Monitoring, Supervision and Information Technology

Proceedings of the first international seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology

15 June 2006

Editors:
P. Kleve
R.V. De Mulder
C. van Noortwijk

LEFIS
LEGAL FRAMEWORK FOR THE INFORMATION SOCIETY

Centre for Computers and Law

OMV
Onderzoekschool Maatschappelijke Veiligheid

Monitoring, Supervision and Information Technology

Monitoring, Supervision and Information Technology

Proceedings of the first international seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology

15 June 2006

Erasmus University Rotterdam
The Netherlands

Editors:
P. Kleve
R.V. De Mulder
C. van Noortwijk

2006

Legal Framework for the Information Society (LEFIS)

Research School for Safety and Security (OMV), Erasmus University Rotterdam

Centre for Computers and Law, Erasmus University Rotterdam

ISBN 905677316X

Table of Contents

Introduction 1
P. Kleve, R.V. De Mulder & C. van Noortwijk

Part 1 – Concerns

Monitoring Electronic Communications: Privacy Issues 5
R. Petrauskas & D. Stitilis

Monitoring and Supervising Children on the Internet: 21
Rethinking the Parental Responsibility
S.A. Shukor

R(87)15. A Slow Death? 27
J. Cannataci, M. Caruana & J.P. Mifsud Bonnici

Part 2 – Tools

Plagiarism and Fraud in Education: 53
The Importance of Monitoring and Supervision
C. van Noortwijk & R.V. De Mulder

Safe and Trustworthy Access in a Working Environment: 65
the MoodlePKI Project
L. Catalinas, F. Galindo & P. Lasala

Ambient Intelligence – Monitoring and Supervision 81
in New Environments
P. Mikulecky

Part 3 – Theory

Monitoring and Supervision in the Economic Analysis 97
of Safety and Security
L.T. Visscher

Surveillance Technology, Constitutional Rights 119
and the 'Monitoring Power'
R.V. De Mulder & P. Kleve

Conclusion 129
P. Kleve, R.V. De Mulder & C. van Noortwijk

Introduction

P. Kleve, R.V. De Mulder & C. van Noortwijk

Information technology has changed society significantly in a remarkably short time. Communication has never been as rapid and as simple as it is today. Nor has so much information been so readily available. While these technological advances have introduced new possibilities, they have also engendered new social issues. These concerns are not confined to one area of social activity, but affect our lives across a wide spectrum. Are our constitutional rights infringed by the use of new technology to monitor our activities? Are we in danger of loosing our right to keep our private lives private? Has increased globalisation stimulated terrorism? Do the possibilities offered by the Internet to download the work of others pose a threat to the integrity of educational diplomas? Are our children at risk from the Internet?

Having recognised these concerns, a solution is not always easy. While monitoring and supervision may alleviate certain problems, they may in themselves create new problems. Nor is it always obvious who should be responsible for monitoring and supervision: should this be imposed from above by governmental agencies or should the self-regulation and privatisation of safety and security be stimulated?

In 2006, the Centre for Computers and Law of the Erasmus University Rotterdam, the Netherlands, hosted a Workshop on the subject of Monitoring and Supervision. The Workshop was organised in close cooperation with LEFIS, the Legal Framework for the Information Society, and with the Dutch Research School for Safety and Security in Society.

This report contains a selection of papers presented during this workshop and concludes with a number of observations by the editors. The scope of the Workshop was very broad. The subjects that were presented can be divided in the following three general categories:

- concerns about the practical and legal consequences of information technology;
- the tools that can be used to monitor and supervise the application of information technology;
- the theoretical analysis of the problems arising from the use of information technology: how worrying are these developments and how effective are the methods that have been proposed to deal with the adverse effects of information technology? Furthermore, there is a problem that existed long before the present information age: ‘Quis custodiet ipsos custodes’(who should monitor the monitors)?

The papers that have been collected in this compilation encompass a variety of subjects that are relevant to today's information society. Subjects range from privacy issues, protection of children when using the Internet, freedom of speech, fraudulent use of the Internet in an educational setting, the cost of legal monitoring and supervision and the need for a monitoring authority to take its place in the balance of power.

The members of the Program Committee:
Prof. Fernando Galindo
Prof. Richard De Mulder
Dr. Pieter Kleve
Dr. Cees van Noortwijk

Part 1 – Concerns

Monitoring Electronic Communications: Privacy Issues

Rimantas Petrauskas, Darius Stitilis
Mykolas Romeris University

Keywords: *private life, electronic communications, control of electronic communications for criminal investigation purposes*

Abstract

The main purpose of this paper is to analyse legal problems related to the restriction of private life in electronic communications for law enforcement purposes. The present work deals with certain problems relating to legal regulation in the field of the control of electronic communications both according to the Law on Operative Activities and the Criminal Procedure Law.

The first part of the present work is devoted to the studies of legal problems related to the control of traffic data which are retained by electronic communication operators and services. The main problem is the lack of secondary legislation regulating the control of private life for criminal investigation purposes. A proposal for a Directive on the retention of communications traffic data that would provide for a possibility to retain Internet data for up to six months, and phone data for one year as well as to compensate ISPs and telcos for their compliance costs may also have a significant importance to the procedures of control of the Lithuanian electronic communications. The proposed Directive would not be applicable within the scope of the contents of communications as such.

In the second part of the paper, the study focuses on the legal aspects of the real-time collection of contents and traffic data. The line between the traffic data (who is called, when, and how long the call lasts) and communication data (contents of the telephone call) stems from the traditional telephone infrastructure. Adapting this situation to the Internet environment is quite a different task, if at all possible. Is a communication to be considered the contents of packages? Is the traffic data to be treated as just packets headers? Or is the traffic data to be regarded as clickstreams or http-requests? A possible step forward would be to define the notion of a communication. Part 2.1 deals with the control of electronic communications during operational activities. In addition, part 2.2 deals with the control of electronic communications in the course of criminal procedure.
In the third part, the need for a special institution is discussed. Currently, the State Security Department is the authorised institution in charge of black boxes. However, this Department performs operational activities and controls of

electronic communications on its own too. Another form of the supervision of the control of electronic communications for criminal investigation purposes is the Parliamentary control which, in Lithuania, is weak and should therefore be strengthened.

1. Introduction

The right to private life is not absolute. Article 8, part 2 of the Convention on the Protection of Human Rights and Fundamental Freedoms provides cases when this right may be restricted under certain conditions. It should be noted that the restriction of the right to the inviolability of private life should be based on certain principles. This is where the case-law of the European Court of Human Rights is very important. The following key conditions for the restriction of human rights have been formulated by the European Court of Human Rights in the cases Amann vs. Switzerland, Armstrong vs. UK, Khan vs. UK and others:[1]

1) legitimacy clause to the effect that restrictions may only be imposed by a publicly declared and explicitly formulated law;
2) necessity clause to the effect that restrictions may only be imposed where these are necessary for the democratic society.

The restriction of the right to privacy in electronic communications[2] should be based on the previously mentioned principles and clauses. The control of electronic communications (in a broad sense) which is performed for operational and other criminal investigation purposes can be divided into two groups:

1) past traffic data control, i.e. collection of information about past electronic communication events (traffic data) from of electronic communications service;[3]

[1] Case-law of the Court is available at the internet address http://www.echr.coe.int.
[2] This restriction can also be referred to as the control of electronic communications.
[3] In the preamble of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) it is mentioned that "Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection". According to these definitions, we may state that, in the sense of traditional telephony, any information about time, duration of connection, telephone number of the calling party etc. is to be considered as the traffic data, and, in the case of electronic mail, the following information may be regarded as the traffic data: sender's IP address and electronic mailbox address, size of electronic message, name of electronic message, size and type of the electronic mail attachments etc.

2) real-time collection of contents and traffic data, i.e. control of electronic communication traffic data and other information via electronic communications by competent enforcement institutions.

