construction sites (Banisar et al. 1999). Satellite surveillance is not limited to state agencies only, but it also includes commercial variants.[4] In addition, it enables the linking of satellite pictures with GIS databases (Geographical Information System) and through them with other databases.

The development of wiretapping technologies is no less fascinating. »Wiretap friendly« phone systems make wiretapping a simple task (Banisar et al. 1999). In 1994 the US introduced the Digital Telephony Act stipulating that the telephone switches used by telephone companies should include remote wiretapping ports. This considerably facilitated the work of the FBI. Today all new telephone switches have the remote wiretapping option, but the problem is that these switches are also available to private persons (e.g. companies) who are not subject to such strict supervision as public telephone operators.

Of course, these interception and wiretapping technologies are also present in virtual space. As early as 1994, in his testimony before the US Senate, Phil Zimmerman alerted the public to the interception of electronic messages, saying that, thanks to modern technology, this task was routine, automatic and discreet, and could

[4] In 1998 *Microsoft* installed *Terraserver* (http://terraserver.microsoft.com/). This server offers satellite images of the earth recorded in 1992 by Russian spy satellites from a distance of 230 km (Microsoft bought these images from the Russian-American company SPIN-2 after they ceased to be categorized as confidential). It is even possible to buy these images, but most intriguing is the clarity of the pictures and their high quality – objects measuring just two meters in perimeter are clearly identifiable. Similarly, the Slovene Environmental Agency published an on-line interactive atlas available at http://212.103.140.243/nvatlas/. It provides aerial photos of the entire territory of Slovenia enabling search and display of any facility in Slovenia.

be performed on a large scale (Zimmerman 1993). Today this type of surveillance is already in place on the Internet. The system in question, to which I will return later in this book, is called Carnivore. In addition, there are other computer programs for mass control of electronic messages – these determine, for each message, the likelihood that it is suspicious, with those deemed most suspicious being analyzed by man.[5]

The Privacy & Human Rights Report states that in 1998 the European Parliament obtained evidence that the American National Security Agency »in collusion with the British Government has created the means to intercept almost every fax, email and telephone call within the European Union« (Banisar et al. 1999). The system in question is called ECHELON and was originally developed to intercept communications by the former Soviet Union, China and other countries that jeopardized (or were alleged to jeopardize) the security of west European states and the US. In its report to the European Parliament dated May 4th, 2001, the EU Temporary Committee on the ECHELON Interception System wrote that »the system for intercepting communications exists ... What is important is that its purpose is to intercept private and commercial communications, and not military communications« (Temporary Committee on the ECHELON Interception System 2001, 88).[6]

Notwithstanding the agitation caused by the report on ECHELON, the European Union has set itself the objective of harmonizing national legislations on wiretapping[7], meaning that the surveillance

5 SpamAssasin (http://spamassassin.taint.org/) is a computer application designed for the detection of spam mail. The application allocates a certain number of points to each mail item, with greater number of points indicating an increased possibility that the message is spam. By using redirecting filters, a message can be forwarded to various addresses on the basis of the number of points. The points can be attributed according to user defineable criteria.

6 An action entitled Jam Echelon Day, intended as a sign of protest against the global surveillance system, was organized in October 2002. The organizers invited Internet users to send as many as possible messages containing words that would spur Echelon into action, for example, »weapons«, »drugs«, »terrorism«, »Bush« etc. The action was intended to overtax the Echelon system. It is not clear whether this could really overtax the system, but it surely raises the awareness of Internet users regarding this problem (Oakes 1999).

7 An interesting article was published in 1999, in the first issue of European Dialogue published by the European Commission in ten languages. The subject is the combating of serious crimes: »Criminals can exploit differences among different states legislations ...

of communications is being globalized. This has also been confirmed by the Working Group on Police Cooperation, in a report dated June 1995 where it is stated that new telecommunications systems represent »a global problem, which looks like it can only be controlled by global cooperation« (Statewatch Report 1999). According to the EU officials, legally permitted interception of telecommunications is an important instrument for the protection of national interest, national security and investigation of serious criminal offenses (Council Resolution 1996, 1–6).

With our society being indisputably characterized by a high level of surveillance, it seems appropriate to raise the question of its purpose and consequences. This essay is devoted to the issues of surveillance and privacy in contemporary information society, while placing stress on the specific features of the Internet. I shall examine existing conditions in the area of privacy in Slovenia and attempt to provide certain guidelines for the more efficient protection of privacy.

In light of endeavours to close legisalation gaps, Commission recommends the state members to arrange an agreement about equable treatment of criminal offences...« (Watson 1999, 26).

In February 1999 the European Commission and the Council of Europe launched a program 'Octopus II', designed to help countries of Central and Eastern Europe and Russia to fight organized crime. This program was a sequel to Octopus I which was carried out from 1996 to 1998. The intention of Octopus II is the adoption of all the acquis communautaire in the field of justice and home affairs. Octopus II will organise joint seminars, workshops and study visits, which will bring together representatives of the participating countries (Agence Europe, 3. 2. 1999, Brussels).

SURVEILLANCE SOCIETY

The issue of (social) control was among the most important subjects of sociology in the 19th century. Sociologists argued that social control was positive and that it was a prerequisite for order and for the coexistence of people in society. Ross argues that effective cooperation among individuals requires a high level of social order (Ross 1969, 2), while a high level of social organization presupposes some kind of control or surveillance. But society also needs an authority to delimit the conflicting interests of individuals. According to Ross, in static societies habit can be a substitute for authority, while in changing societies this authority must be external (Ross 1969, 40). He also argues that institutions of an artificial order are necessary because of social inequality and economic differentiation (Ross 1969, 42, 56).

Cooley holds a similar opinion. According to him, if there exists a certain whole, a certain community, the objective of the individual should be to serve that community; life in a bigger community calls for self-control and discipline in organizational matters (Cooley 1993, 39, 152). Cooley further argues that no individual exists outside society and that there is no freedom without organization. In his opinion there are two types of individuality: one is the individuality of isolation and the other the individuality of choice. The latter is desirable in social life because it makes life rational and free rather than random and local (Cooley 1993, 47, 93).

This led many sociologists to see primarily the positive side of surveillance. »The very idea of truth and reason in human affairs can hardly prevail under a system which affords no observation to corrborate it.« (Cooley 1993, 185). In his opinion, »modern democracy aims to organize justice, and in so far as it succeeds it creates a medium in which truth tends to survive and falsehood to perish.« (Cooley 1993, 184). Viewed from this perspective, surveillance of individuals does not have negative connotations, since social control is

concentrated or dispersed in proportion with people feeling the need for guidance and protection (Ross 1969, 78). Both Ross and Cooley entertained ideas about self-aware individuals and self-control. Cooley's ideal was an individual who would be self-aware and committed to his/her work, while perceiving himself/herself as part of a large and cheerful whole.

On the other hand, control was also treated as an activity performed by social subjects, primarily state agencies and capitalist entrepreneurs with a view to achieving specific objectives. Marx viewed control from the perspective of the struggle between labor and capital; for him, surveillance of workers was a means of exerting managerial control in the interest of capital whose purpose was to ensure competitiveness – i.e. maximization of production – while keeping costs at the lowest possible level.[8] Accordingly, surveillance of workers was aimed at achieving their compliance and discipline, so for Marx it had negative connotations. Weber associated surveillance with the organization and efficiency of bureaucracy. For Weber, a rational administration was a combination of knowledge and discipline, while rationality of a modern organization manifests itself through book keeping or record keeping based on written documents (Lyon 1994, 7, 25–26).

One of the most important theoretical shifts in the study of control was introduced by Michel Foucault. While both Marx and Weber treated surveillance as a means of control, Foucault brought into focus another perspective – the relation of surveillance to power and discipline. Foucault thus speaks about the »disciplining of the bodies« (Foucault 1984, 138). He argues that in the course of the 17th and 18th centuries the disciplines became general formulas of domination. Modern societies developed various instruments of disciplining that invariably include the techniques and strategies of power, so Foucault named them »disciplinary societies«. In his words, the objective of discipline is to produce »subjected and practiced bodies, docile bodies« (Foucault 1984, 137–138). He maintains that the disciplining mechanisms developed by modern societies subtly and indirectly enforce the normative performance of individuals and, since

[8] This type of surveillance was taken to an extreme by Taylorism, or scientific management, which was based on close monitoring and recording of work and work movements, written reports and so on. Its intention was to increase productivity.

individuals are disciplined through surveillance, Foucault argues that surveillance is a means of subjection.

In formulating his influential theoretical approach to surveillance, Foucault drew on the Panopticon, a model presented to the British Government by Jeremy Bentham in 1791. The main effect of the Panopticon is the maintenance of control by creating in prisoners the impression that they are incessantly watched by an invisible eye. What is essential here is the invisibility of the observer, which inspires in prisoners a feeling of uncertainty and through it triggers the mechanisms of self-control. Foucault thus says: »He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.« (Foucault 1984, 202).

According to this view, power is not a possession but a strategy. The panoptic effect is attained by exploiting uncertainty to achieve voluntary subordination of individuals. Observation should therefore be asymmetric or hierarchical. Lyon noted that the asymmetric gaze has become part of the modern project of destroying certainty (Lyon 1994, 65). The awareness that one is constantly visible induces voluntary subordination, that is to say, the establishment of domination on the micro-level, while visibility becomes a kind of trap.[9] According to Foucault, the Panopticon is a political technology which operates through subtle coercion and sustains power. It helps to maintain the fundamental balance in society, so modern society is afraid to eliminate surveillance.

Foucault directly links surveillance to the subjection of individuals and their disciplining. The panoptic effect was also the subject of George Orwell's widely acclaimed novel *1984* where he described a totalitarian society in which the mysterious Big Brother exerts control by way of telescreens, with an individual never knowing whether or not he is being watched. The consequence of such surveillance is a high level of self-censorship and eventually, a fully totalitarian society. Or, as Servan says in the foreword to Foucault's *Discipline and Punish*:

[9] Examples of the panoptic effect are surveillance of polling or video surveillance in department stores.

»A stupid despot may constrain his slaves with iron chains; but a true politician binds them even more strongly by the chain of their own ideas; it is at the stable point of reason that he secures the end of the chain; this link is all the stronger in that we do not know of what it is made and we believe it to be our own work ... and on the soft fibers of the brain is founded the unshakeable base of the soundest of Empires« (Servan in Foucault 1984, 102).

Control in the form of property registration and censuses was introduced, as Lyon observed, with the intention of establishing order and obtaining a clear picture, and consequently, of reinforcing power. Furthermore, the origin of control is closely related to the perception of time in modern society. In contrast to traditional societies, work routines in the modern environment are tied to the clock which coordinates human activities. During the early stages the timetable and the clock enabled the capitalist manager to achieve day-to-day monitoring and control of workers (Lyon 1994, 34–35, 46). Today, the role of the clock has been transferred to the computer, which has been increasingly taking over the function of coordination of human activities in time-space.

Systematic mass surveillance, as we have come to know it in modern society, emerged with the advent of military organizations, industrial towns, state administrations and capitalist enterprises, but it made a quantum leap in the 20th century with the introduction of information technologies and microprocessors. As a consequence, privacy became a serious problem.

Beniger says that information processing is fundamental to every objective-oriented activity (Beniger 1986, 434), so it is no wonder that surveillance is so closely connected with modern organizations. Frank Webster concludes that »organisation and observation are Siamese twins, which have grown together with the development of the modern world« (Webster 1995, 54). Beniger hence speaks of the *control revolution* in the 20th century and compares it to the industrial revolution of the 19th century. The essential feature of the control revolution is the possibility of exploiting information (Beniger 1986, 427), which is an issue related to both organization and technological development.

An important element of modern control is the production of individual dossiers (in the form of databases), which has led Lyon to use

the term »dossier society« (Lyon 1994, 29–30). Individuals are ever more reduced to their own dossiers. One virtually cannot exist without being subject to surveillance and without a record about him/her existing somewhere. Therefore, by participating in social life (by exercising civil rights, health insurance rights, employee's rights), we submit to surveillance. The dossiers can be used to control the activities and needs of people, but they also enable control over past events. Since control is embedded in every type of organization, it is practiced by both the state and the private sector. This said, we have to point out that the driving force behind this process is increasingly the private sector. Control affects individuals both as consumers and as citizens. While the state uses control to ensure external and internal security and to execute administrative tasks, capitalist organizations take as their starting point individual freedoms, while trying to identify consumer's wishes as accurately as possible and to adapt their offer accordingly. Control, therefore, takes on the form of the »supervision of people«, mainly exploited by the state and the ruling powers, and of »data gathering«, which is the basis for the supervision of consumers (Lyon 1994, 11).

Even though stress is placed mainly on the negative aspects of surveillance, it also has its positive side. It facilitates provision of security and maintenance of order, and in relation to organization, it introduces order into social life. Therefore, when studying control we confront an interesting paradox (duality): it is a means of both social control and of ensuring social participation. Lyon has observed that surveillance expanded with democracy since it is closely connected with the demand for equality. The demand that all citizens should be treated equally and be able to exercise their rights entails a need for the differentiation of individuals (Lyon 1994, 24, 31).

Modern society displays a growing trend towards an even higher degree of control. Data classification, gathering and recording is in the process of expansion, while the lives of ordinary people have become increasingly transparent. The ambition of the state is to see and to have control over everything, and that of private enterprise is not much different. »Surveillance is maximized in the modern state« says Giddens (quoted in Webster 1995, 70). Webster therefore suggests that the term »surveillance society« would be more adequate than »information society«.

Surveillance in the workplace and surveillance of consumers

As already pointed out, control is not limited to the state but is also exploited by private companies. One crucial element of 20th century capitalist management is surveillance of the labour force, a doctrine that has been taken to its extreme by Taylorism. Surveillance of employees involves several conflicting interests. Klemenčič mentions the interests of three subjects. One is the *interest of the employer*, who is usually the owner of the work equipment (computers, telecommunications network and other hardware) used by employees. The employer's interest is for this equipment to be used in accordance with its intended use, to prevent abuse and to detect and sanction transgressors. The ultimate objective is the reduction of costs and higher productivity. On the other hand, there is the *interest of the employee*, who expects a certain level of privacy and autonomy in the workplace. It has special implications in cases where the employee has not been acquainted beforehand with the surveillance of telephone communications or electronic mail, or has not given express consent. Unlike in the US, where in principle employee privacy is not legally protected but these issues are left to the discretion of individual companies, European legislation is much more protective of employees. In the well-known case of Halford, the European Court for Human Rights stated that an employee justifiably expects privacy in the workplace. Similarly, the Recommendation of the European Council R(89) 2 specifies that employees have the right to establish personal and social contacts at work. Finally, there is also the interest of the *third party*, one who communicates with an employee and is not necessarily aware that a specific communication act involves the use of work equipment that is subject to surveillance (Klemenčič et al. 2001, 188–189).

Technically and organizationally, surveillance in the workplace is becoming increasingly easy, especially so in companies which use their own telecommunications equipment (e.g. telephone switches, e-mail servers etc.) featuring surveillance options identical to those used by public telecommunications operators, even though private telecommunications networks are far less supervised than public networks (or not supervised at all). Nevertheless, both the legislation

and the judicial practice specify that employees justifiably expect a certain level of privacy in the workplace and that they must be acquainted with and give their consent to any intrusion into their privacy, while the scope and form of surveillance should be reduced to a minimum which, however, still enables the attainment of the objective of such surveillance. Finally, protection of the privacy of any third party must also be taken into account.

Yet commercial companies do not limit themselves to the surveillance of employees, but, in their attempts to improve the organization of their businesses, they have begun to collect data about their customers and consumers. The roots of this practice date from 1920 when Alfred Sloan of General Motors, US, began to collect consumer data and build customer profiles. The gathering of socio-economic and geo-demographic data thus became part of market research (Lyon 1994, 139). In 1930 IBM pioneered a commercial solution for this type of surveillance of consumers. This trend continued later with the demand for freedom of information (e.g. *Freedom of Information Act* in the US), so even census data became publicly accessible and were linked to other data gathered by commercial companies. Batagelj, for example, gives the example of Abacus Alliance, US, one of the biggest providers of consumer databases. Abacus was collating data on on-line purchases. In 1997 there were more than two billions sales transactions (Batagelj 1997).

The introduction of new management concepts and post-Fordist production models, in which the significant environment of an organization has been expanding ever more widely, added to the importance of consumer surveillance. The *just-in-time concept* based on the principle of no-stocks, in which supply is closely matched to demand, is one direct generator of the need for consumer surveillance. Another such concept is *Total Quality Control*, which strives to build consumers' wishes into production.

The importance of amassing consumer information became even more obvious in the period 1980–1992 when direct-mail marketing reached such proportions that the market became saturated and the effect of direct marketing dropped below the desired level. Companies thus began to distinguish consumers on the basis of their geographical location, following the realization that the US postal code was a good indicator of material status. Over time social,

psychological and demographic data were also added to the repertoire of differentiating factors, and statistical analysis of consumers' responsiveness (responsegraphics) was introduced (Batagelj 1997). Current trends move in the direction of increasingly individual treatment, for example, personalized letters and advertisements. Of course, this generates the need to gather more and more items of information about a consumer. Even though information is ostensibly gathered to the benefit of consumers, with the aim being the adaptation of the product offer to the consumers' tastes and wishes, the information so obtained can lead to discrimination against certain groups, on the basis of either their buying power or their preferences.

Information technology is indispensable for this kind of data collection and analysis, particularly in dispersed (decentralized) control. The main reason is that it enables exceptionally efficient collation of data.

Surveillance and information technology

Surveillance would undeniably be in use even without information technology, but it would not be as thorough and all-pervading. The history of the census is a good illustration of the advantages introduced by information technology.

The census has always been an issue of huge importance for state administrations, but it also presented a formidable task. The biggest problem was the analysis, not the gathering, of data. In the pre-computer era the sorting, cataloguing and counting of data was a time-consuming and labor intensive task. Towards the end of the 19th century Herman Hollerith invented a special device for data processing. Hollerith's machine, as it came to be known, is held to be the predecessor of the computer. The device was first used in the US for the analysis of the 1890 census data, and the savings amounted to approximately 5 million dollars. Hollerith's device made data analysis both cheaper and faster. The benefits were soon recognized not only by governments but by commercial enterprises as well. Yet the faster and cheaper analysis also brought, in addition to numerous advantages, previously unknown dangers. So the Third Reich exploited Hollerith's machine in its 1933 census, with one of the

objectives being the identification of the Jewish population (Black 2002, 70). The next steps were the confiscation of property and deportations (Black 2002, 77).

Gary T. Marx has observed the following characteristics of modern technologies for electronic control: they are invisible or of low visibility; involuntary (not focused on a specific goal); capital rather than labor intensive, decentralized, and not targeted at a specific individual but at categories (Lyon 1994, 68).