2. Past traffic data control

Article 77, part 1 of the Law on Electronic Communications of the Republic of Lithuania provides that „any legal entity providing electronic communications networks and/or services, shall submit all available information to competent institutions: governing institutions of bodies performing operational activities, as well as pre-trial investigation institutions, prosecutor, court or judge designated by the Government.“ This notion of information includes information about events related to electronic communication events, i.e. the traffic data.

Provided the information is collected for operational purposes, a court ruling is necessary in accordance to the Law on Operational Activities of the Republic of Lithuania. The Law provides that “bodies performing operational activities may receive specific information on the past traffic data necessary for operational investigation purposes from telecommunication operators and providers of telecommunication services subject to a reasoned ruling of a district court‘s judge on the basis of a reasoned motion by the director or an authorised deputy director of the body performing operational activities”.[4] Article 10, part 13 of the Law states that “a notification shall be lodged with operators of telecommunication services or providers of telecommunication services where the number of motion, date of the court ruling and name of the court that issued the ruling shall be specified”. According to present Law, the responsibility for the coincidence of the contents of the notification and court decision shall be assumed by the officer providing this information.

It is important to note the practice of other countries in the sphere of requirements for control of past traffic data. The analysis of specific acts showed that a general rule is in force in the USA (Electronic Communications Privacy Act) whereby the control of past traffic data is possible only subject to the submission of a court sanction[5]. Furthermore, past traffic data can also be controlled subject to a specific certification issued by competent bodies specified in the Act where terms and conditions have been set.[6] The Federal Wiretapping Act provides similar rules, too, in which it is stated that the

[4] Law on Operational Activities of the Republic of Lithuania VŽ, 2002, No. 65-2633; art. 10

[5] Electronic Communications privacy Act. United States Code. Title 18 – Crimes and Criminal Procedure. Part I - Crimes. Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications http://floridalawfirm.com/privacy.html; 2 (a) (ii) (A).

[6] Electronic Communications privacy Act. United States Code. Title 18 – Crimes and Criminal Procedure. Part I - Crimes. Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications http://floridalawfirm.com/privacy.html; 2 (a) (ii) (B).

principle of the court's permission is applicable with respect to all types of wiretapping of electronic communications. In the USA, a similar procedure has been defined with respect to the real-time collection of content and traffic data, i.e. interception etc., too.

The Criminal Code of Poland, too, states that any control of electronic communications shall be subject to a court sanction on the basis of a motion from the prosecutor.[7] The Ministry of Justice of Poland has issued detailed rules in which the procedure for the interception of electronic communications and use of technical equipment is regulated.

The control of electronic communications (both kinds: traffic data and real-time collection of content and traffic data) in Estonia is regulated by the Surveillance Act.[8] The surveillance of electronic communications can be sanctioned by a reasoned decision of the director of the body in charge of electronic communications surveillance. In cases where the control of electronic communications is essential for the purpose of investigating serious offences, the sanction by a judge of the Tallinn Supreme Administrative Court is necessary.[9] To authors' opinion, such discrepancies in the procedure of the control of electronic communications are unjustified. The procedure of issuing a sanction should not depend on the type of crime as in every specific case the sanction puts a restriction on a certain person's right to private life.

The control of electronic communications in Latvia is possible only subject to a sanction by the court, which is determined in the Criminal Code of Latvia.[10]

The criminal law of Finland regulates the control of electronic communications, too. According to the Criminal Investigation Act, the control of electronic communications is possible only in cases where, for the commitment of a certain crime, a person may be imposed a sentence of imprisonment. Furthermore, the control of electronic communications is possible only subject to the sanction of the court.[11]

[7] Privacy International – Republic of Poland. 2004
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83774.
[8] Surveillance Act of Estonia (February 22, 1994)
http://vlf.juridicum.su.se/master99/library2/teste/Surv.htm.
[9] Privacy International Survey – Republic of Estonia. 2003
http://www.privacyinternational.org/survey/phr2003/countries/estonia.htm.
[10] Privacy International Survey – Republic of Latvia. 2003
http://www.privacyinternational.org/survey/phr2003/countries/latvia.htm.
[11] Privacy international Survey – Finland. 2004
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83553.

In Sweden, the control of electronic communications is possible only subject to the sanction of the court, too.[12] Legislation on the control of electronic communications was revised in 1996 to include all kinds of electronic communications, including internet.

It is very important to take note of the fact, though, that according to the new Criminal Procedure Code of the Republic of Lithuania, which came into force on the 1st of May, 2003, pre-trial investigation officers are no longer expected to receive a reasoned sanction from the court to get any information about past traffic data where this information is required in the pre-trial stage.[13] The only exception is article 155 of the Code which refers to the general rule, that the prosecutor may receive information from a company only subject to the authorisation of a pre-trial investigation judge. This fact leads to a possible conclusion that there is no requirement for other pre-trial investigation officers to lodge a court authorisation when they request information about the past events of electronic communications. The situation referred to above with respect to legislation on the control of information about past traffic data is inconsistent with the constitutional provisions on the protection of private life, and may cause problems in practice. In most cases the pre-trial investigation officers follow the rules of the Criminal Procedure Code of the Republic of Lithuania and, as mentioned above, may request to provide the information without a sanction. On the other hand, the Constitution of the Republic of Lithuania as well as a ruling of the Constitutional Court of the Republic of Lithuania provide for the requirement to receive a reasoned ruling from the court to collect such information. Consequently, monitoring electronic communications should require to file the court ruling before submitting any information about past traffic data as, otherwise, they risk to infringe the right to privacy of life of the persons who are referred to in the information. Moreover, it is essential to ensure that the legal basis for the said procedure is in place and the Criminal Procedure Code of the Republic of Lithuania is amended.

There are some shortcomings in the secondary legislation on the control of electronic communications traffic data, too. Article 77 of the Law on Electronic Communications of the Republic of Lithuania states that "pre-trial investigation bodies designated by the Government shall manage and ensure the collection of information for the benefit of their divisions and/or other pre-trial investigation institutions according to the procedure provided by the Government".[14] Where

[12] Privacy international Survey – Sweden. 2004
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83530.
[13] A new article 198-3 appeared in the 1961's version of the Criminal Procedure Code of the Republic of Lithuania in 2002 which regulates the collection of information from telecommunications operators and providers of telecommunications services. Part 2 of this article notes that information about the control of the past traffic data may be collected only subject to the court ruling.
[14] Law on Electronic Communications of the Republic of Lithuania VŽ, 2004, No. 69-2382; Art. 77, Part. 1.

the control of traffic data restricts the right of a person to private life, a strict procedure should be established. Unfortunately, the above-mentioned procedure has not yet been approved by the Government, which creates conditions for the abuse of the private information received from providers of electronic communication by distributing it to subordinate offices and officials. This situation needs to be rectified by approving the procedure referred to above.

Directive 2006/24/EC of the European Parliament and of the Council of Europe of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks and amending Directive 2002/58/EC[15] will make an important impact for the control of past traffic data for which the providers of electronic communications will be obliged to gather and keep information about traffic data stored for 6 months to 2 years from the moment it has been recorded for the benefit of law enforcement institutions. To this end, the practice shows that, seeking to ensure economic activities, providers of electronic communication services tend to store information about traffic data for as long as a few months; therefore, the requirement to keep information for up to 2 years would mean that the information about private life would be stored for law enforcement purposes for a certain period without the permission of the court. As it has already been mentioned, according to article 22 of the Constitution of the Republic of Lithuania, information about private life can be collected subject to a reasoned decision of the court and only in cases allowed by law. The Constitutional Court of the Republic of Lithuania gave already its opinion regarding this issue. Therefore, such obligation to store information longer than is necessary for economic activities without a reasoned decision of a court can constitute a breach of the right to private life and is, thus, inconsistent with the provisions of article 22 of the Constitution. The fact that the provisions of the Directive with respect to the period of storage of information are inconsistent with international law regulating human rights is already a topic for discussions in jurisprudence;[16] unfortunately, these discussions have only just started. A legislator in Lithuania should estimate the impact of the Directive and its relation with the Constitution of the Republic of Lithuania and be prepared to carry out some actions (including legislative amendments) which would help to avoid the inconsistence between the provisions of the Directive and those of the Constitution of the Republic of Lithuania.