Bentham's plan of the Panopticon dating from 1791 anticipated visual control, but visibility in the information society is no longer merely visual. The major part of modern surveillance is invisible and resides in the realm of the digital signal. It is present in everyday life and pervades our day-to-day errands. In 1983 David Burnham alerted us to the *electronic traces* left behind by individuals. Every time one picks up the phone, or uses a credit card, or a cash machine, or goes to the bank, or to the doctor, or gets married, or uses a mobile phone, or does anything similar, a system or institution *perceives* that event and makes a *record* of it. An electronic trace is a piece of information that points to person's actions and is stored routinely. The major part of this information, which Burnham named *transaction data*, is recorded and stored, if only for a limited period of time. But we should not forget that, in addition to the storage option, modern surveillance systems also have the capacity to create and destroy data and information. Accordingly, another pertinent issue is the reliability of stored data (Lyon 1994, 59).

The enhanced surveillance capacity arises from the fact that gathered data can be *collated*. By collating and processing data it is possible to obtain a new brand of information that can be harmful for an individual and even dangerous in terms of threatening the rights of the individual (Čebulj 1992, 8). The main feature of modern information and communication technologies is precisely the collation and combination of various data. Consequently, if information is not adequately protected, the data gathered can become accessible, by chance or intentionally, to persons or institutions that are not authorized to use them, or these can begin to exploit the collected data differently or for different purposes than were originally intended. This provides good grounds for apprehension that various state institutions or other individuals have access to data that were

collected for other purposes, or that originally unrelated databases have been linked using various identification codes[10] and their information combined (Webster 1995, 68, and Raab 1993, 89). Of course, the development of information technologies only widens the possibilities of recording and collating electronic traces.

As Rule observed, two dangerous trends in the development of surveillance systems can be identified. Both prevent individuals from being fully aware of the scope of control. On the one hand, individuals themselves set these systems into operation through their actions, for example, by paying with a credit card, entering the vision field of the surveillance camera and the like, and on the other, these systems also look up and check information on their own using secondary sources (in Lyon 1994, 40–42). The potential for inaccuracy and mistakes occurring during the indirect collection of data, and particularly the fact that individuals cannot know how their personal data are used, led to the provision found in Article 8 of the Slovene *Protection of Personal Information Act* which specifies that, in principle, personal data may be obtained only directly from the person in question.

Computer technology, with the help of advanced statistical techniques and data mining, also introduces new dimensions of control. Coupled with artificial intelligence, it even steps into the area of prevention and anticipation. The panoptic technology, therefore, does not wait for an act or event to happen but takes measures in advance based on collected data and on estimates. This poses a threat to one of the fundamental legal principles in democracy, the presumption of innocence until proven guilty, and opens new possibilities for various forms of discrimination based on observations and estimations made by artificial intelligence systems. Despite all, prevention has definitely been an increasingly important trend in the development of modern surveillance systems.

[10] In Slovenia such a code is the *EMŠO* – citizen's unique personal number; in the US this is a *Social Security Number*, in Canada *Social Insurance Number*, in Great Britain a *British National Insurance Number*, in Australia a *Tax File Number*, and so on. It is interesting to note than many of these identification codes were originally introduced to ensure social rights, and the recognition that it could be used for the linkage of data came only later.

Electronic panopticon

James Rule argues that capacity of modern surveillance systems depend on four factors: the size of files held in the system; the degree to which these systems can be centralized; the speed of data and information flow between points within such a system; and the number of contact points between the system and the subject. The power of surveillance systems has been radically increased through the use of computers, so Rule is convinced that only the limited capacity of surveillance systems sustains the thin wall that separates us from a society of total control (in Lyon 1994, 51–57).

To return for a moment to Foucault's theory, one could say that the most important characteristic of panoptic surveillance is its invisibility and asymmetry. An imperceptible control that is always potentially present achieves the effect of subjection by exploiting uncertainty. In relation to this, Merton's theory of self-fulfilling prophecy is also interesting. According to Merton, people respond not only to the objective characteristics of specific circumstances, but also, and at times primarily, to the meaning (sense) they themselves ascribe to these circumstances (in Gantar 1993, 62). He further argues that a self-fulfilling prophecy operates in such a way that erroneously or unrealistically defined circumstances induce a new manner of behavior which, in turn, causes the erroneous definition of circumstances to become true. Therefore, the quality of circumstances is not of crucial importance – what is essential is how people perceive specific circumstances (in Gantar 1993, 63). Močnik goes even further. When analyzing the relation of knowledge and belief he, like Merton, concludes that for an entirely untruthful statement to become true it suffices that a »sufficient number of people believe that it is true« (Močnik 1985, 21). Močnik uses the term »hypothetical idiots« to refer to those gullible people who believe such a statement. According to him, an untruthful statement can be turned into a truthful one not only through the conviction of such hypothetical idiots; rather, the mere presumption of a sufficient number of people that these hypothetical idiots exist suffices – and the result is the same as if these hypothetical idiots really existed. It is not necessary that an individual believes in an untruthful statement – he/she may be aware of its untruthfulness – it suffices that he or she supposes

that others believe it to be truthful and acts in accordance with his/her predictions about their conduct. Močnik argues that »the belief function is fulfilled even if it is limited to the belief that there is a subject who is supposed to believe« (Močnik 1985, 23).

These theories can help us elucidate the totalitarian potential of modern surveillance technologies. The mere conviction that surveillance made possible by these technologies is present can operate in a way proposed by the above-mentioned theories. The authors of the Privacy & Human Rights Report assert that modern surveillance technologies have a strong chilling effect, since they can avert people from 'standing out' or exercising certain rights, for example, the right to protest democratically (Banisar et al. 1999). The question that is justifiably being raised is whether actual instances of electronic surveillance, or merely the fact that they exist, have panoptic power? There is no doubt that information and communication technologies potentially threaten the rights and freedoms of individuals. Most importantly, their use could alter the balance of power in society. The reason is that, on the one hand, access to databases is linked to power (it is monopolized), while on the other, the establishment of a huge and decentralized surveillance system requires considerable funds and time. According to the 1999 Privacy & Human Rights Report, surveillance is always exploited, even in the most democratic societies. »Targets include political opponents, student leaders and human rights workers« (Banisar et al. 1999). According to the report on human rights violations, more than 90 countries unlawfully intercept communications of political opponents, human rights workers, journalists and trade unionists. Particularly disconcerting is the increasing number of invasions of privacy on the part of private companies where, according to the 1999 Privacy & Human Rights Report, US companies head the list.

Mass data surveillance is performed routinely and its objective is to identify the segment of the population which could be of some advantage to a company, or in other words, those persons that a company considers worthy of special attention. In this case an individual is placed in a specific category and is designated as suspicious or worthy of attention on the basis of his/her characteristics rather than his/her acts. This method is called profiling and has been in extensive use in the US since September 11, 2001. It chal-

lenges many principles, for example, the principle of »presumed innocence«, because in this case a person is presumed guilty until proven innocent rather than the other way around.

Since the scope of surveillance expands and since it is imperceptible, instrumental, unselective and preventive, it may undermine human rights and freedoms. Charles D. Raab argues that the absence of control (exerted by the ruling power over individuals) and protection of privacy are prerequisites for liberal and participative democracy (Raab 1997, 161). At any rate, surveillance is a typical example of the clash between freedom and restriction of freedom. A certain degree of freedom restriction is necessary in community life, but control over individuals is also closely connected with power. In democratic societies this power must be subject to democratic supervision in order to prevent abuse.

Surveillance and privacy

Technological development has made possible massive and cheaper data and information gathering which, in turn, have enabled surveillance on a large scale. At the same time, consumer surveillance has endowed formerly trivial and uninteresting data with great market value.

In addition, control has been globalized. Recently, it has been possible to observe the globalization of security and administrative systems as well as commercial surveillance. It would be wrong to think that modern technologies are limited to economically developed countries (the majority of which uphold high democratic and legal standards). The Privacy & Human Rights Report includes a disturbing observation that the export of surveillance technologies to third world countries has been increasing (Banisar et al. 1999).

Modern society undoubtedly displays strong tendencies towards the highest possible, if not total, control. Yet it also highly respects individuality. The crucial principles of democratic societies are human rights and basic freedoms. The recognition that fundamental rights are universal and that they spell out *the limits* of state power, gained ground during the Enlightenment and bourgeois revolutions, particularly the French Revolution. In contrast to this principle observed by democratic states, a totalitarian state takes as a starting point the community, to which it accords a higher value

than to the individual. For a totalitarian state, important concepts are »the interests of the community, propaganda elaborated in detail, close control (over everybody and everything) and last but not least, the means of suppression« (Kušej, Pavčnik, Perenič 1992, 53).

Even though many authors relate the level of control over citizens to the level of democracy in a specific society (this relation is inversely proportional), panopticism of the 19th and 20th centuries has, paradoxically, increased along with growing commitments to social rights (Lyon 1994, 76). Historical experience shows that greater control went hand in hand with totalitarianism (e.g. the Nazi, Fascist and Stalinist states), while liberal democratic states respected – at least declaratively – the rights of individuals and restricted control over individuals (Raab 1997, 161). This is one of the reasons why civil society and political activists link control (exerted by the state) to totalitarianism, and protection of privacy to the level of democracy in a country. According to Foucault, panopticism is a political technology that operates through subtle coercion and internalization of the ruling power and thus sustains that power. For Foucault, modern ruling power is disciplinary power whose objective is the creation of docile bodies, while control is aimed at the disciplining and subjection of individuals. One can justifiably conclude that the panoptic effects of modern disciplinary ruling powers are similar to those of open totalitarianism, except that panopticism is more subtle, hence hypocritical.

In contrast to control seen as a political technology used to discipline individuals, administrative and consumer surveillance are apparently more friendly towards the individual. The objective of administrative surveillance is the regulation of individuals' activities and their lives. A typical example would be the use of surveillance to determine the scope of social rights or to set priorities in satisfying the needs of citizens. Consumer surveillance is ostensibly even more beneficial for citizens, because it presupposes the freedom of consumers and underlines their wishes. Consumer surveillance often includes the shaping of »consumer communities« by means of various loyalty cards and loyalty clubs. The document *Privacy on the Internet – An Integrated Approach to On-Line Data Protection* states that web sites often make use of loyalty programs, e.g. games, questionnaires, and net newsletters to obtain data about their visitors (Data Protection Working Party 2000, 18). The technique of profiling

is ostensibly consumer friendly because it guides the consumer in the direction he/she prefers, or in other words, it provides goods and content that are adapted to his/her individual tastes and estimated needs.

But, like any other type of surveillance, consumer surveillance too can have negative consequences, particularly in combination with data analysis and profiling. One is discrimination against certain consumers, for example, when issuing credit cards or granting benefits, especially in connection with dynamic pricing concept. A dynamic pricing model is defined as the »buying and selling of goods and services in free markets where the prices fluctuate in response to supply and demand and changing customer preferences« (Srivastava 2001, 1–2). This model is held to be particularly suitable in connected economy and on big, fragmented and volatile markets (Srivastava 2001, 3) which use information technologies for the gathering and analysis of consumer data.

One instructive example of the consequences produced by such a model occurred towards the end of 2000. Certain customers at Amazon on-line shop realized that they paid more than others for the same products, so they began to suspect that the price was dependent on their consumer preferences (loyal consumers were paying higher prices). Amazon admitted that they were testing the impact of prices on consumer buying habits, but they maintained that the experiment was limited and consumers selected randomly rather than on the basis of their consumer preferences (Bicknell 2000). Dynamic pricing is nothing unusual in the physical world, so a forecast by a Forrester Research's analyst, that »personalized pricing will be part of the natural evolution of the Web« (Bicknell 2000) should not surprise us. No doubt that, in order to ensure the maximum possible efficiency, this approach will be based on consumer data analysis.

Another problem related to consumer surveillance and administrative control is the fact that individuals themselves often do not want to opt out of such a system because of apparent benefits or discounts, while in certain cases opting out is subject to payment. But in the majority of cases opting out is not possible, because companies tie the use of their services to surveillance, meaning that those who want to safeguard their privacy cannot establish a relation with or

use the services of that company. The world of contemporary consumers and citizens is one in which it is necessary to surrender part of one's privacy for the sake of greater functionality and in order to be able to cope with the complexities of modern life.

Protection of privacy

Privacy is the foundation of human dignity and of other values such as freedom of association and freedom of speech. Certain authors even argue that all human rights are, in a way, different aspects of the right to privacy. The right to privacy is a basic human right, but not an absolute right. According to the Privacy & Human Rights Report, it has become one of the most important issues in modern society.

»Privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs« (Banisar et al. 1999). However, privacy is not a one-dimensional concept. Different authors identify different dimensions of privacy. Čebulj lists three elements of privacy: privacy of space (the possibility of being alone), privacy of personality (freedom of thought, determination, and expression), and information privacy (the possibility of keeping data and information about oneself to oneself because one does not want others to be acquainted with them) (Čebulj 1992, 7). The Privacy and Human Rights Report distinguishes between the following facets of privacy: *information privacy, bodily privacy, privacy of communications, and territorial privacy*. In an information society, the most endangered categories are information privacy and privacy of communications.

The same report further lists three important trends that threaten privacy: globalisation (which has been removing geographical limitations on the flow of data), convergence of technologies (increased interoperability and technology linking options), and multi-media (easy conversion between various formats). All of these processes created the need for efficient legal protection of privacy. The constitutions of almost all countries recognize the right to privacy,[11] but its scope varies from one country to another. The legally recognized

[11] Articles 35 to 38 of the Slovene Constitution define the protection of privacy rights and individual rights, the inviolability of dwellings, the protection of the secrecy of correspondence and other means of communication, and protection of personal data.

minimum is the inviolability of dwellings and the privacy of communications, but this right is increasingly extended to encompass access to and handling of personal data.

The origins of these legal provisions can be traced back to the *Justices of The Peace Act* of 1361, which included penalties for peeping toms and eavesdroppers. In 1765 Lord Camden protested when investigators attempted to enter his house and confiscate certain documents. Parliamentarian William Pitt then wrote: »The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement« (Banisar et al. 1999).

In 1776 the Swedish Parliament adopted a law on access to public records which specified that all data collected by the state must be used for lawful purposes. In 1890 the American lawyers Samuel Warren and Louis Brandeis defined privacy as the right of the individual to be left alone (Warren and Brandeis 1890).

The foundations of the protection of privacy in modern times were laid down by the *Universal Declaration on Human Rights* adopted by the General Assembly of the United Nations in 1948.[12] The need for an efficient protection of privacy was primarily prompted by the advent of information and communication technologies, so the interest in the protection of privacy increased in the 1960s and 1970s. Čebulj holds that the individual's privacy was jeopardized even before that and that these technologies only created new threats to privacy and led to an increased awareness of those threats, compared to the level of awareness during the era of manual handling of records (Čebulj 1992, 16). These technologies accelerated data collection and processing and gave rise to the special rules that govern the handling of personal data. The first country to adopt a law about the protection of personal data was Germany (1970), followed by Sweden (1973), the US (1977), and France (1978). Today EU directives place strong pressure on other countries to adopt adequate legislation.

[12] »No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.« *Universal Declaration on Human Rights*, Article 12.

According to the Privacy & Human Rights Report, several reasons led to these comprehensive privacy and data protection laws: the wish to remedy past injustices (and prevent re-emergence of totalitarian regimes), promotion of electronic commerce, and pan-European alignment of legislation. The EU favors comprehensive laws over the sectoral laws and self-regulation (codes of practices) that are preferred by the US, Japan and Singapore among others.

From the legal point of view, the biggest dangers arising from data collection are inaccuracy, mistakes, incompleteness and obsolete information (Čebulj 1997, 8). In addition, data can be collected for preventive purposes, »just in case«, which can prejudice a legal procedure (e.g. police or security agencies' databases). Another problematic issue concerns secret databases, of whose existence individuals are not even aware, or to which they do not have access.

As a result, the 1974 report by the Secretary General of the UN[13] recommends three principles that should be included in legislation regulating the area of information privacy: the principle of relevance, which requires that only those personal data that are necessary to attain a specific purpose are collected; the principle of notification, meaning that the individual should be notified in advance about which personal data are collected, stored and processed; and the principle of consent prescribing that only those data for which the consent has been obtained from the individual may be collected.

The formulation of a legal framework for the protection of privacy inevitably brings up the issue of the clash between freedom and restriction of freedom mentioned earlier. There is no doubt that broad restrictions on the invasions of privacy are unworkable for various reasons, and possibly even meaningless. Mellors thus concludes that »the best safeguard is not that they know less about us, but that we know more about them; and that we are aware of what they know about us and how they use such information« (quoted in Raab 1997, 158). The essential element of the protection of information privacy is the control of the flow and forwarding of data about an individual. Accordingly, contemporary laws on the protection of privacy are primarily concerned with the transparent *use* of per-

[13] This report was prepared for the Economic and Social Council by the UN Secretary General in 1974.

sonal data. To put it differently, data gathering is not subject to restrictions, but it must be grounded in legislation, while its purpose must be known in advance and must be transparent.

This is the reason why the right to privacy of information is today defined as »the right of the individual to demand that data and information about personal relations are not communicated to whomever.« (Čebulj 1992, 7). »Whomever« here means those who are not authorized to use certain data and information. The principle of the transparency of personal data usage is increasingly applied to the Internet, primarily in the form of the privacy policy statement in which the owner of a web page states which personal data are being collected, for what purpose and in which way they will be used.[14]

[14] Of course, the statement of privacy policy in itself does not guarantee that the privacy of a web visitor is really protected. The formulation of some of these statements is intentionally dubious, while others simply declare that the data gathered will be used for any relevant needs and purposes.

PRIVACY IN CYBERSPACE

While it is true that computers have introduced a qualitative change in the nature of surveillance, this assertion is even more pertinent to computer networks, and above all, the Internet.

At the beginning of the 1990s certain sociologists, and Internet users in particular, were convinced that the Internet, owing to its three characteristics,[15] was resistant to state control and surveillance. They maintained that the Internet would evolve towards greater freedom and independence from state control (Boyle 1997). Of course, this was true only during the early stages of the Internet while users were still few and the medium was new and beyond the control of the state and capitalist corporations. As Boyle concludes, the »'technologies of freedom' actually require an intensification of the mechanisms of surveillance« (Boyle 1997). Recently, the Internet has become a subject of increased regulation, while state agencies and commercial companies have been rediscovering the attractions of surveillance on the Internet. While early legal interventions in the area of the Internet were understood as restrictions of freedom, today it is realistic to expect that the users themselves will increasingly demand legal regulation of the Internet in order to be able to protect their rights. The absence of state-imposed rules during the early stages of the Internet could have been a chance for freedom. However, in present circumstances the absence of regulations, and particularly the use of surveillance systems, enables various types of abuse, which amounts to the restriction of freedom of the individual. Factors contributing to this danger are increasing cybercrime and the threat of the privatization of surveillance systems by Internet access providers, and particularly Internet service and content providers.