[15] Directive 2006/24/EC of the European Parliament and of the Council of Europe of 15 March 2006 on the retention of data processed and stored-generated or processed in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism and amending Directive 2002/58/EC OJ L 105/54.

[16] The New Data Retention Directive European Media, IP & IT Law Review, 2006 No. 1; P. 49.

3. Real-time collection of contents and traffic data

What are the contents of electronic communications or other information transmitted by electronic communications? Legislation does not define what communication data are. However, jurisprudence describes that a communication is any information which is exchanged by parties as a result of services of public electronic communications. In other words, a communication is to be regarded as the contents of telephone calls or of correspondence by e-mail.[17] Other information transferred by electronic communications includes information on traffic data etc.

It is assumed that procedural requirements for collecting traffic data and communication data should be different[18] since communication data comprise the content of communication and an illegal disclosure of such data may do more harm in comparison to an illegal disclosure of traffic data. Therefore, stricter provisions should be in place as far as sanctions of the control of communication are concerned.[19] It is worth noting though that in traditional telecommunications it is quite easy to distinguish between communications and traffic data; however, other ways of communication may complicate such separation, for example, internet which is referred to as electronic communications. The distinction between communications and traffic data is determined by traditional telecommunication processes where the line between traffic data (who is called, when, and how long the call lasts) and communication data (contents of the call) is quite clear; however, such separation is quite a difficult task in case of internet, if possible at all. It is not clear whether the communication (data) should be described as the whole contents of electronic packages, whether the headlines of electronic packages are to be regarded as the traffic data only, and whether clikstreams and http-requests are to be included in the notion of traffic data.
The request: "http:///searchengine/com/++aids++homosexuality++symptoms" would be considered as traffic data, though in this very case it is related to the contents of communication.[20] Another example relates to dialling DTMF codes during electronic communications. For instance, when a certain telephone banking code is dialled, after connection it is possible to manage services through DTMF codes, whereas DTMF codes have to be dialled after connection, we can assume that this is the contents of electronic communications. On the other hand, the aim of DTMF codes is to initiate certain services/actions;

[17] Maxwell W. Electronic Communications: the New EU Framework. Part I, Booklet 1.5. – New York: Oceana Publications, Inc., 2002; P. 10.
[18] Broadhurst R. Content crimes: criminality and censorship in Asia. Conference on „The Challenge of Cybercrime". 15-17 September, 2004. Palais de l`Europe, Strasbourg, France http://www.coe.int; P. 10.
[19] Maxwell W. Electronic Communications: the New EU Framework. Part I, Booklet 1.5. – New York: Oceana Publications, Inc., 2002; P. 10.
[20] Banisar D. A Commentary on the Council of Europe Cybercrime Convention http://privacy.openflows.org/pdf/coe_analysis.pdf.

therefore, those commands can also have the features of traffic data. The website of the State Data Protection Inspectorate http://www.ada.lt contains information about some telecommunication operators who have declared technical commands to start connections, i.e. traffic data. The previous examples show that it is necessary to focus on a different issue, namely the problem of combining these two categories (communication and traffic data) by calling them communications, or electronic communications. The State Data Protection Inspectorate should take a more active stand on this issue, since one of the most important tasks, which this institution is in charge of according to article 29 of the Law on Data Protection of the Republic of Lithuania, is related to the supervision of the activity of data owners as far as it concerns the administration of personal data.[21]

It is important to mention that the control of real-time information transferred by electronic communications is performed by the supervisory bodies themselves, which is different from collecting information about traffic data from providers of electronic communications services. According to article 77 of the Law on Electronic Communications of the Republic of Lithuania, "upon the presence of a reasoned court ruling, legal entities providing electronic communications networks and/or services shall make it technically possible for bodies performing operational activities in accordance to procedure prescribed in the legislation as well as for pre-trial investigation institutions in accordance to the procedure prescribed by the Criminal Procedure Code of the Republic of Lithuania to control the contents of information transferred by electronic communications channels".[22] It is important to note that providers of electronic communications services are not obliged to ensure the control of any other information transferred by electronic communications.

One may also question the duration of control of information transmitted through electronic communications networks in accordance to the Law of Operational Activities of the Republic of Lithuania. Although the Law provides the procedure of the prolongation of the period subject to availability of a sanction, the maximum period is not set. The implication is that if the sanctioned period is prolonged pursuant this procedure, the private life of a person may be controlled for an indefinite period of time as far as electronic communications are concerned. Such a situation could be regarded inconsistent with the principle of proportionality, as the inviolability of the right to private life is restricted. A positive example in the legislation refers to the Criminal Procedure Code of the Republic of Lithuania where the maximum period for control of information transferred by electronic communications is 9 months.[23] Consequently, it is

[21] Law on Personal Data Protection of the Republic of Lithuania, VŽ, 1996, No. 63-1479; Art. 29, part 2.
[22] Law on Electronic Communications of the Republic of Lithuania VŽ, 2004, No. 69-2382; Art. 77, Part 3.
[23] Criminal Procedure Code of the Republic of Lithuania VŽ, 2002, No. 37-1341; Art. 154, Part 3.

proposed to determine a maximum period for the control of information transferred by electronic communications in the Law on Operational Activities of the Republic of Lithuania.

According to Lithuanian legislation the control of information transferred by electronic communications may be performed in the course of operational investigation or criminal procedure; therefore, these processes have to be addressed separately.

3.1. Control of information transferred by electronic communications in the course of operational activities

Article 10, part 10 of the Law on Operational Activities of the Republic of Lithuania states that: "telecommunications operator or provider of telecommunications services shall make it technically possible to control information transferred by means of electronic communications". While describing the procedure, this part of the article refers to the definition; "use of technical means under special procedure". According to article 3, part 8, "use of technical means under special procedure implies the sanctioned use of technical means in the course of operational activities subject to a reasoned decision of the court with a view of controlling or recording contents of calls, other communications or actions by a person <...>". The part of the definition "or actions" should in fact include the use of technical means for collecting traffic data such as, the traffic data relates to certain actions by users of telecommunications services. According to this definition, the Law on Operational Activities of the Republic of Lithuania provides procedures for real-time collection of computer data both in respect to communication data and traffic data. However, it is worth mentioning that the Law has one shortcoming. The Law gives definitions which were relevant at the time when the Law on Telecommunications of the Republic of Lithuania was valid. However, slightly different definitions are used in the Law of Electronic Communications of the Republic of Lithuania, for example, the term "electronic communications" is used instead of "telecommunications". Therefore, such definitions should be made uniform, which means that it is necessary to revise the Law on Operational Activities of the Republic of Lithuania.

3.2. Control of information transferred by electronic communications in the course of criminal procedure

Pre-trial investigation institutions perform the control of information transferred by electronic communications according to the provisions of the Criminal Procedure Code of the Republic of Lithuania. Unfortunately, the Code does not provide a detailed procedure for such control, except for certain aspects, such as the requirement[24] for the telecommunications operators to provide conditions to listen to contents of telephone calls or control other information transferred by telecommunications networks. Article 154 of the Criminal Procedure Code of the Republic of Lithuania states that "<...> pre-trial investigation officers can listen to contents of telephone calls, control other information transferred by telecommunications networks or make records <...>". Part 4 of the same article says that "telecommunications operators must provide conditions to listen to contents of telephone calls or control other information transferred by telecommunications networks, or make records". Such legal uncertainty may cause a situation where a telecommunications operator will be unaware of the monitoring of information transferred by certain persons via his/her network.

It should be noted that a court ruling is required for the control of information via internet in accordance to article 154 of the Criminal Procedure Code of the Republic of Lithuania, which states that subject to the decision of a judge it shall be possible to control: "... other information transferred by telecommunications networks". Article 154 of the Criminal Procedure Code of the Republic of Lithuania defines the category of information transferred by telecommunications networks; therefore, at first sight there should not be any problems concerning the distinction between communications data and traffic data since the previously mentioned category includes both communication data and traffic data. As mentioned previously, it is difficult to distinguish between these two in the electronic environment, though. However, article 154, part 2 of the Code states that information transferred by telecommunication networks may be controlled and recorded only if it is traffic data. As a result, there might be problems to implement this provision in case of internet communications. On the other hand, this can be explained by the fact that the conditions for control of communications data and traffic data are different.