[15] These characteristics are: the technology of the medium, the geographical distribution of its users and the nature of its content. Boyle named this the Internet Holy Trinity (Boyle 1997).

The panoptic power of the Internet arises primarily from two important features that deserve to be stressed here. Firstly, computer technology enables decentralized control by linking formally separate surveillance systems via telecommunications devices. Secondly, its data storage and archiving facilities enable the creation of dossiers. As a result, while a few years ago the Internet could have appeared as a technology of freedom, today it looks as if the panoptic dimension has been built in from the start.

Surveillance on the Internet is exploited by various subjects, in a manner similar to that used in the physical world. Governments and their agencies have been increasingly using this form of control, particularly since the September 11th attacks, but commercial companies are also keenly aware of the allurement of consumer surveillance, i.e. the on-line gathering of consumer data. Furthermore, companies have a strong interest in controlling the on-line activities of their employees. Among other potential invaders of privacy, we should mention hackers[16], who are not only motivated by financial or similar reasons, but seek entertainment, self-confirmation or simply want to cause harm.

The Privacy Rights Clearinghouse organization warns that »there are virtually no online activities or services that guarantee absolute privacy« (Privacy in Cyberspace 1998). There are several methods of privacy invasion on the Internet. We shall take a closer look at them later in the text.

The problem posed by computer technology and the Internet arises from the fact that the technology itself enables certain kinds of privacy abuse. This is not to say that surveillance is embedded in the concept of this technology, but some of its properties can be utilized for surveillance purposes. These »side effects« of the technology of

[16] In its popular usage, the term "hacker" denotes a skilled computer user who invades a computer system. However, a hacker is a person with good computer knowledge who does not use this knowledge for malicious purposes. Those individuals who have good knowledge about computers and use it with malicious aims in mind are properly called *crackers*. Another term used in connection with this is *script kiddie*. It denotes individuals having moderate knowledge about computers who exploit well known security holes to invade computer systems or use publicly accessible invader tools. Usually, their attacks are not aimed at specific targets but they randomly invade insufficiently protected servers. A system can also be invaded for criminal or terrorist purposes, or the invasion may be related to industrial espionage, but the majority of computer attackers seek self-confirmation, or engage in such activities out of fun, or are simply vandals.

the Internet have led to the present situation in which a multitude of personal data is gathered via the Internet without seeking consent from users or even without users being aware of it (Data Protection Working Party 2000, 19). Another related concern is that the data gathered are used for purposes other than those originally intended. For example, a bankrupt company can decide to sell the data so collected to pay off debts, despite initial assurances that collected data would not be transferred to a third party without the user's consent. One company that exploited this possibility was Toysmart.com (Morehead 2000).

There are many possible methods of data collection and surveillance, or privacy invasion, in cyberspace. People leave behind electronic traces whenever they use a computer or telecommunications network. This can be an intentional act (e.g. a record posted on one's homepage or a message to an on-line forum), or the user may be unaware of it (e.g. a visit to a web page, the use of a web service and the like). Furthermore, information can be intercepted while being transmitted via telecommunications networks, or the computer system can be invaded. Various techniques for intercepting information in the immediate environment of the computer or telecommunications system are also in use. All of these surveillance technologies will be examined in greater detail later in the text. At this point, let us stress that invasion of privacy is not necessarily tied to any special technology. Intruders sometimes resort to fraud, for example, by persuading victims to allow them access to the system or to supply specific data or information, or by deceiving a victim into such an act. Another method of getting hold of desired data is social engineering. In such cases the attackers usually give a false identity or win a victim's trust and then abuse it. There have been cases in which attackers falsely identified themselves as technical support staff in order to get hold of users' passwords. In other cases, false web pages were used[17]. The majority of users do not know that the location of a web page may include the user name and password in the form

[17] One such page was ebayupdates.com that appeared in December 2002. The users of eBay on line-shop were requested by way of an e-mail to enter the credit card number and password on this web page. But ebayupdate.com was a false web page in no way connected with eBay. It was set up with the intention of stealing credit card numbers (Internet 2002).

http://username:password@www.someserver.com. Of course, most web sites do not require this because access is free for all (you can browse such a web page using any login name or password). But precisely because of this there is a danger that the user will confuse a user name for a web address. In addition, a web page may be accessed by entering the IP address of the server, which can present additional confusion.[18]

Collecting information about computers in a network

The computer in the network is identified by its IP number or IP address,[19] which is the virtual address of that computer. The IP address determines the location of the computer in the network, revealing also how to access that computer. A computer can access the Internet directly, via its IP address, or can be hidden behind a special interface called *Network Address Translation* or NAT, which attaches a group of computers to the Internet through one IP address. The IP address of a computer may be fixed, meaning that every time the Internet is accessed from that computer the same IP address is used, or dynamic, meaning that every time the computer is connected to the Internet it is allocated a different IP address taken from the set of available ones. The dynamic IP address is mainly used for dial-up access, while fixed IP numbers are predominantly restricted to servers and other computers that are permanently on-line by way of a local network, a leased line, an ADSL connection or a similar permanent connection. Obviously, it is easier to identify a user with a fixed IP address, since in the case of a dynam-

[18] For example, instead of entering http://www.arnes.si, it is possible to enter http://193.2.1.66/ or even http://www.somestore.com@193.2.1.66/. In all of these cases, the user accesses Arnes home page. But, unlike in the first two examples, where it is obvious which page is being accessed, the third entry is different even at first glance, since the string »www.somestore.com« is a user name and not the address of the web page. Some older versions of web browsers caused additional confusion by enabling the entry of the so called 'dword' format or the hexadecimal equivalent of @ sign (the hexadecimal code for @ is %40). Using this simple trick anyone can set up a copy of any well-known on-line shop and collect users' data. For more on this see *How to Obscure Any URL*, http://www.pc-help.org/obscure.htm.

[19] The IP numbers are 32-bit numbers, mainly represented in *dotted decimal notation* (in the form xxx.xxx.xxx.xxx). Each decimal number consists of 8 bits of binary data so it can represent values from 0 to 255.

ic IP one first has to determine which user has been allocated that specific IP at a specific time. The identification of users connected via the NAT interface is not as simple, because in this case the IP address stands for an interface and not a specific computer.

Another component of the Internet infrastructure is Internet Control Message Protocol or ICMP, which is implemented in the *ping* command used to check the functioning of the connection between two Internet locations. A user may execute this command to check whether the connection with the remote computer in the network has been established. However, the *ping* command may also be used to check whether a specific computer is currently connected to the Internet, particularly if that computer uses a fixed IP address. It is not difficult to imagine how the *ping* command could be exploited by an employer to check when an employee has switched on/off the computer and, in turn, to determine the start/end of work. Moreover, the same command could be used by any party that has access to the Internet, say, a competitor. However, this method will not produce an accurate identification if a computer is used by several users or is hidden behind the NAT interface. This »deficiency« is eliminated by using interactive systems such as ICQ, Yahoo Messenger and the like, which provide even more detailed information on the status of the user (whether he is connected, whether he is currently using the computer and so on). But these are specialized programs that have to be downloaded by the user, so one should be aware of the options they involve.

Electronic traces left with Internet providers

By moving around in cyberspace, users leave behind many electronic traces, with the majority of these being recorded by Internet access providers. These can log all activities of the individual user (which Internet service has been accessed and when), user name (it can be linked to the physical identity of the user), IP number allocated to that user and the telephone number or other entry point used to log on. These data are collected in log files, and their importance has long been recognized by state administrations. For example, the system called *Carnivore* (its official name is DCS1000)

has been in use in the US since June 2000. This is a special program that is installed at the Internet provider. It can intercept all electronic messages and record all user activities (StopCarnivore 2000). Although the introduction of this system sparked vehement protests by both Internet users and Internet providers, the Privacy International organization estimated that the system would nevertheless be installed with all Internet providers in the US within one to two years (Privacy International 2000). Indeed, the task was completed even sooner – it was accelerated by the September 11th attacks, which were used as a justification by US government agencies to intensify control on the Internet (McCullagh 2001a, Analysis 2001). The web magazine Wired News reported on September 12th 2001 that only a few hours after the terrorist attacks, FBI agents began to visit Internet service and access providers requesting the installation of Carnivore, and did not meet with any significant opposition (McCullagh 2001a).

Usually, Internet service providers also have a *DNS server* (short for Domain Name System, a facility that converts a domain name into an IP address). This means that the provider can trace down the pages accessed by the user and build user profiles. Another method of collecting data about users' tastes is through portals[20]. The 2000 report by the Dutch Data Protection Authority states that a provider running a portal can determine how many advertisements were viewed by the user, how many times the user visited an on-line shop, which products he/she bought and even how much he/she paid for these (Data Protection Working Party 2000, 43).

Electronic traces at content providers

In addition to Internet access providers, Internet service providers (particularly web page providers) also maintain activity log files. The minimum items of information stored in these databases are the user's IP address and information about visits to particular web sites (or pages at a specific address), but certain local environment variables can be included as well. The on-line service provider can thus

[20] Portals or extended entry points are web pages with a number of links and useful information (e.g. weather forecasts, agency news and the like). For a user they represent a starting point for web surfing.

trace the type of the web browser, the operating system running on the user's computer, the type of language support activated, the web page from which that particular service has been accessed and the like. It is true that some of these traces can be deleted or obscured, but most users are not familiar with these procedures. In addition, web browsers exchange information with web pages, a feature known as browser chattering. But some web browsers such as Microsoft Internet Explorer send to a web page more details than others do about the user's environment. The *Privacy on the Internet – An Integrated Approach to On-line Data Protection* includes a comparison of several web browsers, showing that Internet Explorer even supplies information on the presence of Word, Excel and Power Point applications on the user's computer (Data Protection Working Party 2000, 14–15).

Further possibilities opened up with the use of JavaScript.[21] If the user has not disabled the JavaScript option in his/her web browser, the web page may obtain even more items of information about the user's environment, for example, screen resolution, the time zone, Java support[22], connected plug-in modules, estimation of the speed of Internet access and so on.

This information is mainly used to monitor visits to a web page or other providers, but also for other reasons. For example, the web server can use this information to assess the multimedia capacity of the user's environment and adapt the format of content sent to a user (e.g. a flash animation or a video clip in AVI format). On-line search engines use this information in combination with search keywords to build user profiles (Data Protection Working Party 2000, 44). On the other hand, in case of abuse, the web page administrator or the owner of the invaded system can, in cooperation with the Internet access provider, determine the physical identity of the malevolent user on the basis of the IP address and time of access.

The information about the number of web page visitors is interesting primarily for advertisers. However, in the past it used to be impossible to determine the number of different visitors, not to speak of their identity, if users accessed the Internet through a dial-

[21] JavaScript is a script language developed by Netscape for use on web pages.

[22] Java is an object-oriented programming language developed by Sun Microsystems; it is widespread and therefore suitable for the running of web applications.

up connection, a gateway or an anonymous proxy. So, in 1994 Lou Montulli was commissioned by Netscape to develop a solution that became known as “cookies”.

Cookies are small information packets sent by a web server to a web browser which then deposits this information on the user’s computer and transmits it to the server on request. The server may set the expiration date for a cookie and determine which part of the web server has access to it. With regard to the expiration date, we distinguish between session cookies and persistent cookies. The former expire with the conclusion of the browsing session, that is to say, when the user closes the web browser, while the latter last longer, even for years. A cookie is available to the server throughout its period of duration (if not deleted by the user, of course). In addition, we distinguish between first-party and third-party cookies. The importance of this distinction has only recently been recognized. As a matter of fact, third-party cookies are mainly used by web advertising agencies for surveillance purposes (Data Protection Working Party 2000, 52).

A cookie usually contains the identification number of the user which is remembered while he/she browses the pages of a specific web site. Of course, this number can be linked to other data as well, and the next time the user returns to the same web page the server can establish that the user has already been there and retrieve his/her actions. Originally, cookies were developed to handle on-line shopping carts, but today they are used with all kinds of web pages.

Cookies are therefore considered to be distributed databases, since users’ data are distributed among a number of local computers. However, as we have already pointed out, some providers use cookies to trace users from one server to the next, and even to identify them. One of the most imaginative examples of the use of cookies has been furnished by a net company called DoubleClick.

With direct marketing of advertising space on the Internet being impractical, various companies, among them DoubleClick, began to specialize in buying advertising space from a multitude of smaller web owners and selling this space to advertisers. DoubleClick soon realized that they could determine on which web page a specific advertisement was displayed and link this information to the identification numbers contained in the cookies that are sent across the

advertising network by their server.[23] This procedure enables DoubleClick to establish which web pages inside the advertisement network were visited by a user. An advertisement can be substituted with a small graphic, 1 by 1 pixel in size, meaning that it is practically invisible. This method is also referred to as »tracing using pixel technology« and the graphic is dubbed a *web bug*. If the advertising network is sufficiently large, the collected data can be used as a basis for identifying the browsing habits of individual users.

However, this is not all there is to cookies. Cookie information can be associated with the e-mail address which the user types in on a web page, and even with the user's off-line identity, if the user enters other personal data.

Browsing habits can also be established by sending group e-mails with personalized hyperlinks and inviting the recipients to click on them. Since each recipient receives a different hyperlink, preferably one that contains a unique identification code, and since the sender of the message knows to which addresses the message has been sent and which hyperlink it contained, a click on such a hyperlink will enable the originator of the message to link a specific e-mail address with the cookie value and through it build the user's browsing profile. Other types of e-mail messages do not even require a click on the hyperlink but mere reading of the message will do the job. These messages contain an invisible web bug which deposits a cookie on the local computer as soon as the message is read. Of course, this method only works under certain conditions (the user must be connected to the Internet when reading the message, the messaging software must support the HTML format, the »cookies« option must be enabled and so on). Despite this, if used in combination with other techniques, the method is very efficient. At the beginning of 2000, *USA Today* carried an article revealing that DoubleClick collected user names and made an attempt to link cookies to the users' off-line identities[24], and so furnished proof that this type of surveillance is not merely a theoretical option (Schneier 2000).

[23] On October 25th, 2002, DoubleClick published on its web page (http://www.doubleclick.com) a public notice DOUBLECLICK AD SERVING DATA SHOWS RICH MEDIA CLICK-THROUGH RATES TO BE SIX TIMES HIGHER THAN STANDARD ADS, which included information that 55 billion advertisements were displayed in May 2001.

[24] DoubleClick entered into association with Abacus Alliance, the leading consumer data gathering company in the US. In November 1999 the companies began to merge data on consumers (Data Protection Working Party 2000, 45).

This is the main reason why some Internet users disable the cookie and JavaScript options despite the fact that this reduces the functionality of the Internet.[25] But even acquiescing to lower functionality will not guarantee you privacy. At a conference about computer and communications security organized by the Association for Computing Machinery in November 2000 in Athens, Felten and Schneider of Princeton University described the technique dubbed a »timing attack«. This technique is used to determine browsing habits by exploiting the web caching facility (browser's cache) even with the cookies, Java and JavaScript options disabled and anonymizers in place (Felten and Schneider 2000, Standard Feature 2000).

Since this type of information is commercially highly interesting for web page owners, it is very likely to be supplied to third parties such as market research departments or companies specializing in the analysis of web statistics (Data Protection Working Party 2000, 43). In the opinion of Privacy Rights Clearinghouse, the collection of this type of data, particularly information on the number of web page visits, is on the rise (Privacy in Cyberspace 1998). Therefore, one should not be surprised to hear that many on-line search engines are funded by marketing organizations, as claimed by the authors of the report *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* (Data Protection Working Party 2000, 18), or that the providers of free-of-charge e-mail services, who are also massively sponsored, may pass electronic addresses to marketing organizations (Data Protection Working Party 2000, 36).

Many find the gathering of personal data problematic, even if it is done by independent researchers or academic institutions who are obliged to make collected data anonymous before they are published and who, in principle, do not sell these databases. But data gathering and use for marketing purposes are not necessarily harmful. For example, advertising revenues enable certain page owners to offer their web content free of charge. In addition, these technologies enable the personalization of web pages, which is a fea-

[25] Selective disabling of cookies offers more possibilities. For example, Bugnosis is a program designed to detect web bugs that send cookies. Certain web browsers such as Mozilla enable selective blocking and deletion of cookies.

ture that can be useful for a web visitor.[26] A ban on the gathering of such data would by no means dramatically reduce the functionality of the web, and would very likely hamper the development of the Internet economy. Therefore, EU Directive 2002/58 allows such a collection of data but under the condition that the user is notified in a proper manner about the collection and use of data, and that he/she is given an opportunity to decline such data processing (Možina 2002, 3). Indeed the only sensible protection against invasions of privacy seems to be strict supervision of the collection and usage of electronic traces. Unfortunately, as Allard and Cass conclude, databases containing personal data and on-line activities are increasingly publicly accessible (Allard and Kass 1997, 572).

Linking and gathering of distributed data

The Internet stores a huge mass of data and information. The major part of it is unrelated, but this does not mean that interlinking is impossible. Among the available techniques are computer matching and record linkage, but databases can also be conceptualized as relational databases. Computer matching was first used by US government agencies in the late 1970s and became widespread in the 1990s (Lyon 1994, 9).

Today, databases are one of the main tools of mass surveillance. One reason is that they can be exceptionally compact and, following the initial investment, also cheap to maintain. Clarke therefore speaks about dataveillance, which is essentially cheaper and more effective than centralized supervision (Clarke 1988). While it is true that networking and data distribution are much more economical, a prerequisite for successful dataveillance is the linking of various systems by means of a universal identification scheme, preferably via telecommunications networks. The Internet is downright ideal for this kind of surveillance, and the linkage of electronic traces is a typical example of dataveillance.

[26] Despite everything it seems that certain standards for privacy protection have began to take shape. At the end of August 2002, DoubleClick announced that it will enable users to view certain data collected through the use of cookies. Using this cookie viewer, users would be able to see into which category they had been placed. (Glasner 2002).

One particularly attractive possibility is the gathering of publicly accessible personal data voluntarily supplied by the user. The gathering and classification of on-line data has long since ceased to be technically problematic, and on top of that, it is extremely effective and cheap. The technology for gathering data published on web pages is public, but automatic classification and recognition of significant data is somewhat more demanding. The programs designed for data gathering – they are called spiders, worms, (ro)bots, or harvesters – are mainly intended for the collection of e-mail addresses. These programs search web pages, web forums, news groups and mailing list archives. Web page administrators who want to prevent such data gathering can specify which area of the web page should not be accessed by robots,[27] but robots do not necessarily observe these rules.[28] As a result, many tricks are used to confuse robots so that they are no longer able to recognize specific information as being an e-mail address.[29]

In Slovenia the *Directory of Electronic Addresses* was published on October 6th, 1997 (http://afna.telekom.si). It was followed by an e-mail directory compiled by the Najdi.si search engine (http://www.najdi.si). Modern web search engines as Najdi.si include artificial intelligence features that are capable of recognizing, to a certain extent, the language of the text, and can extract or record certain data, for example, a published e-mail message, a telephone number or a graphic.

Of course, there are other methods of data gathering that are even more efficient. Many web services or web pages require from the user the entry of specific personal data in exchange for certain services, for example, information provision, a benefit, or simply access to the web page. Tricks involving various awards are also widespread. Web page owners who collect data on-line often do not state clearly for what purposes the data will be used, or the data collected

[27] This is called a *robot exclusion protocol*; it creates a list of web pages from which robots are banned stored in the robots.txt file on the web server.

[28] A robot behaves like an ordinary web browser and it can be identified by the value of the environment variables which include the signature of a web browser (USER_AGENT). However, technically, a robot can pretend to be an ordinary web browser.

[29] One tool used for this purpose is a script for the random generation of non-existent e-mail addresses. The logic behind those is to furnish false data and thus render such a database useless.

are used for purposes different from those officially stated. Furthermore, an e-mail address can be obtained when the user registers a free copy of a software program (Data Protection Working Party 2000, 32), or by exploiting viruses, a subject which will be examined more thoroughly later in the text.

On December 15th 1997 the American Federal Trade Commission published the results of a research study titled *Kids Privacy Surf Day,* in which the 126 servers most popular with children were analyzed. The results showed that approximately 86% of all servers included in this study collected personal data (names, addresses, telephone numbers, e-mail addresses), with less than 30% of those displaying a privacy policy statement, that is to say, a statement about the purpose of such information gathering. Another alarming fact was that less than 4% of these servers required parental authorization of data. To sum up, the study showed that kids' privacy on the Internet was poorly protected and that many more measures would be needed to achieve good protection (Kids Surf Day 1998).

Intercepting data in a network

Network interception of information is analogous to telephone wiretapping. One method of intercepting information is »packet sniffing« (the term originates from the fact that data on the Internet are exchanged in the form of packets).[30] This technique is usually difficult to identify because intrusion is passive rather than active (the attacker only monitors the traffic). It is often used by hackers to intercept and steal passwords (password sniffing).

The introduction of wireless LAN networks (mainly using 802.11b protocol) opened still new channels for abuse. This includes the stealing of Internet access (unauthorized access to the Internet or stealing of passwords), interception of network traffic, and attacks on networks or specific computers in a wireless network (Wireless

[30] So called *promisc sniffing* used to be very popular with Ethernet networks using hub technology, since initially each computer located in a specific segment of an Ethernet network using hub could control traffic on all other computers in the same network segment. If one of the computers has been set to »promisc mode«, it was able to listen to the traffic on all other computers in the same network segment. However, this technique is not imperceptible. Today, data interception is effected mainly by monitoring the router traffic or wires transmitting signals.

2002). Researchers from Berkley who managed to break in real time the Wired Equivalent Privacy (WEP) coding algorithm used in wireless networks[31] have established that this security protocol was so poorly conceptualized that it made possible an imperceptible falsification of packets transmitted over wireless networks (Sandberg 2001). Since the user or intruder can be up to 120 meters away from the base station (or several kilometers if a directional antenna is in use) and is not physically connected to the network as is the user of an ordinary network, it is very difficult, if not impossible, to locate such an intruder. As a result, the responsibility for potential criminal offense can fall on the wireless network owner. This danger is even greater if access to the wireless network is not protected by a password.[32] The hacker community has already devised a special system of symbols to denote the physical points from which access to wireless networks is possible. This practice is called *warchalking* because the hackers use chalk to mark public places to indicate the presence of a wireless networking node and the method of connection (Loney 2002). The English term denoting such network access point is *hotspot*.

Intercepting electronic messages

The evidence so far clearly indicates that electronic messages are much easier to intercept or to search for keywords than are ordi-

[31] WEP is an encryption and authentication system. At the moment, two types of WEP are in use, a 64-bit and 128-bit WEP. In reality, these are 40-bit and 104-bit algorithms since the remaining 24 bits are used for system generated data (initialization vector) enabling the synchronization of data packets. In 2001, several researchers demonstrated that it was possible to break the 128-bit algorithm in several hours at minimal costs (under $100). (Stubblefield et al. 2001). Yet WEP deficiencies do not arise from RC4 algorithm (also used in SSL) but from the poor conception of the whole security system. Another serious deficiency of this system arises from the fact that all users share the same access key (Schneier 2001b). Some of these deficiencies are expected to be eliminated by new 802.11i protocol. Computer experts recommend the use of *IP security protocol* and *Virtual Private Networking* in wireless networks.

[32] Access to wireless networks can be protected by controlling serial numbers of network interfaces (MAC or *Media Access Control address*). The network administrator allows access to a wireless network only to the users with specific MAC addresses (different for each network card). But MAC addresses can be counterfeited. Moreover, certain types of wireless network cards support user-definable MAC address. It should also be stressed that this type of fraud is not easy to identify.

nary mail or telephone communications. One reason is that electronic messages are ordinarily transmitted over the Internet as plain text rather than encrypted text. In addition, electronic mail is, in principle, accessible on the mail and relay servers (relay servers are intermediate points in a network that forward mail from one Internet server to the next) until forwarded to the recipient, although the principle of secrecy of correspondence is observed in the majority of countries. As regards the transmission of electronic messages, a message should be deleted from a relay server as soon as it has been forwarded (Data Protection Working Party 2000, 33). The same rule applies to the mail server, unless the recipient chooses to leave a copy of the message on the server. It is also important to make a distinction between traffic data, which are necessary for the transmission of messages and calculation of costs, personal data, and message content. The e-mail server automatically stores certain technical data, i.e. the size of the message, sender's and recipients' addresses, date and time of the message, and several other pieces of information pertaining to message transmission. However, special software and parameters enable the recording of many other data, for example, the number and size of attached files, a character set that has been used, the subject and content of the message and so on. The document *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* points out the danger of mail providers erroneously treating these data as traffic data which they think they can save (Data Protection Working Party 2000, 33). The paradox of electronic mail lies in the fact that it more closely resembles a postcard than a sealed envelope or private correspondence – as users or legislation tend to see it.

Other issues are also raised in connection with electronic mail (and other web services). Certain mail servers use special programs to scan electronic messages for viruses or to intercept *spam mail*. While it is undoubtedly true that messages containing viruses and spam mail should not be forwarded to third parties (Data Protection Working Party 2000, 34), the installation of these programs without the consent or even without the knowledge of the users raises interesting legal issues. While the scanning of messages for viruses is in

principle permitted (despite false alarms resulting in the interception of uninfected messages), the filtering (deletion) of spam mail on the basis of criteria not approved by the user is legally more controversial.

Another dilemma is whether all or only certain electronic mail is to be regarded as personal mail. The US *Electronic Communications Privacy Act* prohibits the reading of the content of electronic messages, albeit with some exemptions. For example, an employer is permitted to inspect the electronic mail of its employees – if they use the company's mailbox, of course (Privacy in Cyberspace 1998). Regulations in Slovenia are different. An employee in Slovenia must be acquainted with such a possibility and must give his/her consent. Similar questions pertaining to the restrictions on the privacy of electronic messages are occasionally raised in relation to free e-mail providers. But even with these legal loopholes, users have the opportunity to protect their mail by encrypting messages (this topic will be discussed in greater detail later in the text).

Intrusions into computer systems

In addition to the invasion of communications and information privacy in cyberspace, there are also abuses of territorial privacy.

Intrusion into a computer system is one of the most direct invasions of privacy. It may be a consequence of negligence in setting file permission parameters, or may result from the use of badly written programs (a typical example would be a web application that does not check the commands for work with databases), but usually it involves sophisticated methods of detecting vulnerable points and exploiting them. In the past, such an intrusion required a lot of computer knowledge, but even this has recently begun to change.

In 1995 Wietse Venema and Dan Farmer published on the Internet the freeware program called SATAN (*Security Administrator's Tool for Analyzing Networks)* which looks for security holes by way of the Internet or a local network (What SATAN is 2002). The program is intended for detection, not abuse, of security holes. The authors described it as a tool intended primarily for computer system administrators seeking to improve the security of their systems (Improving 2002). Three years later, in 1998, a group of hackers who call them-

selves The *Cult of the Dead Cow* group published on their page the *Back Orifice* Trojan horse,[33] a remote administration tool that allows control of Windows-based computers. *Back Orifice* is a program that opens a back door on the computer, enabling the attacker to take control of the computer from a remote location via the Internet, while remaining imperceptible to the user. The program is very simple to use and does not require any special computer skills; moreover, it is free of charge. The only problem is how to sneak this program on to the victim's computer. Another competitive program that appeared simultaneously was *NetBus*. Today, more and more tools for the control and invasion of computer systems are available on the Internet.[34]

Unlike these programs, which are used to invade a specific system, viruses spread with no definite target in mind. The term »computer virus« is loosely used to denote any type of program or program code that reproduces on its own and is designed to cause harm or to overtax a computer system. But viruses are not necessarily destructive. In May 2000 the former director of the CIA, R. James Woolsey, drew attention to a new kind of virus – the instructive virus (Poulsen 2000). This type of virus is designed to use the minimum possible system resources, and its task is to steal data (e.g. the list of e-mail addresses from the user's address book), make changes to the content of files and carry out electronic eavesdropping.

In December 2001 it came to light that one such program was used by the FBI. In 1999, while conducting an investigation into the case of Nicodemo S. Scarfo, allegedly a Mafia member, FBI agents realized that he used PGP encryption, which prevented them from reading the content of his files. On May 10th they secretly entered Scarfo's office in New Jersey and installed a keyboard-sniffing device on his

[33] A Trojan horse is a malevolent application which, unlike viruses, does not reproduce on its own, nor can it infect other files on the computer. Trojan horses usually »pretend« to be ordinary applications (hence their name) while their hidden functions usually serve to open »back doors« on the victim's computer, to steal passwords or cause some other kind of harm.

[34] It may be useful to draw attention to the fact that some of these programs have built in back doors that can be used by the authors of these programs to control the computer on which such a program is used as well as the computer of the victim. A measure of caution when using such a program is certainly recommended, but above all, we should point out that the use of such a program is unlawful.

computer which intercepted his password for content encryption (McCullagh 2000 and Schneier 2001a). It then came to light that the FBI developed a special tool named *Magic Lantern* for the interception of passwords. This is a Trojan horse application that utilizes security holes and deficiencies in a computer system and can even be remotely installed via the Internet or an e-mail. This discovery, together with the FBI's confirmation that such a tool existed, triggered a heated debate on whether companies selling anti-virus programs should modify their programs to suppress the alerts about Magic Lantern, should it be detected. Anti-virus producers decided not to go along with the FBI – one reason probably being public pressure – and to continue alerting users to all viruses detected regardless of their source (FBI 2002).

Other tools include spyware software with built-in secret surveillance tools. These applications are designed for the gathering of data (mainly data of some market value, for example, e-mail addresses or browsing habits) which are then sent to the originator's server. These programs are sometimes referred to as E.T. applications because they »call home« once they have collected the desired data (the term is based on a phrase from the movie *E.T.*).[35]

However, the surveillance mechanisms are embedded not only in applications offered by less prominent producers, but also in widespread applications. At the beginning of 1999, the FBI managed to trace down the author of the notorious Melissa virus within a surprisingly short time. Given that the virus was written using the script language that is part of the MS Office environment, the intriguing question was how the FBI managed to trace the author among the millions of MS Office users. It turned out that Microsoft had covertly integrated into Office 97 the Global Unique Identifier function (GUID), which inserts a unique identifier into each Office document. If the user's computer includes a network card, the serial number of that card becomes a part of GUID, making possible accurate identification of the computer from which the program originated (Lemos

[35] *RealPlayer* (Macavinta 1999) and *Windows Media Player* (Labriola 2002) are also believed to be spyware applications. RealNetworks and Microsoft collected information on users' video and musical preferences and there were even suspicions that this information was linked to electronic messages. Microsoft denied these allegations but it is clear that technical possibilities for such activities exists.

1999). The related issues that came into focus were whether this technology could be abused to achieve other objectives as well, for example, to trace political opponents (Joel 1999). The EU Directive 2002/58 also draws attention to the threat to privacy posed by spyware applications and hidden identifiers specifying that these should be used only for lawful purposes and users must be acquainted with them (Možina 2002, 3).

Computer systems have many security holes.[36] Even though these are mainly well documented and promptly amended, users do not keep pace with new service releases and many do not even know that these exist (indeed, pertinent information is sometimes difficult to find). Therefore, we can expect that the privacy invasion trend will continue to grow and that it will be exploited by hackers, private companies and government agencies.

Intercepting data and information in the immediate environment of the system

Although the technology for intercepting electromagnetic signals was first described as early as 1967 (Kuhn and Anderson 1998, 125), only few studies in this area have been published to date. As a result, this method of data interception, which exploits electromagnetic signals sent out by the computer equipment, remains one of the least known techniques of surveillance. The technique is called TEMPEST – *Transient Electromagnetic Pulse Emanation Surveillance Technology*. It was described by the Dutch scientist Wim van Eck in 1985 in an article titled »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?«. According to Van Eck, this kind of eavesdropping system could be constructed using relatively cheap and commercially available components, and would be capable of reconstructing TV screen content from a distance of several hundred meters, in some cases even more than 1 km (Van Eck 1985, 2–3), even with a wall or some other physical obstacle intervening between the screen and the eavesdropping device.

[36] Security holes in Windows are regularly treated by net newsletters such as Crypto-Gram (http://www.counterpane.com/crypto-gram.html) or Security Focus (http://www.securityfocus.com); extensive information is also available at *Microsoft's* web page (http://www.microsoft.com/technet/security/).

Kuhn and Anderson of the University of Cambridge also described other possible uses of TEMPEST. It enables, for example, the interception and identification of signals transmitted along cables (e.g. a keyboard cable, a telephone line, Ethernet network etc.). Coupled with Differential Power Analysis, a method described by Kocher, Jaffe and Jun of Cryptography Research, it can be used to extract certain secret information, for example, an encryption key or a PIN code (Kocher, Jaffe and Jun 1999). Similar threats are presented by the timing attack technique discovered by Paul Kocher. This technique relies on measuring the processing time of a device to crack the encryption key (Kocher 1996).

Kuhn and Anderson further explained how this technique could be used to circumvent smart card protection which sets a limit on the number of retries of a password or a PIN code entry. The majority of smart cards will lock up after entering a wrong password or a PIN code several times in succession. However, on the basis of electromagnetic emanation, an attacker can establish whether a PIN code entered is correct even before the card locks up, and reset the card if the password is incorrect. This would enable unlimited retries for password entry.

Another potential use of TEMPEST technology is for the detection of piracy within companies. A special virus could be produced for such purposes. It would exploit an increased activity of a hard disk or a screen saver to emit, at certain time intervals, a signal encoding license serial numbers along with a random number. By counting the number of signals received from the software with the same serial number, it would be possible to detect piracy without entering the premises of a specific company (Kuhn and Anderson 1998, 125–126, 136).

THE PROTECTION OF PRIVACY IN CYBERSPACE

When speaking about privacy protection on the Internet, we first have to distinguish between various actors that participate in the process of data and information exchange. These are telecommunications operators, Internet access providers, Internet service providers and users (Data protection Working Party 2000, 11–12). All of these actors can use their own instruments of control, which were described in the previous chapter. I will now proceed to describe potential methods of protection against certain surveillance techniques.

The laws that cover the area of privacy protection in the real world also apply to the virtual world. However, the fact that the Internet is not territorially delimited as is the real world can affect user's rights. This is particularly true in cases of abuse involving several countries with non-harmonized legislations. A user surfing the Internet in effect moves across various territorial jurisdictions and interacts with globally dispersed subjects. Data packets can travel across various countries on their way to the recipient, including those countries with a low level of legal protection. This even applies to the Internet traffic between participants who come from the same country, because data are transmitted along the least loaded route, and occasionally this route traverses several countries.

A certain number of users soon realized the importance of self-protection and the development of security culture. In addition to the reasons described above, another factor contributing to the awareness was the fact that, at the beginning of the 1990s, legislation regulating the Internet was only beginning to emerge. Yet, as the International Working Group on Data Protection and Telecommunications pointed out, self-protection alone cannot ensure privacy on the Internet, so a comprehensive legal framework is needed in order to ensure the efficient protection of privacy. The security and priva-

cy issues are not only technical, but also social issues. Computer users should be better acquainted with various forms of potential abuse, and more importantly, with the means of protection available on the market. But first of all, one should be aware that protection cannot be bought as a product or, to put it differently, it is not a matter of a one-time purchase but rather of a *process*. The culture of security should be developed and continually cultivated. In addition to specialized applications, most of which are cheap or even available on-line free of charge, prudent behavior can also be of great assistance.

Anonymization

Anonymity services offer one possible form of protection. Of course, full anonymity is impossible to achieve, except for special cases, because a computer user who wants to obtain access to the Internet must sign a contract with an Internet access provider, meaning that he/she cannot remain anonymous. Unfortunately, only unlawful actions provide complete anonymity. For example, one can access the Internet secretly through a wireless or a local network,[37] or give false details when signing a contract with an Internet access provider. But even in such extreme (and unlawful) cases, the Internet access provider can store data about the entrance point from which the user accessed the Internet (a telephone number), so to remain truly anonymous such an intruder would have to use a pre-paid mobile phone. Anonymization pertains, therefore, to the use of web services, rather than to anonymous access to the Internet.

There are several ways of remaining anonymous when accessing Internet services. One is the use of remailers to send electronic messages. These are mail servers that erase information about the origins of the message once it has been forwarded. The other is the use of a proxy server to browse the web. A proxy acts as a kind of intermediary between a local computer and the Internet. It sends requests for access to web pages on behalf of users and forwards web content to them. It also stores frequently requested data (e.g.

[37] Even in this case it is possible to record the serial number of the network interface or *Media Access Control address*, which could be used to reveal the identity of the user (see the description of *Microsofts'* GUID in the previous chapter).

images) into its cache memory and forwards these to local users on request, thus reducing Internet traffic. But proxies can also be used for other purposes. The proxy server identifies itself on the Internet with its own IP addresses, so the identity of the actual user remains undisclosed.[38] The type known as the anonymous proxy server neither stores nor forwards data about its users, ensuring anonymous web browsing. Roughly speaking, there are two kinds of anonymous proxies – standalone and web-based anonymous proxies. Of course, a user behind a proxy is anonymous only for the web server being visited, while the Internet access provider, or some interceptor, can nevertheless monitor the traffic on the user's computer. This can be avoided by encrypting the connection between the local computer and the anonymous proxy server, but even in this example it is possible to analyze the traffic, primarily to identify the anonymous proxy that was used and the quantity of data that was transmitted. Besides, a certain degree of caution when using anonymous proxies is in order, because not all are anonymous despite assurances to the contrary. In principle, the level of anonymity they offer suffices for, say, participation in an on-line forum (where anonymity is a matter of trust), but in the case of police investigation it could easily turn out that many allegedly anonymous proxies are not fully anonymous in reality.