The Criminal Procedure Code of the Republic of Lithuania provides wider possibilities for the control of information (other than communications data) transferred by electronic communications: The control of such information is possible even in cases "where there is a reason to consider that in such a way it shall be possible to collect information about minor crimes specified in articles

[24] Moreover, the nature of this requirement requires to provide it in the Law on Electronic Communications of the Republic of Lithuania rather than the Criminal Procedure Code of the Republic of Lithuania.

166, 196, 197, 198 (1) as well as parts 1 and 2 of article 309 of the Criminal Code of the Republic of Lithuania".[25] Therefore, the Code implements the principle of different requirements for the monitoring of communication data and of traffic data, respectively, even though, as has already been mentioned, it is difficult to implement this principle in the internet environment.

Moreover, the Criminal Procedure Code of the Republic of Lithuania can be criticised for the definitions used (in case of the Law on Operational Activities); therefore, appropriate amendments (even if only formal) of the Code are welcome.

4. Supervision of the control of information transferred by electronic communications

The Government of the Republic of Lithuania waited for a long time to authorise a specific institution to perform the operational activities involved with the control of information. It was in December 2000 only when a Resolution of the Government[26] resolved that the State Security Department would act as the authorised body. Unfortunately, there is no procedure yet whereby the State Security Department would make it technically possible for every body performing operational activities and, in the course of criminal procedure, for a pre-trial investigation institution to exert independent control over the contents of information transferred by electronic communications. Non-existence of such procedure may result in the misuse of power by the body performing operational activities or pre-trial investigation institution while controlling the communication contents. The court practice of the European Court of Justice as far as it concerns the European Human Rights Convention maintains that the states have to ensure that their legislation would provide guarantees and protection from possible misuse of power in the field of control of the contents of electronic communications. As Lithuania has already ratified this Convention and entered into commitments, it is obliged to ensure the implementation of these provisions in national law.

When the State Security Department received the status of authorised institution, it became obvious that technical commands "to start" or "to finish" the interception or other control of information transferred by electronic communications would be safeguarded in the premises of the Department. This means that in specific cases the same institution would organise both the control of transferred information and storage of the evidence of such control. Supposedly, technical commands to start and to finish the interception or other

[25] Criminal Procedure Code of the Republic of Lithuania VŽ, 2002, No. 37-1341; Art. 154, Part 2.
[26] Resolution No.1593 of the Government of the Republic of Lithuania of 6 December 2004 concerning the provision of authorisations for the implementation of the Law on electronic Communications of the Republic of Lithuania // http://www.lrs.lt.

control of information transferred by electronic communications have to be safeguarded by other than the institution performing operational activities since, in the case where the same institution performs both the operational activities and control over such activities, it is impossible to ensure transparency. Therefore, to guarantee the right to private life of a person, while limiting possibilities to change the information about the control of electronic communications which is being stored, the task of storing such information should be trusted to the Prosecutor General rather than the State Security Department, unless the prosecutor makes sure that a proper control of such storage is ensured.

Another possible form of the control of interception of the contents of electronic communications or other information transferred by electronic communications is the parliamentary control. It should be mentioned that according to the Law on Operational Activities the protection of constitutional rights and freedoms of persons in the course of operational activities is supervised by the Committee of parliamentary control over operational activities.[27] The Committee was established at the end of 2003 as a result of the presidential scandal; however, the statutes of the committee were approved only in 2004.[28] Nevertheless, the question is, if a single parliamentary committee with political powers to exert control over operational activities, is capable of ensuring the protection of the right to private life when it comes to a specific person? Of course, the rights rooted in the statutes of the Committee provide certain preconditions for the control of law enforcement institutions. However, the fact that the members of the committee are all members of Parliament,[29] i.e. politicians, makes it difficult to avoid political decisions. Evidently, the control of this Committee should be coordinated with the control over operational activities performed by a special institution (committee) which is free from political power. In accordance to the present Law of Operational Activities of the Republic of Lithuania, the Parliamentary Committee is entitled to investigate serious infringements of the Law on Operational Activities and cases of misuse of powers by bodies performing operational activities only.[30] A special institution could investigate

[27] Law on Operational Activities of the Republic of Lithuania VŽ, 2002, No. 65-2633; Art. 23, Part 2, Point 1.

[28] Resolution No.IX2022 of the Seimas of the Republic of Lithuania of 12 February 2004 concerning the approval of the Statutes of the Committee of parliamentary control over operational activities // http://www.lrs.lt.

[29] On the 15th of March, 2005 the Parliament of the Republic of Lithuania (the Seimas) adopted Resolution No.X-132 "On forming a committee on operational parlamentary control of the Seimas" whereby, pursuant to article 80-1 of the Statute of the Seimas and article 23, part 1 of the Law on Operational Activities, the Seimas of the Republic of Lithuania resolved to form a parliamentary committtee on parlamentary control of operational activities consisting of 7 members: Vytautas Čepas, Kęstutis Daukšys, Gediminas Jakavonis, Juozas Palionis, Viktoras Rinkevičius, Vidmantas Žiemelis, and Zita Žvikienė.

[30] Law on Operational Activities of the Republic of Lithuania VŽ, 2002, No. 65-2633; Art. 23, Part 2, Point 5.

ordinary complaints about infringements of the right to private life (including the evaluation of legitimacy of fait accompli with respect to the control of electronic communications). This committee should also report periodically about the "surveillance" measures (number of controls of electronic communications, types of crimes for which measures of electronic surveillance were used, duration of the use of electronic surveillance measures (time) etc.).[31] For example, in the USA reports about the measures and extent of the control over electronic communications are published on the internet.[32] However, in Poland as in Lithuania, the Government does not publish reports about the extent of the control over electronic communications claiming it is a national secret. We have to admit that the scale of such practice is decreasing. Supposedly, society should be aware of the statistics on control over electronic communications and its extent. For instance, in Sweden the Prosecutor General makes annual reports about the supervision of electronic communications for the Parliament. According to the 2002 report made in 2003, the extent of the control over electronic communications increased (courts rejected only two requests to carry out controls of electronic communications, and 553 requests were granted. In addition, the report gave information that in 50% of the cases, where electronic communications have been controlled, non evidentiary material was collected.

In 2003 a non-governmental organisation supervising the treatment of human rights, the Swedish-Helsinki Committee, offered to strengthen the Parliamentary control of the surveillance of electronic communications and ensure an independent mechanism of the surveillance of electronic communications in Sweden.[33] One of the solutions made was to create an independent institution for supervising.

A possibility to form a special institution in Lithuania has been provided in the new version of the draft Law on Operational Activities; unfortunately, this draft document was not accepted by the Seimas, although it was presented as a discussion paper. It is important to note that similar institutions already function in Germany, France, the UK and other states. Another subject for discussions would relate to a possibility to assign the State Data Protection Inspection to carry out the tasks of this special committee.

[31] Annual reports with information on the extent of the control of electronic communications, its duration etc, are already published in a number of countries as, for instance, France, Sweden, Australia, Canada, the USA and others.

[32] The Nature and Scope of Governmental Electronic Surveillance Activity http://www.cdt.org/wiretap/wiretap_overview.html.

[33] Privacy international Survey – Sweden. 2004 http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83530.

Conclusions

The valid version of the Criminal Procedure Code of the Republic of Lithuania does not provide a requirement to give a sanction for the collection of information about traffic data from providers of electronic communication services, which is inconsistent with the rule from the Constitution of the Republic of Lithuania declaring the inviolability of the right to private life.

There is a lack of secondary legislation which needs to be immediately adopted to ensure a proper respect for private life in the course of control of electronic communications for criminal investigation purposes.

The EU directive on the retention of communications traffic data can have a great impact on the period of retention of traffic data administered by providers of electronic communications services. The provisions of the Directive are possibly inconsistent with those of the Constitution of the Republic of Lithuanian as far as it concerns the requirement to store information about the traffic data longer than it is needed to ensure economical activities. Competent institutions should take all necessary measures to evaluate this possible inconsistency when implementing the Directive.

It is difficult to distinguish between traffic data and contents data in the internet environment which may cause difficulties in implementing the task of controlling and recording traffic data transferred by electronic communications in accordance to article 154, part 2 of the Criminal Procedure Code of the Republic of Lithuania. Therefore, a possibility to unify the categories of contents data and traffic data in the course of control of electronic communications should be discussed.

We question the decision to authorise the State Security Department to safeguard in its premises the technical commands via electronic communications "to begin" and "to finish" the interception or perform other controls over information transferred by electronic communications in the way the commands could not be changed as the Department is a body performing operational activities too. This situation is inconsistent with the principles of a democratic state since the same institution cannot perform operational activities and control them at the same time. There should be a procedure in place, which safeguards such activities. This should not be performed by a different body than the one responsible for operational control, or at least a proper control of this safeguarding procedure should be implemented.

The supervision of the control of electronic communications is one of the ways to ensure respect for private life in electronic communications. It is obvious that the supervision of the control of electronic communications should be strengthened. The existing supervising institutions should have more rights.

Finally, we propose to establish a special independent institution for the supervision of control of electronic communications.

Bibliography

1. Resolution No.1593 of the Government of the Republic of Lithuania of 6 December 2004 concerning the provision of authorisations for the implementation of the Law on electronic Communications of the Republic of Lithuania http://www.lrs.lt;
2. Resolution No.IX2022 of the Seimas of the Republic of Lithuania of 12 February 2004 concerning the approval of the Statutes of the Committee of parliamentary control over operational activities http://www.lrs.lt;.
3. Banisar D. A Commentary on the Council of Europe Cybercrime Convention http://privacy.openflows.org/pdf/coe_analysis.pdf;
4. Broadhurst R. Content crimes: criminality and censorship in Asia. Conference on „The Challenge of Cybercrime". 15-17 September, 2004. Palais de l`Europe, Strasbourg, France http://www.coe.int;
5. Directive 2006/24/EC of the European Parliament and of the Council of Europe of 15 March 2006 on the retention of data processed and stored-generated or processed in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism and amending Directive 2002/58/EC OJ L 105/54;
6. Electronic Communications privacy Act. United States Code. Title 18 – Crimes and Criminal Procedure. Part I - Crimes. Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications *http://floridalawfirm.com/privacy.html*;
7. Law on Personal Data Protection of the Republic of Lithuania VŽ, 1996, No. 63-1479;
8. Criminal Procedure Code of the Republic of Lithuania VŽ, 2002, No. 37-1341;
9. Law on Electronic Communications of the Republic of Lithuania VŽ, 2004, No. 69-2382;
10. Law on Operational Activities of the Republic of Lithuania VŽ, 2002, No. 65-2633;
11. Maxwell W. Electronic Communications: the New EU Framework. Part I, Booklet 1.5. – New York: Oceana Publications, Inc., 2002;
12. Privacy International – Republic of Poland. 2004 *http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83774*;
13. Privacy International Survey – Republic of Estonia. 2003 http://www.privacyinternational.org/survey/phr2003/countries/estonia.htm;

14. Privacy International Survey – Republic of Latvia. 2003 *http://www.privacyinternational.org/survey/phr2003/countries/latvia.htm*;
15. Privacy international Survey – Finland. 2004 *http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83553*;
16. Privacy international Survey – Sweden. 2004 *http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83530*;
17. Surveillance Act of Estonia (February 22, 1994) *http://vlf.juridicum.su.se/master99/library2/teste/Surv.htm*;
18. The Nature and Scope of Governmental Electronic Surveillance Activity *http://www.cdt.org/wiretap/wiretap_overview.html*;
19. The New Data Retention Directive European Media, IP & IT Law Review, 2006 No. 1;
20. Implementation of Human Rights in Lithuania: overview, 2005. Human Rights Monitoring Institute. 2005 http://www.hrmi.lt;
21. Human Rights Monitoring Institute: Restrictions of Private Life in Electronic Communications for Crime Investigation and Prevention Purposes. 2005 http://www.hrmi.lt.

Monitoring and Supervising Children on the Internet: Rethinking the parental responsibility[1]

Syahirah Abdul Shukor

Abstract

Nowadays, children possess more technological knowledge than any previous generation. Parents, however, fear that the excessive usage of the Internet may harm their children. There have been discussions that parents should take responsibility in protecting their children from harm on the Internet by installing filtering software. Parents face problems as some of them are not familiar with the Internet compared to other media like television. Furthermore, with the very nature of the Internet, supervising and monitoring children's activities is difficult. The United States courts have decided that the burden of protection from media content in the home "firmly rests on parents". This paper examines whether parental responsibility should be extended to monitoring and supervising their children's activities on the Internet. The notion of punishing parents for their children's criminal or anti-social behaviour is emerging, from Australia to the United States of America and Great Britain. Hence, is it possible to punish parents for children's misdeed on the Internet? This paper aims to demonstrate that it is high time to rethink legal aspects of parental responsibility regarding their children's activities on the Internet.

1. Introduction

Realising the acclaimed importance of Information and Communication Technology (ICT), most parents who can afford it provide their children with a computer and Internet access. Some parents think that a computer as a tool of communication helps children to get information and will keep them off the streets and out of trouble. Nixon has written on the increasing interest of parents in the benefits of ICT to their children's future as follows:

> *The family is being constructed as an important entry point for the development of new computer-related literacy and social practice in young people….what is discursively produced within the global cultural economy as digital fun and games for young people, is simultaneously constructed as serious business for parents.*[2]

Earlier moral panics regarding the Internet were mainly about child pornography, paedophiles and sexual explicit content. Undeniably, the Internet

[1] The author would like to thank Dr Lieve Gies for her comments on the draft. Also to Mr Leslie Terebessy in proofreading this paper. All opinions and errors are, of course, those of the author.

[2] Nixon, H. (1998), "Fun and games are serious business", in: J, Sefron-Green (ed). *Digital Diversions: youth culture in the age of multi-media*, London: UCL Press, p 23.

provides a social structure with applications such as email, newsgroups etcetera, which bear the potential for social implications such as bullying, cheating and so forth. In terms of using the Internet, there are two perspectives that create fear with parents; firstly, the popular claims about the adverse effects of the Internet caused by paedophiles and sexually explicit images and secondly, that children may transgress the boundaries of law and morality by acts such as hacking and downloading viruses. It is difficult for parents to supervise and monitor children due to the very nature of the Internet. Putting the responsibility on parents for children's activities on the Internet is perhaps one of the possible solutions available. I believe, however, that state and Internet Service Providers (ISPs) should assist parents in accomplishing this duty. This paper begins by asking: "why parental responsibility?" Then, it further asks if parental responsibility should be extended to cyberspace. It concludes with the urge to rethink parental responsibility and the innocence of childhood as the Internet user.

2. Why parental responsibility?

Parental responsibility law is not a new concept. It has been part of the response to juvenile delinquency since the 19th century.[3] It comprises a "cyclical phenomenon with a very long history".[4] In the UK, parental responsibility provisions have been consolidated in a series of legislative provisions.[5] The relationship between parents and child has been defined in terms of parental responsibility. According to this legal construction, childhood is a preparation for adulthood and parents are responsible for caring and raising the child to be a properly developed adult both physically and mentally.[6] The problem is that no precise definition is given of the rights, powers, duties and responsibilities that go along with this obligation. Although Hershman and MacFarlene have listed the rights of parent that have been confirmed judicially and/or statutorily[7], it is my opinion that this list needs to be revised from time to time to ensure its conformity with current developments of technology and its relation with family ties, between children and parents. Popular belief is that parents are entirely responsible for children's behaviour and learning, which is one of the most mistaken assumptions in parenting.[8] Despite this assumption, there have been aetiological researchers (those who are studying the causes of problems) who interrelate juvenile delinquency with parental responsibilities.[9] In a research

---

3 Arthur, R. (2005). "Punishing parents for the crimes of their children", *The Howard Journal*, Vol 44, No 3, July, p 234.