In addition to this anonymization of the IP address, there are also programs that block the tracing of users through the use of cookies or web bugs described in the previous chapter. Another issue that should be considered is the disabling of the cookies option in the local web browser, especially third-party cookies, then Java and JavaScript options. Since overly tight security may affect comfortable use of the web, balancing of both sides seems to be the right solution. Unfortunately, by disabling cookies and JavaScript, you also reduce the functionality of the web, so a retreat into privacy is not always an efficient option in practice.

[38] While an ordinary proxy application sends requests from its own IP address, it also sends to a web server (using *X-forwarded-for* variable) the IP address of the user who requested specific content. Anonymous proxy applications do not supply this item of information thus ensuring the anonymity of its users.

Protection against data interception

As already stressed, data transmitted on-line can be intercepted. Direct protection against interception is not possible in unprotected or public networks. But there is another solution – data can be converted into a format unintelligible for the attacker even if it is intercepted.

One of the best known and most efficient protection techniques is cryptography. Cryptology is the science of secrecy, coding and encryption of messages, and decryption of encrypted data (cryptanalysis). In Greek, *cryptos logos* means hidden word. So, we encrypt messages to prevent interceptors from reading them.

In cryptography, the basic message is termed cleartext or plaintext, while the encrypted one is the cryptogram or a ciphertext. A cleartext is converted into a ciphertext using some pre-defined procedure (an algorithm or a method), where parameters contained in the encryption algorithm are assigned certain values that represent a key or a password. This implies that partners in correspondence must agree on the algorithm and key to be used if they want to exchange encrypted messages. Viewed from the perspective of keys, two cryptographic methods exist: symmetric cryptography, which uses the same key for the encryption and decryption of a message, and asymmetric, where the encryption key is different from the decryption key. Besides, there are also hash algorithms (also called message digests or fingerprints)[39] which convert a character string of arbitrary length into a number of fixed length, meaning that they actually calculate the digital fingerprint of this string as a basis for the digital signature. By using various combinations of cryptographic methods, digital signature and certificates, which may include the time of origin, information about the owner, expiration date and the like, it is possible to ensure confidentiality, integrity and authentication of messages.[40]

Mathematicians and computer experts have developed a number of encrypting algorithms, but a milestone in the history of cryptog-

[39] The most popular algorithms for the implementation of digital fingerprints are MD5 and SHA.

[40] In addition, the security application should also ensure the prevention of data nonrepudiation and access control.

raphy occurred towards the end of the 1970s with the introduction of the RSA algorithm which was mentioned in the foreword. Its creators were Rivest, Shamir and Adleman of the Massachusetts Institute of Technology. The RSA algorithm has become known for being highly secure (Vidmar 1997, 181). It is an asymmetric encrypting algorithm which presupposes that the sender and the recipient both have their own pair of decryption keys, one public and one private. One advantage of this method is that it does not require safe channels for the transmission of these keys, since public keys are accessible to all and private ones are kept secret by their owners. In order to send such a message, the sender needs to know which public key is used by the recipient and to have his/her own private key, and vice versa.

In June 1991 the computer programmer Phil Zimmerman wrote the PGP (*Pretty Good Privacy*) software based on the RSA algorithm. Zimmerman was strongly convinced that democracy and privacy were closely connected and that the only way to protect one's privacy was powerful cryptography (Zimmerman 1993). Therefore he published his program as freeware on the Internet, and it soon spread across the world (Phil Zimmerman Case 1998). The program evolved over time, so today it enables digital signatures, the exchange of public keys via keyservers, encryption of files and disks, wiping of files, and it even includes an ingenious system for testing how trustworthy a public key is.

Within just two years of its publication, Zimmerman's software became de facto the standard for the efficient protection of e-mail (Zimmerman 1993), so in February 1993 he was visited by FBI agents under suspicion that he had made possible unlawful export of military technology (Phil Zimmerman Case 1998). In the US, cryptography is considered a military technology[41] whose export is subject to authorization. In January 1996 the investigation was discontinued with no lawsuit brought against Zimmerman, because investigators could not find proof of suspected criminal offense. But the bitter feeling that Zimmerman's case was an attempt at intimidation lingered on.

[41] Export of cryptographic products from the US is regulated by the *Arms Export Control Act* and *Export Administration Act*. According to these acts, most cryptographic products are categorized as ammunition and their export is subject to authorization (Allard and Kass 1997, 574).

Of course, encryption is not only utilized in e-mail transmission but can also be used to encrypt file contents and even entire hard disks, that is to say, to protect message content within a specific system.

The most important element of encryption is the encryption method used. While a weak cryptographic method may appear to provide safety, in reality it does not. It should also be kept in mind that some encryption methods were developed in cooperation with various US state agencies (particularly the National Security Agency), so they are not necessarily as secure as they may appear at first glance. Similarly, certain methods developed in secrecy by unknown companies should not be trusted. The argument, or rather the marketing trick, that the secrecy of the method used guarantees security, is false and usually points to the fact that the method has not been tested in public or not tested at all. A principle that gained ground in cryptography is that all cryptographic methods must be publicized and tested by leading cryptanalysts, since only that can guarantee their quality. A good method will prevent an attacker from employing well-known and efficient techniques, so he will have to resort to a brute force attack (in which all possible combinations of passwords should be tested), which is an exorbitant task and therefore relatively inefficient.[42]

It is good to know that even superior cryptographic methods have limitations. The degree of security of an RSA algorithm, for example, depends on the keylength. In addition, the RSA encrypted message can be decrypted by factoring the key. This is a special mathematical procedure which searches for prime number factors of the given key. In March 1994, Atkins, Graff, Lenstra and Leyland wrote an article titled »The Magic Words Are Squeamish Ossifrage«, in which they described how they managed to factor a 129-digit number (426-bit key). The experiment involved 600 volunteers and 1,600 computers, and they needed 8 months to decipher the key. In August

[42] A brute-force method requires a considerable processor capacity, but it could be augmented through distributed processing. There are certain volunteer projects, the most popular being *RC5 Challenge* conducted in 1997, in which users make available their computer for the processing of data received via the Internet while their computers are not in use. The processed data are then sent back to the central server. In effect, they donate a portion of their processor time which immensely increases the processor capacity. Distributed.net (http://www.distubuted.net) is one organization involved in the breaking of encrypted messages using brute force attack.

1998 Lenstra and Riele managed to factor a 155-digit number (512-bit key) within just seven months. It is estimated that by using distributed on-line data processing this time could be reduced to as little as a few days (RSA Laboratories 2000, 48, 52).

But selecting the right method is not enough. The choice of password is equally important. A password must be such that it is not easy to guess. The best method is to combine digits and letters. A username, partner's name or the name of your favorite pop band is definitely a bad choice, since this would enable the potential attacker to use a »dictionary attack« to crack the password. Similarly, a password must not be too short, since the number of combinations rises exponentially with the number of characters it contains. A password must be remembered and not jotted down, and different passwords should be used for different systems. Experts recommend regular changes of passwords, and certain systems are indeed based on one-time passwords, meaning that each time the user logs on a new password must be used.

A self-protective attitude further implies that one should be aware of the possibilities of abuse and consequently use encryption wherever needed. So, for example, it makes a lot of difference whether sensitive data are transmitted via the Internet using secure connections, for example, the Secure Sockets Protocol or SSL (a protocol which enables encrypted connection between the server and the client) when using web services. In the case of e-mail or other interactive systems such as ICQ, a powerful encryption method should be used. There are many cases in which victims of abuse were individuals or companies that had at their disposal quality encryption technology but were too negligent to use it or insufficiently strict about its use.

Protection against intrusion and stealing of data

Of course, encryption can also be used to protect information stored on a specific computer system by which we prevent abuse if an intruder gains physical or virtual access to the system. Today there are software solutions which create a special encrypted file on a hard disk which is mounted as a virtual disk in the operating system. Work with such a virtual disk proceeds as usual, but the data are

stored in the encrypted file to which access is possible only by entering the required password.

Messages can also be hidden rather than encrypted (e.g. within audio or video files), and this method belongs to the area of *steganography*. The hiding of messages is more useful if one wants to use a digital watermark or digital serial numbers for files than for the protection of sensitive data. A combination of cryptography and steganography is also an option.

Yet sometimes it is possible to intercept data even before they are encrypted, or immediately after decryption. The most typical example is the use of the instructive viruses mentioned earlier. An intruder may use one to intercept the password or data while they are entered into the computer or to retrieve them from the disk if stored in an unencrypted format. Other viruses steal data such as files or e-mail addresses from the address book and send them to random addresses across the Internet. Computer security experts stress anti-virus protection as the most important precaution. Since new viruses appear on a day-to-day basis, it is important that a virus protection package is updated regularly. The anti-virus packages mainly enable live updates[43] to facilitate the procedure. These packages and updates are not available free of charge, but the investment definitely pays off by reducing the risk of infection and the potential loss of data.

The most basic protection against harmful intrusions is regular updating of software (here we primarily have in mind the Windows operating system and Microsoft's service Windows Update, although other systems are not excluded). The risk of intrusion may be reduced by using a firewall[44], which is a kind of intermediary between the user's computer and the network to which it connects. A firewall checks all communications between the local computer and

[43] On the one hand, the technology of live updates makes easier the updating of software, but one should also be aware that it opens new channels of abuse. This service opens door for the sneaking in of a malicious software application, a false virus-protection software (e.g. an empty file instead of new virus definitions), and even overtaxing of a system by sending huge amounts of (random) data using this service.

[44] Even though a firewall is a cheap and fast solution, one should keep in mind that it is powerless if the system contains a security hole.

the external world, so it can prevent undesired data input or output. A firewall may consist of a separate computer or a special program that is activated every time one turns on the computer, just like any anti-virus package. The limitations on access can pertain to the IP address or ports through which the communication takes place. Since there is a danger that a virus or a Trojan horse may pretend to be a program to which a firewall allows passage, certain firewall packages use digital signatures to check on a case-by-case basis the authenticity of the application attempting to establish a connection.

Deleting electronic traces

There are two types of electronic traces that should be distinguished: one involves the electronic traces left behind in the local system, and the other electronic traces outside a local system. Naturally, the user cannot intervene outside the local system – all he/she can do is to leave behind as few traces as possible, or to destroy them. This subject was discussed in the chapter dealing with the anonymization on the Internet.

However, the user usually has free access to the electronic traces stored within the local system he/she uses. Information about computer usage and web services accessed is stored on the hard disk, so it may be useful to consider deleting these traces, particularly if one computer is used by several users or if the user intends to sell the computer. This includes the deletion of cookies, of old records in the register (applicable to Windows-based computers) and of local log files, as well as the wiping of data files and free space on the hard disk. The Delete function actually does not remove files permanently from the disk, so the content of the deleted files may be recovered partly or in full by using various tools. File content is permanently deleted (wiped) only when old data are *overwritten* by new (usually random) data. In most cases old data will be permanently removed only after several instances of overwriting (referred to as »the number of passes«), because in certain cases old data could be reconstructed using an electronic microscope even after one (or several) passes. This is possible thanks to the thermal contraction and expansion of the disk. The methods of magnetic force microscopy and the wiping procedure have been described by Peter Gutmann of the

University of Auckland in an article titled »Secure Deletion of Data From Magnetic and Solid-State Memory«,[45] so one among many data wiping methods has been named after him. This method requires 35 passes using a special procedure. Of course, the deletion of traces also includes the deletion of a temporary memory named swap file before a computer is shut down, to prevent later recovery of memory content when it is switched on again.

Protection against TEMPEST attacks

Despite the potential of the TEMPEST technique described earlier (the technology of intercepting electromagnetic signals emitted by electronic devices), there is at least one possible method of protection against this type of eavesdropping. Hardware solutions include the coating of cables, electronic equipment or even entire buildings with metal sheets which prevent the »leakage« of electromagnetic signals, but these solutions are rather costly. Kocher et al. of Cryptography Research propose various types of protection for use with smart cards, all of which imply modifications of the smart card's basic concept. However, in addition to not being cheap, these solutions are not easily accessible.

Kuhn and Anderson described a much cheaper software protection against TEMPEST attack – the use of special TEMPEST prevention fonts which make it impossible for an eavesdropper to reconstruct a satisfactorily clear picture of the screen under attack. In other words, an eavesdropper can still intercept the signal, but cannot make much use of it. Furthermore, they have invented two other methods of preventing the interception of signals coming from a keyboard or a hard disk. Both methods could be implemented at relatively low cost by upgrading the keyboard or disk drivers (Kuhn and Anderson 1998, 139). Today, ordinary users have at their disposal only special TEMPEST prevention fonts which are integrated with the PGP package.

[45] The article was presented at the USENIX Security Symposium Proceedings in California in 1996; it is available at http://www.safedelete.com/a-gutmann.phtml.

Cryptography and the movement for electronic privacy

The demands for ever higher levels of surveillance may indeed stem from the need for an utterly secure and predictable society, but the introduction of cryptography has given rise to apprehensions that the state will no longer be able to exercise control over criminal offenders or activities undertaken by its enemies. Since self-protective conduct also includes techniques which make surveillance (either lawful or unlawful) much more difficult, the question is whether the state should be given just a *possibility* of exercising control over individuals, or have an *absolute right* to exercise such control. Two articles of the Slovene *Criminal Proceedings Act* are interesting in this respect. Article 5 specifies that the defendant is not obliged to testify against himself/herself or his/her relatives or to plead guilty. In practice this means that a defendant who made use of some cryptographic method is not obliged to reveal the password and thus enable investigators to access the encrypted data and eventually obtain incriminating evidence. However, a person who is not a defendant in the criminal procedure cannot evade testimony unless he/she is the defendant's relative and unless it is likely that such a testimony would bring heavy shame upon himself/herself or his/her close relative, or would cause a considerable harm to them or lead to criminal prosecution (Article 238 of the Criminal Proceedings Act).

Besides, one characteristic of modern information society is that it increases the potential for ubiquity. Territorial borders are ever more permeable, and their role in restricting the flow of data and information has been diminishing. However, if space is removed as an obstacle, its protective role is also lost (Mlinar 1994, 11).

Denning and Baugh mention that the terrorist organization Hamas uses encrypted Internet communications to distribute maps, pictures and other terrorist attack details. Similarly, cryptography and the Internet are exploited in child pornography distribution, thefts of credit card numbers, drug trafficking, intrusions into computer systems, money laundering and spying (Denning and Baugh 1999, 252–274). The September 11th terrorist attacks aroused suspicions that those planning the attacks made use of cryptography (these suspicions were not later confirmed) (Harrison 2001). Yet in

the opinion of these authors, the biggest problem is not the exploitation of the Internet but of cryptography.

By the late 1920s, the FBI had established a special department that dealt with the use of cryptography by bootleggers (Shireen 1998) during Prohibition in the US. Criminal offenders were quick to start exploiting computer technology as well, so in 1998 the FBI's department composed of computer experts handled 299 cases in which computer technology was used for criminal purposes. The use of cryptology accounted for 4% of these cases (Denning and Baugh 1999, 259). Denning and Baugh note that the use of unbreakable encryption techniques, which can completely prevent eavesdropping, is on the rise. The authors thus mention that in 1995 the FBI was unable to break encrypted information in 5 instances, with this number rising to 12 in 1996 (Denning and Baugh 1999, 253). They also note that high costs and the incompatibility of various types of equipment for the encryption of telephone conversations slow down the expansion of cryptographic methods into the field of telephony, but also point out that Internet telephony is extremely cheap enabling the encryption of audio communications at minimal costs.

The term *crypto anarchy* was coined in connection with the criminal usage of cryptography. Those predicting crypto anarchy agree that it will come as an inevitable consequence of the expansion of publicly accessible cryptography. »With this technology,« they say, »it will be impossible for governments to control information, compile dossiers, conduct wire-taps, regulate economic arrangements and even collect taxes.« (Denning 1997, 175). To put it differently, by preventing the state from exercising control over computer and telecommunications systems, the latter become "safe heavens for criminal activity" (Denning 1997, 177), and this could lead to social chaos. Cryptography is therefore considered as being exploited for purposes primarily targeted against the state (Denning 1997, 187 and Zimmerman 1994), and consequently, against citizens as well.

Various countries at various times have striven to gain control over cryptography (Bert-Jaap Koops 1997), so it is not surprising that the discovery of an *efficient* cryptographic method (the RSA algorithm) caused alarm within the US administration. As a matter of fact, before the invention of the RSA algorithm the majority of cryptographic keys could be broken.

One of the most widespread cryptographic algorithms in civil spheres and in banking is (was) the DES algorithm (short for *Data*

Encryption Standard) developed by IBM. DES was a derivation of the cryptographic algorithm *Lucifer* previously used by the US military. Since the theoretical background for this algorithm had not been fully explained, there was a suspicion that the military knew how to break the civil variant of DES (Vidmar 1997, 179). It later turned out that the civil variant was actually a modified version of the algorithm used by the military, in which a 64-bit key replaced the original 128-bit key. Moreover, of these 64 bits, 8 were control bits, meaning that the effective key length was 56 bits. Another detail that subsequently came to light was that, at the time of development, IBM experts were aware of the mathematical shortcuts that could lead to the breaking of this algorithm, but this fact was concealed under pressure by the NSA. In 1990 and 1991 the Israeli cryptographers Eli Biham and Adi Shamir presented a new variant of cryptanalysis – differential cryptanalysis. This gave rise to a suspicion that DES was purposefully modified in such a way that the efficiency of this previously unknown attack method was even higher (Bach et al. 1999).

In 1993, at a conference about cryptography, Michael Wiener presented a plan for a device intended for the breaking of the 56-bit variant of the DES algorithm. Its price was estimated at 1 million dollars, and it was expected to be able to break the DES algorithm in three hours and a half on average. Phill Zimmerman calculated that a somewhat more complex device worth 100 million dollars could complete this task in two minutes on average. In his testimony before a sub-committee of the US Senate in 1996 he stated that, given its budget, the NSA would need just one second to break the message encrypted using a civil variant of the DES algorithm (Zimmerman 1993). In July 1998 John Gillmore of Electronic Frontier Foundation presented a device named DES Cracker which used a brute-force method and distributed data processing via the Internet to break the DES encrypted message, and it completed the task in 22 hours (RSA Laboratories 2000, 64). Since then DES has been known to be unsafe.[46]

[46] Other, modified version of DES are also in use in civil spheres and particularly in banking, for example, *Triple DES*, which is indeed a stronger algorithm although still based on the original DES algorithm. It is expected that DES will soon be replaced with AES – *Advanced Encryption Standard*. The algorithm for this standard called *Rijndael*, by Joan Daemen and Vincent Rijmen, was chosen among several shortlisted ones towards the end of 2000. All shortlisted algorithms for AES were published and tested by leading world cryptoanalysts.