4 Day-Sclater and Pipper, C. (2000), "Re-molising the Family? Family Policy, Family Law and Youth Justice", *Child and Family Law Quarterly*. 12:2. p 135

5 *Powers of the Criminal Courts (Sentencing) Act 2000 (initially part of the Criminal Justice Act 1991, the Crime and Disorder Act 1998 and the Anti-Social Behaviour Act 2003).*

6 Lord Mackay (1998). *Hansard*, House of Lord, Vol 502, col 490.

7 Hershman and MacFarlane (1997), *Children Law and Practice*, Family Law, para A[4]

8 D. Evans, T and A.Evans, M. (1993), "The Fallacy of Parent Responsibility", *Individual Psychology*, Vol 49, No 2, June, p 231.

9 See Graham, J and Bowling, B. (1995), "Young people and Crime", *HORS* 145, D Riley and M Shaw, (1985), "Parental Responsibility and Juvenile Delinquency", *HORS* 83, London: Home Office.

project, it was disclosed that poor parental supervision is strongly connected to juvenile convictions.[10] Parental supervision is regarded as an essential element of good parenting in today's modern society due to existing risks and dangers. For instance, those who live near a busy road must take precautions to ensure that their children are not exposed to the dangers of traffic.

With the emergence of ICT, life as a parent is more complex as parents are expected to monitor and supervise their children's activities in using the Internet. There are discussions that parents should have the responsibility to protect their children from the harm on the Internet by installing filtering software. United States courts have decided that the "burden of protection from media content in the home firmly rests on parents".[11] It was argued that solutions must come from the family, stating, "people in their own homes can control the events in their own living room. They can indeed turn off the TV".[12] Some people think that the Internet is just like television, but the reality is that the nature of the Internet differs from other media as the Internet is more interactive and multipurpose. Allowing children to explore the Internet without any guidance from adults will generate a huge generation gap especially in terms of the relationship between parents and children, as Turkle points out. This is mainly due to parental unfamiliarity with the Internet.[13] If parents keep a distance with the advance of the Internet, they will not comprehend the usage and benefits as well as the dangers of it. Parents nowadays need to be involved in their children's activities though they have different perspectives about the new technology. The notion of control on the contents of the Internet by parents implicitly shows that society expects parents to show the risks and dangers of the Internet to their children. But again, the question is if that implies that parents should be punished for their children's misdemeanours on the Internet.

Supervising the activities on the Internet of children and young people is difficult in the sense that some parents are not familiar with this new technology. A US study has explored the relationship between parental supervision and the growing popularity of the Internet.[14] In fact, prior research shows the importance of parental monitoring for the child.[15] Tyler questions parental responsibility laws, arguing these could be "quick-fixes" to satisfy the increasing concern about delinquency and could be unfair to parents: should parents be held

---

10 Graham and Bowling (1995).

11 Feather, M. (2005), "Censorship, Cookies and Milk: Children and Protections on the Internet", Available at http://www.cqcm.org/kidsfirst/html/info/netkids.pdf, accessed 1st June, 2005.

12 Yushkiavitshus (1989), as quoted in Stanley, J., "Child Abuse and the Internet", *Issues Child Abuse Prevention*, Australian Institute of Family Studies, No 15, Summer 2001, p7.

13 Turkle, S. (1995), *Life on the Screen: Identity in the Age of the Internet,* p 227.

14 Wang, R *et al.* (2005), "Teenagers' Internet Use and Family Rules: A Research Note", *Journal of Marriage & Family,* 67, December, pp 1249-1258.

15 Armato,.P & Fowler, F. (2002), "Parenting Practices, Child adjustment and Family Diversity", *Journal of Marriage & Family,* p 64.

responsible for their children's behaviour or should society share the blame?[16] Parental laws which punish parents for their children's misbehaviour may deliver a confusing message, namely that young people can shirk their responsibility to their parents.[17] Punishing parents for their child's misdemeanours on the Internet will not assist the situation but may lead to other conflicts between parents and children. Furthermore, some parents have taken initiatives to prevent their child from getting involved with delinquency and crime. Yet, it is difficult to determine the causes of a child breaking the law. Gelsthorpe has voiced her concern about vulnerable parents (those parents who worked hard to be good parents) as follows:

> *Whilst the need for early intervention in the lives of children to prevent delinquent behaviour and to protect those at risk is overwhelmingly convincing, the need to punish already vulnerable parents is not.*[18]

Furthermore, it has been argued that the offence for which to punish the parents is not clear and that punishing them is ambiguous in the sense that all forms of child delinquency may result in the parents bearing the consequences. Yet, legislators often do not recognize efforts made by parents to prevent children from misbehaving and breaking the law. Parents should be given the right to appeal for their share when held responsible for their children's offences. Courts need to recognise "neglect parents", "responsible parents" or "abusive parents" before imposing penalties to them for child misbehaviour. What concerns me is that economic loss, for instance occurring in cases where a child hacks a company's website, can be huge compared to that invoked by other forms of delinquency. The question is how this problem should be addressed legally and who should bear the consequences.

3. Parental responsibility in the advance of the Internet

Jagodinzinki considers the two Disney films, "Honey, I shrunk the kids" (1989) and its sequel "Honey, I blew up the kid" (1992) as symptomatic manifestations of a general societal guilt felt from the breakdown of modern family structure where, in both films, the parents have been ignoring their children due to work related commitments. These were warning fantasies to parents not to neglect or abandon their children. He further argues that we fail to "see" our children and when we finally do, they are monsters we never expected.[19] Much emphasis is put on protecting children from being victimized on the Internet due to their vulnerability and dependency to adults, especially parents. Therefore, an

---

16 E.Tyler, J. (2000). 'Parental Liability Laws: Rationale, Theory and Effectiveness', *The Social Science Journal,* Vol 37, Number1, p 79.

17 Gelsthorpe, L. (1999). Youth crime and criminal responsibility. In Bainham, A. (1999). *What is a Parent? A Socio-Legal Analysis.* Oxford- Portland Oregon: Hart Publishing, p229.

18 Gelsthorpe, L. (1999), p 236.

19 Jagodzinski, J. (2004). *Youth Fantasies, the perverse landscape of the media.* New York: Palgrave Macmillan, p 235.

important task is helping children and parents to use the Internet safely. This is illustrated by the mushrooming of websites that discuss children's safety on the Internet. Another factor, which also needs to be considered, is how the Internet shapes the thinking of our children; can they still differentiate between life online and offline? Although parents may control their children's access to adult websites by using software developed for this purpose, this software cannot filter out sexually explicit images. Akdeniz argues that the current solutions consisting of various regulations, for instance, the development of rating and filtering systems, may not be the real answer to the problem.[20] If that is the case, shall we seek for a private solution by imposing the responsibility on parents? The discussions which suggests that parents should be able to control the Internet usage of their children is not new. According to Flint:

> *At the end of the day, whatever the law and rules enacted and however vigilant the authorities, there can be no substitute for parental responsibility and oversight. If you don't know where children are going whether on cyberspace or realspace, it can hardly be unexpected if they go somewhere where you prefer they avoided.*[21]

In itself, it is simple to impose on parents the responsibility to look after their children's activities but we cannot deny that as children grow up they need some space and privacy. Children represent a large group which includes anyone below the age of eighteen. Hence, as children grow up, parents tend to provide their children with some independence. Furthermore, research findings suggest that parents are not necessarily well informed about their children's activities on the Internet, in particular in the case of adolescents due to their developing need for independence and privacy.[22] Livingstone argues that there is an internal threat connected to supervising and monitoring children on the Internet, because it puts to risk the crucial relationship of trust between parents and children.[23] However, Valentine and Holloway argue as follows:

> *ICT emerges in different ways in differential household depending on parents' differential; in understanding of technology and conceptions of online and offline space, family regimes and parenting styles, and differential levels of social and competencies among household members.*[24]

Different parents have different parenting styles which are greatly influenced by their social background, culture and belief about parenting. There is no

---

20 Akdeniz, Y. (2001). Controlling illegal and harmful content. In Wall, D. (ed). *Crime and the Internet*. London & New York : Routledge, p 130.

21 Flint, D. (2000). The Internet and Children's Rights Suffer the Little Children. *Computer Law & Security Report,* Vol 16. no 2, p

22 Finkelhor et al. (2000). Online Victimization on a report on the Nation's Youth, Crimes against children research centre. Available at http://www.missingkids.com, accessed on 1st April 2006.

23 Livingstone, S. (2004) Children's Privacy Online. Experimenting with boundaries within and beyond the family. Available at http://www.lse.ac.uk/collections/media@lse.whowho/Sonia.Livinsgtone.htm, accessed on 1st February, 2006.

24 Valentine, G and Holloway, S. (2001). On-line Dangers? Geographies of Parents' Fears for Children's Safety in Cyberspace. *Professional Geographer*, 53(1), p 81.

consensus on what is a good parental style. Similarly, in the case of supervising and monitoring children's activities on the Internet, there is no clear indication of how parents should supervise their children's activities. Though there are debates and suggestions that parents should use filtering software, such suggestions for me come with economical burden. Not every parent can afford to buy filtering software, although, in some circumstances, the software can be downloaded from the Internet be it with limited efficiency. Subscribing to firewalls or filtering software from the Internet Service Providers (ISPs) sometimes has a high price tag too, so parents prefer to provide the facilities of a computer and Internet first before thinking about the safety aspects.

4. Discussions and Conclusions

To make parents responsible for the adverse effects of the Internet to children *per se* is not fair as we need to examine external factors which may influence the upbringing of children. Many adults need help in learning how to grow with their children as ICT advances. Some need education and guidance from professionals in order to function as competent parents. However, the notion to totally blame or punish the parents for their child misdeed or crime needs to be placed with caution. Fortin argues that government intervention in family life between all parents and children through legislation has traditionally provoked strong hostility especially if such legislation threatens to interfere with the parent-child relationship.[25] The responsibility to protect children from risks should not be on parents alone, society must also protect children from risks. However, risks on the Internet are difficult to assume due to the very nature of the Internet. Hence, the state and the ISPs play a crucial role in educating parents on safety on the Internet. Before parents subscribe to the Internet, they should be informed by ISPs on the dark side of using the Internet that may affect them and their children. Without a reminder from the ISPs to keep an eye on child safety, parents will overlook the need to supervise their children's activities. It is possible to punish parents if it is proven that parents have negligently failed to take precautionary steps to ensure that their children's activities on the Internet are in line with the nature of children who need protection and guidance from parents from time to time. Parenthood itself should not be seen as burden but it is a developmental stage in the life cycle. Parenthood itself needs the support from state and society at large. Westman states that the maturing and emotionally satisfying elements of parenthood are fundamental, if not explicit, motivations to become parents.[26] The support given will definitely be cherished by today's modern parents in facing the challenges in bringing up children in an age of technology. I believe that the notion of punishing parents for child's misdeeds on the Internet is a reminder to negligent parents to take their duties seriously.

---

[25] Fortin, J. (2003) *Children's Rights and the Developing Law*, 2nd Ed UK, LexisNexis Butterworths, p8

[26] C. Westman, J. (1999) Children's Rights, Parents' Prerogatives and Society's Obligations. *Child Psychiatry and Human Development.* Vol 29(4), Summer, p 327.

R (87) 15: A Slow death?

Joseph A. Cannataci, Mireille M. Caruana,
Jeanne Pia Mifsud Bonnici[1]

Abstract

Recommendation R (87) 15 was vaunted as being possibly one of the most successful products of the Council of Europe's Committee of Experts on Data Protection. Its adoption as an Annex to the Schengen Agreement meant that it became (or was expected to become) the de facto data protection standard for police forces across Europe.

Nearly twenty years have passed since R (87) 15 was finalised in the teeth of much opposition from a number of security forces across Europe. The methods chosen by terrorists and criminals since 1987 have also taken a number of new directions making police and security forces even hungrier users of personal data. On the face of it, in spite of three review exercises, R (87) 15 has been retained intact. Indeed by 1992 (in Recommendation 1181(1992)1 on police co-operation and protection of personal data in the police sector) the member states of the Council of Europe had agreed to move towards a convention enshrining the principles of R (87)15. Fifteen years from R 1181(1992)1, R (87)15 has never made it to convention status. The data protection star is on the wane and, while some continue to pay lip service to R(87)15, a number of measures have been agreed at the European level which appear to undermine the spirit if not the letter of the landmark recommendation which is so unloved by police forces.

This paper traces the review processes of R (87) 15 within the Council of Europe and the up-grade measures considered within the CJ-PD (Committee of Experts on Data Protection). These are then contrasted with actual developments which resulted in the recommendations of the Working Party on Data Retention and the resultant ignoring of the data protection position by the Council of Ministers and Parliament. New technologies like biometric passports have led to agreement at the European level which further promise widespread collection of personal data by police and security forces. These recent developments fuelled by concerns rendered more acute in the wake of 9/11 may be interpreted as signifying the beginning of the end for R (87) 15 or alternatively as being merely part of the downward graph in a cyclical evolution of a data protection culture.

---

[1] Professor Joseph A. Cannataci is Head of the Lancashire Law School at the University of Central Lancashire UK. Dr. Mireille M. Caruana is a Visiting Lecturer at the University of Malta. Dr. Jeanne Mifsud Bonnici is a Research Fellow at the Centre for Law & IT at the University of Groningen, The Netherlands.

"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than (British) society would feel comfortable with..."

(Richard Thomas – August 2006)

1. Introduction

Many newcomers to the field of data protection law, at first, fail to notice that the crux of most arguments boils down to "purpose" or, as the French would call it, "*finalité*". What is the purpose for which the personal data is being collected in the first place and what is the onward-use of such data? Is it compatible with the purpose for which the data was collected in the first place?

This is the fundamental tension underlying use of certain personal data by police and security forces and it revolves around a central tenet of data protection law i.e. that personal data can only be processed for the purpose(s) for which it was collected. This is a principle inimical to the basic instincts of many police officers in what they often view as being their sometimes unequal war on crime. Police officers often wish to use personal data irrespective of the purpose for which it was given: what they view as important is "does it provide a lead? Does it help detect or prevent an offence?". If that is the case, then purpose can take a second seat to the security of society and/or the prevention of crime.

This tension is not something new. It has existed from the very beginning, from the very first attempts of applying basic data protection principles to the police and security sectors. Indeed, it arises out of, or is at least related to, a tension that pre-dates classic data protection laws. Privacy and security have never been easy bedfellows. Numerous attempts at keeping police forces in check within a democratic society (e.g. interception of telecommunications) have always striven hard (and sometimes failed) to strike the right balance between the individual's right to privacy and the public's (in this case the police's) right to know.

Nor is it solely police use of personal data that raises problems of underlying tensions with the fundamental principle of purpose that underpins all of European data protection law. The UK Information Commissioner, Richard Thomas, recently summed up his concerns in the following manner:

> *"Some of my counterparts in Eastern Europe, in Spain, have experienced in the last century what can happen when government gets too powerful and has too much information on citizens. When everyone knows everything about everybody else and the Government has got massive files, whether manual or computerised..."*
>
> *"I don't think people have woken up to what lies behind this. It enables the Government of the day to build up quite a comprehensive picture about many of your activities. My job is to make sure no more information is collected than necessary for any particular purpose*."