Before the invention and public announcement of the RSA algorithm, a *de facto* monopoly over the development of new cryptographic methods was in the hands of the military, and partly academic circles. The situation changed with the development of information and communication technologies which enabled the production and publication of quality, cheap encryption software. After losing its *de facto* monopoly in the field of cryptography, the state continued to make attempts to enforce a *de jure* monopoly. Supporters of restrictions on cryptography, including the US administration, made a number of proposals with this objective in mind.

Among the earliest proposals was one dating from 1991 which suggested that cryptographic products should include trap doors to enable state authorities to access encrypted messages. This bill was not passed, but in 1993 the US government published another proposal for a *key escrow system* which envisaged authorization of encryption keys issued by authorized agencies to individuals (EPIC 1998c and EPIC 1998d).

Another similar proposal pertained to cryptographic standards. The basic idea was that the state should enforce upon the market cryptographic standards that would enable the state to access encrypted data. All other cryptographic tools not complying with these standards would not obtain licenses and their use would be restricted, which was expected to prevent their dissemination on a wide scale (Denning 1997, 188). It soon became obvious that this proposal was pointless, since it was not reasonable to expect that criminals would use licensed cryptographic tools (Denning 1996, 216). One variant of this proposal even envisaged legal prohibition of the use of specific cryptographic methods. According to this proposal, individuals could still develop their own cryptographic methods, but only for personal use and educational purposes, while their dissemination would be subject to authorization (Denning 1997, 187–188).

Still another flawed proposal suggested the use of weak cryptology exclusively, with a view to enabling state authorities in the possession of adequate equipment to break the protection quickly in emergency situations (e.g. kidnapping) (Denning 1997, 184). Unfortunately, this type of cryptography does not ensure adequate protection to the user, since the encrypted message can be broken by anybody possessing a computer of some capacity and having computer knowledge.

The deficiency of the majority of these proposals stemmed from the implied restrictions on freedom of speech. Viewed from the legal and security perspectives, the proposal to use cryptography only inside closed systems i.e., link encryption, seemed to be the most adequate one. According to this proposal, encryption would be used only inside a specific closed network, but data would leave that network unencrypted, so that state authorities could intercept these at the point of their leaving such a system (Denning 1997, 184, and Denning and Baugh 1999, 253–254). A similar system is in use in GSM networks for data transmitted by way of radio waves from a telephone handset to the base station.[47]

Another proposal aimed at curbing abuse of cryptography envisaged double penalties for criminal offenders using cryptography.[48]

The leading role in the struggle to ban, or at least restrict, the use of cryptography in the US was played by the FBI, in close cooperation with the National Security Agency and other state bodies (EPIC 1998b). Even though the use of cryptographic equipment in the US is today legal (its export is restricted), the US state authorities do not miss any opportunity to attempt to restrict its use or increase their competences in the area of eavesdropping and interception of electronic messages. Demands for the prohibition of cryptographic products were voiced soon after the September 11th attacks (Harisson 2001), including demands that the police should have the right to order surveillance of Internet communications for the duration of 48 hours without a court order (McCullagh 2001b, 2001c and 2001d).

The US government's attempts to criminalize cryptography and a subsequent boom in commercial surveillance, triggered a strong movement for the protection of electronic privacy on the Internet. Privacy activists strive to increase the awareness of individuals

[47] It should be pointed out that GSM encryption algorithms have already be broken, which is not surprising given that they were developed with the »help« of the NSA. In GSM telephony, audio messages are encrypted using A5/1 (stronger) and A5/2 (weaker) algorithms, while encryption keys are generated using A8. A8 was broken by Ian Goldberg and David Wagner in April 1998. In August 1999 the same authors proved that A5/2 could be broken in real time. The first successful attack on A5/1 was made by Jovan Golić in May 1999. Biryukov and Shamir have proven that it could be broken in less than one second using a copmuter with at least 128 Mb RAM and two 73 Gb hard disks (Schneier 1999).

[48] This proposal was put forward in the US Senate Trade Committee (EPIC 1998a).

about possible ways of control by providing practical advice and software packages for the protection of privacy, with the stress being on the promotion of cryptography. In addition, these organizations and individuals strive to thwart all attempts at prohibiting or restricting the use of cryptography.

In the opinion of various organizations fighting for electronic privacy, future communication will be mainly electronic, that is to say, such as can be controlled imperceptibly and on a large scale. They hold that cryptography is one instrument that ensures privacy, and since privacy is a constitutional right, the right to use cryptography is also equated with the right to privacy. Even though aware of the potential abuse of cryptography, they are convinced that the harm caused by prohibiting it would outweigh any harm arising from its free use (Zimmerman 1993).

The controversies between opponents and advocates of the unlimited use of cryptography issue from their different understanding of the state's role. While its opponents see the state as an efficient safeguard of citizens' safety and welfare, advocates see it as an institution in Foucault's sense of the word, that is to say, as limiting their rights and freedoms.[49] Phill Zimmerman thus stated that »if we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of« (Zimmerman 1993).

[49] »What the government really seems afraid of in the Zimmerman case is not Pretty Good Privacy, but privacy itself.« (The Zimmerman Case 1995).

SLOVENE LEGISLATION AND PRACTICE

The right to privacy within Slovene legislation appears in two forms – as an individual right of a private character, and as a human right, meaning that it also has a public nature (Šturm et al. 2002, 369). The right to privacy protects an individual against interventions from other individuals and against interventions from the state. The right to privacy is a constitutional right in Slovenia. It is the subject of the second chapter of the *Slovene Constitution*, which is concerned with the protection of various aspects of privacy. According to Klemenčič, the fact that the right to privacy is broken down into many sub-categories arises from specific conditions enabling various forms of privacy invasion. Klemenčič further notes that each right pertaining to the area of the protection of privacy should invariably be interpreted from the perspective of general and integral protection of privacy and individual rights (Šturm et al. 2002, 392).

Article 35 of the *Slovene Constitution*, therefore, specifies that privacy and individual rights are inviolable; Article 36 deals with the inviolability of dwellings; Article 37 is concerned with the privacy of correspondence and other means of communication which may be considered to include audio and digital forms of communication, and Article 38 with the protection of personal data. Of course, the *Constitution* determines the framework for the protection and exercising of these rights, while their implementation is regulated by legislation and judicial practice. Naturally, the scope of the protection of privacy rights is not absolute.

Territorial privacy

The inviolability of dwellings, or territorial privacy, has evolved from a historical presupposition, which originated in England, that a citizen's home is inviolable. Zupančič holds that this involved only the territorial dimension of the protection of dwellings. The problem today arises from the fact that advances in surveillance technologies

radically reduced the importance of territorial privacy protection (Šturm et al. 2002, 387). In consequence, the principle of protecting reasonable expectation of privacy gained recognition, so the term »dwellings« is not understood in its narrow sense but covers all premises in which a citizen can reasonably expect privacy, including hotel rooms, holiday resorts and the like. Klemenčič thus states that »not only premises, property and owners are legally protected, but also individuals who (justifiably) expect to have privacy at a specific moment and a specific place or by adhering to a specific conduct« (Šturm et al. 2002, 401).

The *Penal Code of Slovenia* specifies sanctions for an invasion of territorial privacy in Articles 149 and 152. Article 149 prohibits unauthorized recording or image taking of individuals or their premises if such an act means a serious invasion of privacy. Article 152 specifies sanctions for the violation of dwellings through an unauthorized entry into or search of private facilities, or an attempt to do so.

It is not as clear, though, which approach would be appropriate to deal with virtual space. By all means, in the realm of the virtual world, an intrusion into a computer system and a search of that system by way of a telecommunications network (interception excluded) would represent an intrusion into one's (virtual) space. Intrusion into a computer system is the subject of Article 242 of the *Penal Code*, but according to this article, such an intrusion is punishable only if it is connected with business dealings and made with the aim of acquiring illegal property-related benefits or causing material harm to others. Unfortunately, this wording could lead to a situation in which an intrusion into a computer system not resulting in material harm, or not yielding other kinds of benefit for the intruder, would not be sanctioned. In such a case, Article 152 of the same act would need to be applied i.e., one which prohibits unauthorized entry into someone's premises (of course, if a court would be willing to accept the notion of virtual space), and Article 309 which sanctions the production or acquisition of tools for intrusion into a computer system.

Privacy of communications

Article 37 of the *Slovene Constitution* deals with the secrecy of correspondence and other means of communication, where means of

communication should be interpreted in the widest sense of the word – it may include telephone communications, electronic mail, SMS and the like, since the form or content of communication is irrelevant in this context. In addition, messages are not necessarily communicated via public telecommunications networks – privacy protection also applies to private or closed telecommunication systems (Šturm et al. 2002, 395). Obviously, in the latter example, for example, when an employee uses the company's telephone network, the scope of protection is not as wide.

In addition to the content of communications, traffic data, which are also an integral part of communication, are a subject of protection (Šturm et al. 2002, 396). This means that provisions pertaining to privacy of communication protection are also observed with regard to other information, for example, telephone numbers, data about the length of communication or the quantity of transmitted data and so on.

The Constitution guarantees this right to all who reasonably expect privacy, regardless of whether data are intercepted in real time or a seizure (e.g. of a postal package) is involved. This right is infringed as soon as somebody unlawfully intercepts a certain piece of communication and becomes acquainted with its content, even if this information is not put to use (Šturm et al. 2002, 398).

However, Klemenčič states that »the scope of the right to the privacy of communication is not limited to ensuring secrecy of communication content and related data, but also prohibits disproportional prohibition of communication with the outer world.« (Šturm et al. 2002, 395) The ruling of the *French Court of Cassation* No 99-42.942 dated October 2, 2001 explicitly states that »an employer who reads messages by an employee sent from or received on a company's computer, violates the basic rights of that employee as defined in Article 8 of the European Convention on Human Rights. ... This is applicable regardless of whether the employee was informed in advance that a company's computer should not be used for non-business purposes. ... A company or another institution must not be a place where employers would arbitrarily or without limits exercise their rights of discretion; they must not become areas of total surveillance in which basic human rights would have no value. ... In our opinion, a general and full prohibition of the use of e-mail for non-

business purposes is unrealistic and violates the legal principle of proportionality.« (Šturm et al. 2002, 402). Accordingly, any move on the part of the state involving disproportional prohibition of cryptography or anonymous mail servers could represent an invasion of the constitutionally guaranteed privacy of communication (Šturm et al. 2002, 395).

The right to privacy of communication is also dealt with in Article 150 of the *Penal Code* prescribing sanctions for the violation of the secrecy of means of communication. This article prohibits unauthorized opening of letters and other post and interception of messages transmitted via telecommunication networks, or reading of their contents without opening a letter or other post. Similarly, it prohibits unauthorized acquaintance with the content of a message transmitted by telephone or other telecommunication equipment, as well as unauthorized forwarding of someone's letter to a third party. Article 151 further prohibits the publication of private communication without consent of the authorized person.

Privacy of communication may only be invaded on court order and if such an invasion is deemed necessary for the purpose of criminal proceedings or in order to protect the security of the state. In Slovenia, this area is regulated by the *Criminal Proceedings Act* and the *Slovenian Intelligence and Security Agency Act* and carried out by the police or Slovenian Intelligence and Security Agency (SOVA). Unlawful invasions of the privacy of communications are prohibited and sanctioned. Article 130 of the *Telecommunications Act* deals with surveillance of telecommunications. Among other things it specifies that telecommunication operators must ensure, at their own expenses, adequate software and suitable interfaces. Article 50 of the *Postal Services Act* prescribes that providers of postal services should enable an authorized body to access, on the basis of a court order, the content of post. Both telephone operators and providers of postal services must ensure an indelible record of such moves.

The powers of authorized state bodies regarding intrusions into privacy differ. Article 151 of the *Criminal Proceedings Act* specifies that surveillance of communications and messages, eavesdropping, secret monitoring, following and recording are permitted in the case of the following criminal offences:

- criminal offences against the security of the Republic of Slovenia and its constitutional order and criminal offences against humanity and international law, punishable by imprisonment of up to five years;
- kidnapping, unauthorized production and traffic of drugs, enabling others to take drugs, extortion, unjustified taking or giving of presents, forgeries, money laundering, smuggling, receiving or giving of bribes, associating for criminal purposes, prohibited production or trafficking of weapons or explosive substances, and hijacking of a plane or a ship;
- other criminal offences punishable by imprisonment of eight years or more.

(Article 151 of the *Criminal Proceedings Act*)

The *Slovenian Intelligence and Security Agency Act* lists the following cases in which surveillance of letters and control over and recording of telecommunications is allowed (excluding eavesdropping within facilities):

... if there is a probability that the security of the state is threatened through:

- secret activities aimed against its sovereignty, independence, integrity or strategic interests;
- secret activities, plans and preparations for the realization of international terrorist acts against the Republic of Slovenia and other forceful acts against state bodies and individuals holding public functions in the Republic of Slovenia and outside it;
- forwarding to an unauthorized person outside Slovenia data and documents which are categorized as classified in the Republic of Slovenia;
- preparations for an armed attack on the Republic of Slovenia;
- intelligence activities of individuals, organizations or groups carried out to the benefit of foreign countries;
- international organized criminal activities;

and there are grounds to expect that a specific means of telecommunication is used in connection with such an activity or that it will be used, whereby it is possible to conclude that intelligence cannot be obtained in another manner, or that by obtaining intelligence in another manner the lives and health of people would be jeopardized. (Article 24 of the *Slovenian Intelligence and Security Agency Act*).

While the *Criminal Proceedings Act* includes a detailed list of criminal offences and cases in which privacy of communications may be invaded, the *Slovenian Intelligence and Security Agency Act* is not as specific. For example, it stipulates that state security is threatened by »activities aimed against ... the strategic interests of the Republic of Slovenia,« but experts draw attention to the problems potentially arising from such a wording which enables loose interpretations of »strategic interests« in contrast to other precisely defined criminal offences. This could result in SOVA acquiring too easily a court warrant for communications interception.[50] An important provision is that SOVA is obliged to inform the prime minister about its activities, as well as the president of the republic, the president of the National Assembly and other ministers if these activities are related to their fields of competence (Article 6 of the *Slovenian Intelligence and Security Agency Act*). SOVA does not prosecute criminal offenders. If it deals with a suspected criminal offence, it must provide information about it to the director general of the police force and the public prosecutor in accordance with Article 8 of the same act. It seems that it is precisely the wording of Article 24 of the act that enables potential abuse on the part of SOVA.

Privacy of information

Privacy of communications is closely related to the protection of personal data, or privacy of information. Unfortunately, the conditions within this area seem to be much worse. Although privacy of information is relatively well regulated by existing legislation, the problem is a serious disorder in practice, even though this field is subject to supervision by inspection agencies.

The protection of privacy of information is guaranteed by the *Constitution*. Furthermore, article 154 of the *Penal Code* stipulates sanctions and prohibits any use of personal data that is in contravention of the law, or any intrusion into an electronic database for the purpose of obtaining some item of information for personal use or for the use of a third party. In addition, Article 225 prohibits un-

[50] It can also make it more difficult, since such a loose formulation leaves more manoeuvring space for the president of the district court who can thus turn down more easily a request for the surveillance of letters and telecommunications. From the perspective of privacy protection, not only abuse its problematic but also the *possibility* of abuse.

authorized access to an unprotected database, modification and copying of its content or insertion of viruses. The conditions under which personal data may be gathered, processed and used are regulated by a separate law – the *Personal Data Protection Act*. In addition, Slovenia also applies the provisions contained in the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ratified in 1994. The Convention and the said Act stipulate that everything that is not explicitly allowed in connection with data gathering and processing is prohibited. The first version of this act was adopted in 1990, with amendments dating from 1999 and 2001. Its provisions pertain to personal data exclusively, that is to say, the data that reveal the properties, state or relationships of the individual. Among other things it also prescribes the conditions under which processing of these data is allowed, then the rights of the individual relating to his/her personal data, the conditions under which these data can be taken out of the country and the supervision of personal data protection.

Article 3 stipulates that personal data can be gathered, stored and processed only if such gathering, storage or processing is prescribed by the legislation (by-laws excluded) or if the database administrator obtains written consent from the individual in question. Persons whose personal data are gathered must be acquainted in advance with the purpose of data gathering (by giving written consent, or such a purpose must be prescribed by the legislation), while personal data can be gathered only for the purposes so defined (Article 9). In principle, personal data can be gathered and stored for only as long as needed to attain that objective (Article 10), and deleted or blocked once this objective is attained. Exemptions must be defined in the legislation.

The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* is even stricter in this respect, since it envisages security measures aimed at ensuring that data are stored for specific and lawful purposes exclusively and that only data that are adequate, relevant and not excessive with regard to the purpose are processed (Šturm et al. 2002, 411).

The *Personal Data Protection Act* defines in detail the duties of the personal data administrator. Article 8 thus stipulates that personal data may only be acquired directly from the individual in question,

except in special examples which must be defined in the law. The same article further prohibits the use of the same linkage symbol in databases maintained in the areas of public security, state security, defence, judiciary and health. The linkage of these databases is allowed only if there is a legal basis or the individual has given his/her written consent. The manager of such a database must enable free of charge access to and copying of personal data to an individual within 15 days of receiving such a request, or must supply a printout of these data within 30 days of receiving such a request. If a manager of such a database fails to fulfil this obligation, he must provide a written explanation of the reasons for failing to do so. The 30-day deadline is also applicable to the provisions in Article 18, stipulating that the list of recipients who received the personal data of an individual must be supplied at the request of that individual.

If an individual provides evidence that his/her personal data were gathered in contravention of the law, the database owner must delete these data or update them, or correct them if the data were incomplete or inaccurate. The costs are borne by the database owner. The database owner must also keep a separate catalogue for each database, which contains, among other things, a detailed description of the kind of data that are gathered and the manner in which they are gathered, the purpose of their use and the duration of storage, the list of users of these data and a description of how these data are secured (Article 15). Furthermore, the Ministry of Justice, which is responsible for the protection of personal data, must keep a register of all databases containing personal data. Information in this register is provided by database owners (Article 16).[51]

Personal data can be taken across the border only to those countries in which personal data protection regulations cover foreign citizens as well, unless the individual gives written consent to take his/her personal data out of the country and is acquainted with potential consequences (Article 24). According to Article 4, the transfer of certain delicate types of personal data (e.g. those that pertain to race or origin, political, religious or other orientation, affiliation

[51] The register of the databases containing personal data is available at the web page of the Ministry of Justice at http://www.sigov.si/mp/; it is updated on a daily basis.

with a trade union, sexual orientation, criminal offences or medical details) via telecommunications channels is allowed only if data are encrypted and protected with a digital signature.

In special cases pertaining to national security, defence, public security, prevention, discovery and prosecution of criminal offenders, the right of the individual to access or copy gathered data may be restricted. The law also prescribes that the implementation of these legal provisions will be supervised by the *Inspectorate for Personal Data Protection*, which is obliged to submit an annual report on its work to the *Ministry of Justice* and the *Human Rights Ombudsman*.

In its 2001 annual report, the Inspectorate noted an increase in the number of complaints and initiatives on the part of individuals in the period 1996–2001. This points to a growing awareness about privacy rights. The report further contains a conclusion that the majority of violations result from insufficient knowledge or misunderstanding of particular provisions in the *Personal Data Protection Act* (Bogataj 2001, 18). The following types of violations have been noted: failure on the part of database owners to supply required information to the Ministry of Justice, inadequate protection of personal data, deficient records about the forwarding of personal data to other users, occasional supply of personal data to unauthorized users (e.g. in hospitals or medical centers). The Inspectorate further identified several cases of unauthorized gathering of data not grounded in legislation or carried out without obtaining written consent from the individual (e.g. video surveillance in public facilities if images are stored and used to build a database of personal data), excessively long periods of personal data storage, or storage of an excessive amount of personal data. In principle the public sector may process only personal data prescribed by the law, unless the law prescribes that data gathering is subject to written consent by the individual. In contrast, the private sector can also process those types of personal data that are not mentioned in the law, but it must obtain consent in writing from individuals. The Inspectorate for the protection of personal data has thus concluded that in practice there are many examples of extortion and gathering of excessive personal data (Bogataj 2002, 20–21). It has further established that database owners frequently infringe the rights of individuals by preventing them from accessing, copying

or printing out their personal data, and by not fulfilling their obligations to correct or delete personal data on request.

A review of the register of databases containing personal data found on the web site of the Ministry of Justice at the end of 2002[52] showed that only one Internet access provider supplied information about personal databases, and was later joined by another one.

Internet access providers can collect personal data on the basis of the contract signed by the user, but they should nevertheless inform their users about certain facts, such as which personal data will be gathered (including data that is stored in log files), for what purpose and for how long these data will be stored. To our knowledge, most Internet users are unacquainted with these details. The second paragraph of Article 131 of the *Telecommunications Act* specifies that for the purpose of accounting and until the service is paid or the deadline for a delayed payment expires, the operator may store data needed to calculate the cost of the service provided. However, we could establish that log file data are stored longer than prescribed, as well as that data pertaining to users who do not pay for Internet access or pay a fixed price are stored. EU Directive 2002/58 enables member states to store any kind of traffic data for a limited period of time. A measure that is currently under preparation will oblige member states to legally bind telecommunications providers to store traffic data from 12 to 24 months (Možina 2002, 4). These data will be (are already) avialble to state authorities on the basis of court order. The problem involved is that such a rule enables the state to have an »(excessive) overview of the activities of users who are not suspects« (Možina 2002, 4).

Another question related to the Internet is which data gathering qualifies as non-excessive data gathering, particularly if the purpose of data gathering is not known. Certain Internet access providers and service providers (e-mail and web providers), gather a multitude of personal data including those that may indicate the social or economic status of the individual. It should be stressed that the law only allows the gathering of data supplied directly by the individual in question, so the gathering of certain other data, for example, those

[52] The report is available at the web page of the Ministry of Justice; it was prepared by Jože Bogataj, deputy inspector in the area of personal data protection.

about an individual's relatives, is unlawful. Similarly, the question about the quality of personal data protection seems reasonable, since one cannot know whether the internal documentation held by Internet access providers contains descriptions of relevant organizational, logistic and technical procedures for data protection.

So far there has not been recorded any request by an Internet user to view his/her personal data or to copy them. Article 18 of the *Personal Data Protection Act* stipulates that the database owner will bear the costs arising from such a request. But are Internet access providers organizationally and technically capable of fulfilling these legal obligations? Given the technical peculiarities of the Internet, consideration of amendments to the existing legislation would also seem to be in order. Such amendments should be aimed at ensuring that the transfer of personal data via an unprotected medium such as the Internet is always secured through the use of cryptographic methods and perhaps also digital signatures.

Similar questions emerge in relation to the on-line gathering of data and registration of software packages. In addition to the fact that users are frequently not acquainted with the purpose of data gathering and the duration of data storage, data are often transmitted without protection and forwarded to foreign countries. The law explicitly prescribes written consent, but meeting this obligation in practice is not easy in the case of the Internet. Article 15 of the *Electronic Business and Electronic Signature Act* stipulates that a secure electronic signature,[53] one which is confirmed by an authenticated certificate, is equal to a signature in one's own hand, but the use of electronic signatures in Slovenia has not yet become established in practice.

The reasons mentioned above make it necessary to ensure, as soon as possible, consistent protection of personal data in the area of the Internet, but also certain amendments to the existing legislation would be needed, in particular those parts prescribing written consent. As a matter of fact, the implementation of this rule has

[53] Article 2 of this law defines a safe electronic signature. According to these definitions, an electronic signature is safe if it is: connected only with the signatory; created using tools for safe electronic signatures that are under exclusive control of the signatory; is linked to the data to which it refers in such a way that any subsequent change to these data or to the links between them and the signature is obvious.

proved to be too complicated in cases involving on-line data. Furthermore, it would be sensible to define other conditions for the protection of certain types of on-line data, since owing to their nature these data should be publicly accessible even though the supervision of access to these data is not possible for practical reasons (we primarily have in mind information about the owners of Internet domains and DNS record). Also those types of data that are not strictly personal should be legally protected, for example, electronic traces on publicly accessible computers.

It would also be necessary to think about a mechanism for adequately preventing the private sector from gathering unnecessary data and making cartel agreements. The present arrangements could lead to a situation in which companies offering certain services could agree to offer their services exclusively to those users who consent in writing to data gathering on a large scale. In such a case, those users who decline to give such consent would be left without access to these services.

Another issue that should be considered is the standardization of organizational, logistic and technical procedures for data protection. In the report mentioned earlier, the Inspectorate for Personal Data Protection stated that personal data protection within the police was satisfactory (Bogataj 2002, 10). Perhaps their system of protection could serve as a model. At any rate, protection should include the supervision of access and the possibility of establishing who accessed which data, when, in what manner, and for what purpose. The use of cryptography and physical protection would enable the prevention of unauthorized access.

Organizational issues make the prevention of data gathering in certain areas unrealistic, but one condition that must be fulfilled is to make data gathering and use a transparent process and thus reduce the possibility of abuse to a minimum. The task of the legislation is to set the game rules that must be followed. Therefore, it would seem sensible to consider strengthening the staff of the Inspectorate for Personal Data Protection.

CONCLUSIONS

According to Beniger, the revolution in surveillance perpetuates itself and three factors make this possible. The energy utilization, the speed of information processing and control technologies coevolve in a positive spiral – advances in any one factor cause or enable improvement of others. One should not overlook technological advances, since technological innovations trigger the need for ever new technological innovations (Beniger 1986, 433–434). This opens new possibilities and creates new needs for surveillance. Data gathering technologies are a typical example. They caused the need for data storage technologies, while increased memory capacities created possibilities for improved and extensive data gathering methods.

These are the reasons why surveillance will continue to increase over time, with this trend very likely being impossible to reverse. Another issue is whether it would be sensible to reverse it. The issue of privacy oscillates incessantly between totalitarianism and anarchy, so the question is not to which side to tip the scale, but how to strike the right balance. It is important that the surveillance society should not become a totalitarian society. Accordingly, protective legislation which would make surveillance a transparent process is of outstanding importance, as is democratic supervision of surveillance. As our study has shown, one of the most dangerous dimensions of surveillance is its panoptic effect. The only efficient means of countering it is strong protection of civil and political liberties, particularly freedom of speech and freedom of political action. Privacy should by no means be reduced to an individual or individualistic level, but should be considered within a wider context of civil liberties. Privacy is one of the fundamental conditions for active citizenship, but the ultimate objective of protective legislation should not become a type of privacy that leads to individualism and isolation from society, but privacy that leads to active citizenship. While

some understand the right to privacy as generally having an explicitly negative status, meaning the right of the individual to be left alone, the privacy of communications, which is closely related to the privacy of personal data, brings with it an equally important value – the establishing and maintenance of contacts with others. In 1981 the US Supreme Court noted that the right to privacy is important because it accelerates the exchange of information with others, and not simply because it ensures independence and isolation (Šturm et al. 2002, 392). This, precisely, is one of the preconditions for active citizenship.

The determination of the limit to which the state and other individuals are allowed to intrude into personal matters constitutes one of the challenges that will be repeatedly confronted in the future. The struggle for individual rights and the development of democratic culture and technology will alternately tip the scales to one side or another. This cannot be prevented, since these areas are connected with change and development in an essential way. But we should continually strive to strike the right balance, and this is the point at which law and society need to keep pace with technological developments.

BIBLIOGRAPHY

Allard, Nicholas W. in Kass, David A. 1997. Law And Order In Cyberspace: Washington Report. In *Hastings Communications and Entertainment Law Journal (Comm/Ent)*, 19 (3): spring 1997.

»Amsterdam Schiphol Launches 'Iris Scan' Trial«. 2001. *Airwise News*. <http://news.airwise.com/stories/2001/10/1004008821.html>. (August 17, 2002).

»An Analysis of How the Events of September 11 May Change Federal Law«. 2001. *Tech Law Journal*. <http://www.techlawjournal.com/terrorism/20010917.asp>. (September 17, 2001).

Bach, E., et al. 1999. »The Cryptography FAQ (05/10: Product Ciphers)«. <http://www.faqs.org/faqs/cryptography-faq/part05/>. (August 17, 2002).

Banisar, David et al. 1999. *Privacy & Human Rights 1999*. <http://www.privacyinternational.org/survey/index99.html>. (May 23, 2000).

Batagelj, Zenel. 1997. »Direktni marketing, oglaševanje in internet« (»Direct marketing, advertising and the Internet«). <http://www.cati.si/papers/zbymm0003.html>. (May 23, 2000).

Beniger, James R. 1986. *The Control Revolution*. Cambridge, Massachusetts and London: Harvard University Press.

Bicknell, Craig. »Online Prices Not Created Equal«. 2000. Wired News. <http://www.wired.com/news/print/0,1294,38622,00.html>. (August 17, 2002).

Black, Edwin. 2002. *IBM and the Holocaust*. London: Time Warner Paperbacks.

Bogataj, Jože. 2002. *Poročilo o delu Inšpektorata za varstvo osebnih podatkov v letu 2001 (A report on the work of the Inspectorate for Personal Data Protection in 2001)*. Ljubljana: Ministrstvo za pravosodje Republike Slovenije (Ministry of Justice).

Boyle, James. 1997. *Foucault In Cyberspace: Surveillance, Sovereignity, and Hard-Wired Censors*. <http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm>. (January 19, 1998).

Raab, Charles D. 1997. »Privacy, democracy, information«. In *The Governance of Cyberspace,* Loader, Brian D., 155–174. London, New York: Routledge.

The Center for Democracy and Techology. <http://www.cdt.org/>. (January 19, 1998).

Chaum, David. 1996. »Achieving Electronic Privacy«. In *High Noon on the Electronic Frontier*, Ludlow, Peter. 1996. Cambridge, London: The MIT Press.

Clarke, Roger A. 1988. »Information Technology and Dataveillance«. V *Communications of the ACM*. 498–512. <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

Compass. 1998. Government of Ontario. <http://www.mto.gov.on.ca/english/traveller/compass/>. (December 20, 1998).

Cooley, Charles Horton. 1993. *Social Organization: A Study Of The Larger Mind; introduction by Philip Rieff*. New Brunswick and London: Transaction Publishers.

Council Resolution of 17. January 1995 on the Lawful Interception of Telecommunications. 1996. Brussels: Official Journal, C 329. 1–6.

Cult of the Dead Cow.1998. <http://www.cultdeadcow.com>. (May 23, 2000).

Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in Sloveniji (The Protection of Information Privacy in Europe and Slovenia)*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.

Data Protection Working Party. 2000 (21. november). *Privacy on the Internet – An Integrated EU Approach to On-line Data Protection*. <http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_2k.htm>.

Denning, Dorothy E. 1996. »The Clipper Chip Will Block Crime«. In Ludlow, Peter. *High Noon On the Electronic Frontier*. 215–216. Cambridge, London: The MIT Press.

——. 1997. »The Future of Cryptography«. In Loader, Brian D. *The Governance of Cyberspace*. 1997. 175–190. London, New York: Routledge.

Denning, Dorothy E. and Baugh, William E. 1999. »Hiding Crimes in Cyberspace«. I*nformation, Communication & Society*, (2) 3. 251–276.

DoubleClick. 2002. »Doubleclick ad serving data shows rich media click-through rates to be six times higher than standard ads«. <http://www.doubleclick.com>. (October 26, 2002).

Dunnett, Jim. 1998. »Secret Phone-Tap Plan«. DejaNews. <http://www.dejanews.com/getdoc.xp?AN=419710899>. (February 2, 1999).

Dupuis, Clement. 1999. *A Short History Of Crypto*. <http://webhome.idirect.com/jproc/crypto/crypto_hist.html>. (July 25, 2002).

E-mail directory of Najdi.si search engine. 2000. Noviforum. <http://www.najdi.si>. (October 1, 2002).

EPIC. 1998a. *Crptography Policy*. <http://epic.org/crypto/>. (January 19, 1998).

———. 1998b. *Efforts to Ban Encryption*. <http://www.epic.org/crypto/ban/>. (January 19, 1998).

———. 1998c. *Key Escrow*. <http://www.epic.org/crypto/key_escrow/>. (January 19, 1998).

———. 1998d. *The Clipper Chip*. <http://www.epic.org/crypto/clipper/>. (January 19, 1998).

———. 2002. *Face Recognition*. <http://www.epic.org/privacy/facerecognition/>. (August 9, 2002).

»FBI 'Fesses Up to Net Spy App. 2000«. Wired News. <http://www.wired.com/news/print/0,1294,49102,00.html>. (December 12, 2000).

Felten, Edward W. and Schneider, Michael A. 2000. »Timing Attacks on Web Privacy«. Proc. of 7th ACM Conference on Computer and Communications Security. <http://www.cs.princeton.edu/sip/pub/webtiming.pdf>. (December 1, 2001).

Foucault, Michel. 1984. *Nadzorovanje in kaznovanje (Discipline and Punish)*. Ljubljana: Delavska enotnost.

Gantar, Pavel. 1993. *Sociološka kritika teorij planiranja (A Sociological Critique of the Theories of Planning)*. Ljubljana: Znanstvena knjižnica FDV.

Glasner, Joanna. 2002. »DoubleClick to Open Cookie Jar«. Wired News. <http://www.wired.com/news/print/0,1294,54769,00.html>. (August 27, 2002).

Gutmann, Peter. 1996. »Secure Deletion of Data from Magnetic and Solid-State Memory«. USENIX Security Symposium Proceedings. <http://www.safedelete.com/a-gutmann.phtml>. (december 1. 2001).

Harrison, Ann. 2001. »Terror attacks revive crypto debate«. Security Focus. <http://www.securityfocus.com/news/256>. (September 19, 2001).

Hastings Communications and Entertainment Law Journal (*Comm/Ent*). 1998. 19 (3). San Francisco: Hastings College of the Law.

How to Obscure any URL. <http://www.pc-help.org/obscure.htm>. (January 13, 2002).

»Internet Watchdog Warns of Fake eBay Web Site«. 2002. Yahoo News. <http://story.news.yahoo.com/news?tmpl=story2&cid=575&ncid=738&e=6&u=/nm/20021211/wr_nm/crime_ebay_email_dc>. (December 11, 2002).

Imenik elektronske pošte Slovenije (A Directory of e-mail addresses in Slovenia). 1998. Telekom Slovenije. <http://afna.telekom.si>. (October 7, 1998).

Improving Your Network Security Using SATAN. 2000. <http://www.cs.umbc.edu/~woodcock/cmsc482/proj1/satan.html>. (May 23, 2000).

Information service of Agence Europe. 1999. Brussels. <http://www.agenceurope.com/>. (February 3, 1999).

Information, Communication & Society. 1999. 2 (3). London: Sage Publications.

Interaktivni naravovarstveni atlas (Interactive atlas of environmental protection). 2002. Agencija RS za okolje.<http://212.103.140.243/nvatlas/>. (December 1, 2002).

International Working Group on Data Protection in Telecommunications. 1998. *Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the WorldWideWeb*. <http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm>.

Joel, Deane. »Melissa manhunt creates precedent«. 1999. ZDNet News. <http://www.zdnet.com/zdnn/stories/news/0,4586,2237838,00.html>. (April 7, 1999)

Kids Surf Day. 1997. <http://www.ftc.gov/opa/9712/kids.htm>. (January 19, 1998).

Kocher, C. Paul, Jaffe, Joshua and Jun, Benjamin. 1999. »Differential Power Analysis«. Conference Crypto '99, August 15–19, 1999. University of California, Santa Barbara. <http://www.cryptography.com/resources/whitepapers/DPA.pdf>. (December 1, 2001).

Kocher, C. Paul. 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Advances in Cryptology – CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 1996, Proceedings. In Koblitz, Neal. ed., *Lecture Notes in Computer Science*. Vol. 1109, Springer. <http//www.cryptography.com/resources/whitepapers/TimingAttacks.pdf>.

Klemenčič, Goran et al. 2001. *Internet in pravo (The Internet and Legal Issues)*. Ljubljana: Pasadena.

Kooiman, Jan. 1993. *Modern Governance – New Government-Society Interactions*. London: Sage publications.

Koops, Bert-Jaap. 1997. *Crypo Law Survey*. <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>. (January 19, 1998).

Kuhn, Markus G. and Anderson, Ross J. 1998. »Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations«. In Aucsmith, David. ed., *Information Hiding, Second International Workshop*. 124–142. IH'98, Portland, Oregon, USA, April 15–17, 1998, Proceedings, LNCS 1525, Springer Verlag. <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>.

Kušej, Gorazd, Pavčnik, Marijan and Perenič, Anton. 1992. *Uvod v pravoznanstvo (An Introduction to the Science of Law)*. Ljubljana: ČZ Uradni list RS.

Labriola, Don. 2002. »Is Media Player Spyware?«. Ziff Davis Media Inc. <http://www.extremetech.com/article2/0,3973,9615,00.asp>. (December 20, 2002).

Lemos, Rob. 1999. »How GUID tracking technology works«. ZDNet News. <http://www.zdnet.com/zdnn/stories/news/0,4586,2234550,00.html>. (March 30, 1999).

Leskovšek, Tomaž. 2001. »Poznavanje lokacije uporabnika – Locating mobile users«. In *Razkrij svojo digitalno substanco: zbornik predavanj: telekomunikacije OI telecommunications mednarodna konferenca: človeku prijazna / tehnološko popolna / informacijska družba, Nova Gorica, 19.–21. september 2001,* 18–22. Ljubljana: Inštitut za telekomunikacije.

Loader, Brian D. 1997. *The Governance of Cyberspace*. London, New York: Routledge.

Loney, Matt. 2002. »Want Wi-Fi? Learn the secret code«. CNET News.com. <http://news.com.com/2102-1033-939546.html>. (June 26, 2002).

Ludlow, Peter. 1996. *High Noon On the Electronic Frontier*. The MIT Press: Cambridge, London.

Lyon, David. 1994. *The Electronic Eye*. Cambridge: Polity Press.

Macavinta, Courtney. 1999. »RealNetworks faced with second privacy suit«. CNET News.com, <http://news.com.com/2102-1001-232766.html>. (August 17, 2002).

Manjoo, Farhad. 2001. »Making It Harder for Hijackers«. Wire News. <http://www.wired.com/news/print/0,1294,46782,00.html>. (September 13, 2001).

McCullagh, Declan. »FBI Hacks Alleged Mobster«. 2000. Wired News. <http://www.wirednews.com/news/print/0,1294,40541,00.html>. (December 6, 2000).

———. 2001a. »Anti-Attack Feds Push Carnivore«. Wired News. <http://www.wired.com/news/print/0,1294,46747,00.html.>. (September 12, 2001).

———. »Senate OKs FBI Net Spying«. 2001b. Wired News. <http://www.wired.com/news/print/0,1294,46852,00.html>. (September 14, 2001).

———. »Bush Bill Rewrites Spy Laws«. 2001c. Wired News. <http://www.wired.com/news/print/0,1294,46953,00.html>. (September 19, 2001).

———. »Wiretap Bill Gets Third Degree«. 2001d. Wired News. <http://www.wired.com/news/print/0,1294,47111,00.html>. (September 26, 2001).

McKay, Nial. 1998. »Europe Is Listening«. WiredNews. <http://www.wired.com/news/news/politics/story/16588.html>. (March 23, 2000).

Mesenbrink, John. 2002. »Biometrics Plays Big Role with Airport Security«. Security Magazine. <http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,69728,00.html>. (December 20, 2002).

Mlinar, Zdravko. 1994. *Individuacija in globalizacija v prostoru (Individualization and Globalization)*. Ljubljana: SAZU.

Močnik, Rastko. 1985. *Beseda ... besedo*. Ljubljana: ŠKUC.

More About the Privacy Rights Clearinghouse. 1998. <http://www.privacyrights.org/fs/services.html>. (January 19, 1998).

Morehead, Nicholas. 2000. »Toysmart: Bankruptcy Litmus Test«. Wired News, <http://www.wired.com/news/business/0,1367,37517,00.html>. (December 20, 2000)

Možina, Damjan. 2002. »Se Evropa odreka zasebnosti v korist varnosti?« (»Has Europe been relinquishing privacy for the sake of security?«). *Informatika in pravo (Information Technology and Legal Issues)*, (1): 3-5, a supplement to the *Legal Practice*, No 43. Ljubljana : Gospodarski vestnik.

Oakes, Chris. »Monitor This, Echelon«. 1999. Wired News. <http://www.wired.com/news/politics/0,1283,32039,00.html>. (October 22, 1999)

»The Phil Zimmerman Case«. InfoNation <http://www.info-nation.com/philzima.html>. (January 19, 1998).

Poulsen, Kevin. 2000. »Ex-CIA Chief: Beware Spy-Viruses«. Security Focus on-line. <http://online.securityfocus.com/news/38>. (December 20, 2000).

Privacy in Cyberspace. 1998. <http://www.privacyrights.org/fs/fs18-cyb.html>. (January 19, 1998).

Raab, Charles D. 1993. »The Governance of Data Protection«. In *Modern Governance – New Government-Society Interactions,* Kooiman, Jan, 89–103. London: Sage publications.

Ross, Edward Alsworth. 1922. *Social Control: a survey of the foundations of order*. New York, London: The Macmillan Company.

RSA Laboratories. 2000. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*. RSA Security Inc. <http://www.rsasecurity.com/rsalabs/faq/index.html>.

Sandberg, Jared. 2001 (4. februar). »Hackers poised to land at wireless AirPort«. The Wall Street Journal Online. <http://zdnet.com.com/2100-11-527906.html?legacy=zdnn>. (December 20, 2002).

Schneier, Bruce. 1999. »European Cellular Encryption Algorithms«. Crypto-Gram. <http://www.counterpane.com/crypto-gram-9912.html>. (December 15, 1999).

———.2000. »Cookies«. Crypto-Gram. Counterpane Internet Security, Inc. <http://www.counterpane.com/crypto-gram-0002.html>. (February 15, 2000).

———. 2001a. »PGP broken«. Crypto-Gram. <http://www.counterpane.com/crypto-gram-0101.html>. (January 15, 2001).

———. 2001b. »802.11 Security«. Crypto-Gram. Counterpane Internet Security, Inc. <http://www.counterpane.com/crypto-gram-0103.html>. (March 15, 2001).

Shireen, Herbert J. 1998. *A Brief History of Cryptography*. Cybercrimes. <http://cybercrimes.net/Cryptography/Articles/Hebert.html>. (July 25, 2002).

Srivastava, Anita. »Dynamic Pricing Models – Opportunity for Action«. 2001. Center for Business Innovation. <http://www.cbi. cgey.com/pub/bi-news/pdf/dynamic_pricing_models_with_ cover.pdf>

»Standard Feature of Web Browser Design Leaves Opening for Privacy Attacks«. 2000. Science Daily. <http://www.sciencedaily.com/releases/2000/12/001208074325.htm>. (December 20, 2000).

Statewatch Organisation (Monitoring the State and Civil Liberties in the European Union). 1999. <http://www.statewatch.org/>. (February 5, 1999).

A Statewatch Report. 1999. <http://www.freenix.fr/netizen/swreport.html>. (Februar 2, 1999).

STOA. 1998. An Appraisal of the Technologies of Political Control (Summary of Interim Study). <http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm>. (February 2, 1999).

StopCarnivore.org. 2000. <http://www.stopcarnivore.org>. (December 20, 2000).

StreetBeam. 2002. <http://www.streetbeam.com>. (October 17, 2002).

Stubblefield et al. 2001. »Using the Fluhrer, Mantin and Shamir Attack to break WEP«. AT&T Labs, <http://www.cs.rice.edu/~astubble/wep_attack.pdf>.

Šturm, Lovro ur. 2002. *Komentar Ustave Republike Slovenije (Comments about the Constitution of the Republic of Slovenia)*. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

Temporary Committee on the ECHELON Interception System. 2001. Working document in preparation for a report on the existence of a global system for intercepting private and commercial communications (ECHELON interception system). European Parliament. <http://www.fas.org/irp/program/process/europarl_draft.pdf>

Terraserver. 2001. Microsoft Corporation. <http://terraserver.microsoft.com/>. (December 1, 2001).

Towards a European Framework for Digital Signatures and Encryption. <http://www.ispo.cec.be/eif/policy/97503toc.html>. (January 19, 1998).

Van Eck, Wim. 1985. »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?«. Computers & Security. 296–286. <http://jya.com/emr.pdf>.

Vidmar, Tone. 1997. *Računalniška omrežja in storitve (Computer Networks and Services)*. Ljubljana: Atlantis.

Watson, Rory. 1999. »Unija ukrepa proti nevarnosti kriminala« (»The Union Takes Measures Against the Threats of Crime«). V *Evropski dialog: revija za evropsko integracijo* [Slovenska izd.] (*European*

Dialogue: a magazine for European integration [Slovene edition]). 1999. (January–February). Brussels: European Commission, General Directorate for Information.

Webster, Frank. 1995. *Theories of the Information Society*. London: Routledge.

What SATAN Is. 2000. <http://www.cs.ruu.nl/cert-uu/satan.html>. (April 30, 2000).

Wireless LAN Security. 2002. An ISS Technical White Paper. Internet Security Systems. <http://documents.iss.net/whitepapers/ wireless_ LAN_security.pdf>.

»The Zimmerman Case«. 1995. The Ethical Spectacle. <http://www.spectacle.org/795/zimm.html>. (January 19, 1998).

Zimmerman, Phil. 1993. *Testimony of Philip R. Zimmerman to the Subcommittee on Science, Technology, and Space of the US Senate Committe on Commerce, Science, and Transportation*. <http://www.pgp.com/phil/phil-quotes.cgi>. (January 19, 1998).

Zimmerman, Phill. 1994. PGP™ User's Guide. In the file PGP-DOC1.TXT supplied with PGP software version 2.6.2.

The list of Slovene legislation referred to in this study. All Acts including amendments are available on-line (in Slovene only)

- *The Penal Code*
- *The Convention on the Protection of Individuals with Regard to the Automatic Processing of Personal Data*
- *The Constitution of the Republic of Slovenia (English version available on-line)*
- *The Criminal Proceedings Act*
- *The Postal Services Act*
- *The Slovene Intelligence and Security Agency Act*
- *The Telecommunications Act*
- *The Protection of Personal Data Act*
- a proposal for the *Book of Rules* regarding the equipment and interfaces for the lawful interception of communications (prepared by the Ministry of Information Society and submitted for public debate on December 20th, 2002)

GLOSSARY

Algorithmic surveillance: data analysis using complex algorithms and enabling automatic identification and monitoring.

Back door: an entry point used by an attacker to execute remote control over a computer via the Internet.

Biometry: a process of collection, processing and storage of data about the physical characteristics of individuals for the purpose of their identification.

Browser's cache, web caching: a cache memory of the Internet browser storing frequently accessed static information on the web page, e.g. images. Exploited in *timing attack* technique.

Browser's chattering: exchange of information about the user between an Internet browser and a web server.

Brute force attack: in computer contexts this term is used to denote a method of breaking password relying on the testing of all possible combinations of passwords. It requires a lot of processing time and is relatively inefficient.

Carnivore: an application used by the US state agencies to intercept Internet traffic. The official name of the system is DCS1000. The system has been in use in the US since 2000.

CCTV (Closed Circuit Television): surveillance cameras.

Cleartext, plaintext: unencrypted message.

Cryptoanarchy: a term related to the wide use of public encryption keys. Some authors believe that eavesdropping and control of information will become impossible because of the use of this technology.

Cryptogram, cyphertext: encrypted text.

Cryptology: the science of secrecy, encryption and decryption of encrypted data (cryptanalysis). *Symetric cryptography:* one and the same key is used to encrypt and decrypt messages. *Asymetric cryptography:* a key used to encrypt data is different from the one used to decrypt it.

Cookies: small data packages sent by a web server to an Internet browser and stored on the local computer. These data can be retrieved by the web server. *Session cookies* expire once the session is concluded, i.e. when the user exits the browser. *Persistent cookies* last longer, even for years. *The first-party cookies* are cookies sent by a web page that is visited, while the *third-party cookies* are sent by other web pages hosted by the visited web page, usually owned by advertising agencies.

Cult of the Dead Cow: a group of hackers who in 1998 published a Trojan horse named Back Orifice, an application used to take control over a remote computer.

Data mining: an array of statistical and mathematical methods used in the analysis of huge databases and search for patterns within these.

Dataveillance: surveillance based on dispersed data collection; these data can be collated.

Spider, worm, harvester: a software application for data collection on the Internet; often used to collect electronic addresses.

DES (Data Encription Standard): one of the most widely used coding algorithms in civil spheres, used mainly in banking; the shortcut that could lead to the breaking of this algorithm is known to the US military.

Dictionary attack: searching for passwords through the elements prepared in advance, usualy the words frequently used in a given language.

Differential Power Analysis: one among *tempest techniques*, used to break encryption keys.

Distributed data processing: a processing of data by many computers connected via the Internet in which each computer processes one part of information. The aggregate processor capacity is thus increased enormously.

DNS (Domain Name System): a system that converts domain names into corresponding IP addresses. Developed in 1983 at the University of Wisconsin.

Dossier society: a society which keeps record of every individual.

ECHELON: a system originally designed to intercept communications from the former Soviet Union, China and other communist countries; now used for the interception of civil communications.

Electronic trace: routinely stored information pointing to the activities of some individual or a trace left behind by an individual in virtual space.

Encryption key: the value of the parameter in an encryption algorithm used to convert plaintext into cyphertext. In asymmetric cryptography two types of keys are in use: *private key* and *public key*.

Environment variables: data about the local environment of an Internet user sent to web page administrators (e.g. type of the browser used, operating system etc.)

Face-recognition system: a biometric methods used in the USA to track down criminals and missing persons.

Factoring: a mathematical procedure which searches for prime number factors of the given key. This procedure can be used to break private encryption keys.

Fingerprint of a string: a unique number of a fixed length calculated from a character string of an arbitrary length. Used with *digital signatures*.

Firewall: an interface between the local user and the network designed to prevent unauthorized access to or from a local network.

GIS databases: Geographical information system database. Can be linked to other databases and satellite images.

GUID (Global Unique Identifier): an identification number inserted into all Microsoft Word 97 documents enabling identification of the author.

Hollerith machine: a device for data processing invented by Herman Hollerith towards the end of the 19th century; first used in 1890 census in the US.

ICMP (Internet Control Message Protocol): a protocol for the exchange of control messages on the Internet.

IP address: computer's virtual address in the network. An IP address is either fixed or dynamic.

Java: object-oriented programming language by Sun Microsystems widely used and thus suitable for Internet applications.

JavaScript: a programming language by Netscape used on the Internet.

Keyboard-sniffing program: a program which intercepts keyboard input; mainly used to steal passwords. *Magic Lantern:* a special tool for keyboard sniffing, developed and used by the FBI.

Live update: automatic update of software applications and antivirus samples.

Log file: a journal file for the storage of data about the activities of the user.

Magnetic force microscopy: a method based on the exploitation of thermal contraction and expansion enabling the reconstruction of overwritten data using electronic microscope.

NAT (Network Address Translation): an interface enabling several users to access the Internet using one IP address. Sometimes referred to as *masquerade*.

Non-recoverable erasure of data: a special method for permanent erasure of data so that they are not recoverable even using the method of magnetic force microscopy. The method was developed by Peter Gutmann and it requires 35 passes using a special procedure.

One-time password: a password that can be used to access a system only once.

Packet sniffing: this technique is used to monitor and analyze traffic on other computers. Packet sniffing used to be very popular with Ethernet networks (promisc sniffing), since initially each computer located in a specific segment of an Ethernet network could control traffic on all other computers in the same network segment. However, this technique is not imperceptible. Today, data interception is effected mainly by monitoring the router traffic.

Panoptic effect: an effect of asymmetrical or hierarchic surveillance which produces uncertainty leading to voluntary subjection of individuals.

Panopticon: a prison plan presented to the British government in 1791 by Jeremy Bentham. The plan had never been realized. Foucault used Bentham's idea to develop his theory of the Panopticon, a political technology based on sublime coercion and enabling the maintenance of power.

Password sniffing: interception of packages containing user names and passwords.

Personalized link: user-specific link to a specific web page; often linked to an e-mail address and used to monitor user's response.

Plain text: unencrypted text; this format is used in electronic messages.

PGP (Pretty Good Privacy): a program written by Phil Zimmerman in 1991; intended for the encryption of messages on personal computers.

Portal: an Internet entry point containing links to other pages and other useful information.

Privacy statement: a statement published on the web page by a web page owner usually stating what data are collected and for what purpose.

Profiling: a methods used to categorize individuals on the basis of their characteristics.

Proxy: an interface between the local computer and the Internet which sends requests for access to Internet pages on behalf of the local user and forwards information received from a web page to the local user. *An anonymous proxy* is a type of this interface that does not store data about the local users and thus enables anonymous browsing. Roughly, two kinds of proxies are in use: *stand-alone anonymous proxy* and *web-based anonymous proxy*.

Relay server: a server forwarding electronic messages on their route from the sender to the recipient. The EU legislation specifies that relay servers must delete messages as soon as these are forwarded.

Remote wiretapping port: a port enabling wiretapping within the telecommunication network.

Responsegraphic: a graphic representation of statistical response e.g. of consumers to advertisements..

RSA: an asymmetric encryption algorithm developed in 1997 by Rivest, Shamir and Adleman. It is one of the most popular encryption algorithms; implemented in PGP.

SATAN (Security Administrator's Tool for Analyzing Networks): one of the first freeware programs used to detect security holes in a computer system either via the Internet or local network.

Satellite surveillance: surveillance based on satellite images used for military and civilian purposes.

Spam Assassin: a software application that intercepts spam (unsolicited) mail. The program accords certain number of points to each message, with the higher number of points denoting higher probability that the message is spam. Identification criteria are user definable.

Spyware, E. T. application: programs intended for the collection of data about a user; mainly used for collecting marketing information.

SSL (Secure Sockets Layer): a protocol enabling encrypted connection between the client and the server; used in electronic banking or on-line shops.

Steganography: a technique of message hiding (e.g. within graphic, audio or text files). Steganography can be used to implement a *digital watermark* or *digital serial numbers*.

Surveillance revolution: exploitation of surveillance made possible by the 20th century technologies; often compared to the industrial revolution of the 19th century.

Surveillance society: a society which has maximized surveillance of individuals; the term was proposed by Webster.

Swap file: a swap file is a temporary memory file stored on the disk which can be retrieved later. By wiping this file it is possible to prevent the retrieval of data when the computer is switched on again.

Tempest prevention font: special fonts used to prevent an attacker to reconstruct a sufficiently clear picture of the screen using *tempest attack*.

Timing Attack: one among the *tempest techniques*, used to break encryption keys based on the measuring of time needed to process data.

To wiretap friendly: a term denoting wiretapping capabilities of modern telephone exchange systems enabling simple wiretapping.

Trojan horse: a malicious application usually pretending to be an ordinary program while using hidden functions to invade the system. In contrast to viruses, it does not reproduce on its own.

Vehicle Recognition System: identification of vehicles on the basis of surveillance camera footage.

Virus: any program or code designed to cause harm or overtax a computer system and reproducing on its own. Two types of viruses are in use: destructive and instructive.

»*Warchalking*«*:* a system of signs used by network invaders to mark spots from where one can access wireless networks.

Wiping of files: a method of file removal preventing later retrieval of the data. Wiped data cannot be retrieved as these are usually overwritten with new data.

Web bug: an image usually 1 x 1 pixel in size used for tracing the users on the Internet.

WEP (Wired Equivalent Privacy): an encryption algorithm used in wireless networks.

Wireless LAN network: wireless local networks usually based on 802.11.b protocol.