Thus although Thomas does not oppose the idea of identity cards, insisting that he cannot be *"for or against",* he is critical of the UK Government's failure to spell out in a draft Bill the cards' exact purpose. He says*:*

> *"The Government has changed its line over the last two or three years as to what the card is intended for. You have to have clarity. Is it for the fight against terrorism? Is it to promote immigration control? Is it to provide access to public benefit and services? Various other reasons have been put forward... I don't think that is acceptable."*[2]

In this interview, Richard Thomas is questioning the precise purpose of proposed ID cards in the UK and asking as to whether the fight against terrorism is the main purpose for having personal data collected and stored in order to issue UK citizens with an ID card. Thomas appears to be here still fighting for the basic tenet of purpose, but this paper asks whether this battle has already been lost, at least insofar as use of personal data by the police is concerned. It is crucial, at this stage, to also determine certain perspectives: are laws and fundamental principles so absolute that, once recognized, they can exist inviolate or are they cyclical in their appreciation, development and consolidation? Are certain principles in data protection law rather like trees and plants that are laid bare by the winter but return in full bloom by the spring and the summer before moving again into the less clement cycles of autumn and winter…only to flourish again once the climate is favourable in the next part of a perpetual cycle? Or are such perspectives merely wishful thinking on the part of privacy advocates who refuse to countenance the fact that some rights have been irretrievably lost?

Thinking about cycles and taking the long view of the history of legislation is a salutary exercise for, clearly, the fragility of man's respect for fundamental human rights may be measured by the relative youth of such concepts in legal

---

[2] In an interview with The Times available at http://www.timesonline.co.uk/newspaper/0%2C%2C2710-1218615%2C00.html as reported on the 16th August 2006

history. It took the best part of four thousand years from the Codex of Ur-Nammu[3] and the more famous one by Hammurabi[4] for society to come up with the 1948 United Nations Declaration of Human Rights,[5] the first international instrument to recognize a right to privacy.[6] Article XII states that "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."

Then again some would argue that this advance from a system of law that was largely property-based[7] to one that recognizes rights pertaining to human beings, their personality and their dignity, wherever they may be and whatever their ethnic origin or religious belief, had to be jolted along by the carnage wrought by two world wars. The internationalization of war on such a massive scale as seen during the twentieth century, coupled with the ubiquity of media and information technologies, has led to an almost proportionate internationalization of law, and privacy is no exception.

The space available in this paper does not afford a full-scale debate on the notion of cycles in history or in legislative history in particular, yet "the recent development of mathematical models of long-term ("secular") socio-demographic cycles has revived interest in cyclical theories of history ".[8] It is tempting to view the past and current developments of data protection law as part of an historical cycle, though where the cycle will lead to next is difficult to predict since privacy is such a relatively new area of law.

Such patterns and cycles, including legal development at the national level[9] and subsequent spread to the international level have long been discernible in privacy law, as have been the links to various forms of information technology. The printing press was the technology that communicated and amplified the thinking of the French *philosophes* and underpinned a lot of what happened at the national level during the French Revolution of 1789. Yet, the same

---

3 Ca 2050 BC

4 Ca 1780 BC

5 Adopted and proclaimed by the UN General Assembly on 10 December 1948.

6 See Article XII.

7 Hammurabi's code focussed chiefly on focuses on theft, agriculture (or shepherding), property damage, women's rights, marriage rights, children's rights, slave rights, in addition to more fundamental issues such as murder, death, and injury

8 http://en.wikipedia.org/wiki/Philosophy_of_history. See, for example, Peter Turchin, Historical Dynamics: Why States rise and Fall, (2003) Princeton University Press, for an American take on macromodels and the even more recent Andrey Korotayev et al. Introduction to Social Macrodynamics (2006) Moscow, URSS for a Russian but not altogether dissimilar line .For a different approach to historical cycles see William McGaughey, Five Epochs of Civilization (2000) Minneapolis: Thistlerose Publications .

9 Although even the term "national development" is suspect in an area where thinking is growingly international, since the exchange and influence of ideas across national boundaries is already well apparent at the time of the US Declaration of Human Rights and the French Revolution.

technology also contributed enormously [10] to the birth of a new nation even before the French revolution, as may be seen, say, in the impact of the articles and pamphlets of Thomas Paine in the period leading to the American Declaration of Independence of 1776. Between 1789 and 1791 the Bill of Rights, comprising the first ten amendments to the United States Constitution, was adopted. All ten amendments relate to limiting the power of the federal government. The Fourth Amendment in particular guards against searches, arrests and seizures of property without a specific warrant or a "probable cause" to believe a crime has been committed. A general right to privacy has been inferred from this amendment and others by the Supreme Court of the United States[11], although it remains to be said that the line of cases deriving there from remains controversial and has drawn accusations of judicial activism.

It took over another 150 years for some of the principles established and developed within the First Amendment of the United States constitution to become sufficiently internationalized at the UN and European level. A couple of years before the European Convention of Human Rights of 1950[12] upheld a general right to privacy[13], in 1948 George Orwell was writing "Nineteen Eighty-Four". The nightmare fantasies depicted by George Orwell in this classic work of fiction did not even contemplate the existence of what was to come – the pervasiveness of computers and the invention of the World Wide Web. Yet they were part of an important cycle, as the Europe of the dictators that preceded World War Two came together to reject the past, the spectre of totalitarianism that was to cast a sinister shadow over the whole of the Cold War. 1989 saw the beginning of the end of what historians may eventually call the "Soviet cycle of totalitarianism". 1989 led to 15 years of optimistic growth with a European Economic Community that became a Union which went from 9 to 25 members by 2004 and a Council of Europe that, during the same period, went from 21 members to 46.

If the misery of the two world wars led to the birth of the welfare state and the prosperity of the 1960's, the death of the European colonial empires and the battle of ideologies led to the cycles of terrorism that afflicted France, Germany and Italy in the 'sixties and the 'seventies. The industrial unrest of the 'seventies and early 'eighties also witnessed the crushing of the Baader-Meinhof gang in Germany and the Brigate Rosse in Italy, and once again gave way to the prosperity and optimism of the late 'eighties and early nineties. Could anyone be blamed for seeing up-beat privacy legislation at the national and European levels

---

10 See for example the impact of the various publications as evidenced in Gertrude Himmelfarb, The Roads to Modernity: The British, French and American Enlightenments, (2004) and especially in this example, the writings of Thomas Paine as summarised in http://en.wikipedia.org/wiki/Thomas_Paine

11 See Griswold v. Connecticut, 381 U.S. 479 (1965), a landmark case in which the Supreme Court ruled that the Constitution protected a right to privacy.

12 Signed in Rome on 4 November 1950, available at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

13 Article 8; Article 10 of the same Convention guarantees the right to freedom of expression.

in the latter half of the eighties and the first half of the nineties? Convinced that the values of the liberal West had triumphed, it was perhaps only natural that the years 1986-1996 were characterized by an apparent entrenchment of the data protection principle of purpose specification in many levels.

This entrenchment had been a long time in the making: the privacy debate in the US between 1966 and 1973 which led to the Federal Privacy Act 1974 had made its way across the Atlantic and, following two resolutions of the Parliamentary Assembly in 1974 led to the birth of the Council of Europe's Committee of Experts on Data Protection in 1976. Yet another five years of international haggling led to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14] (hereinafter referred to as Convention 108) and almost another 5 years for this Convention to come into force in 1985. Spurred on by visions of "1984" and with totalitarianism in the East still apparently very much in the driving seat, the years 1984-1986 were taken up by intensive debate which, in 1987, saw agreement being reached upon Recommendation No. R (87) 15 regulating the use of personal data in the police sector (hereinafter referred to as R (87) 15).

1995 saw the European Union twist the arm of (at least some of) its member states to enact harmonized national legislation on data protection when it passed Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as Directive 95/46)[15], which all EU member states were required to implement into national legislation by 24 October 1998. The Schengen Agreement also came into effect in 1995, including a reference to R (87) 15.

It will be seen that the 1986-1996 period of consolidation in data protection law gave way to another dip in the cycle. Directive 95/46 had barely come into effect in 1998 when concern with data privacy was heavily off-set by security concerns, especially following certain specific events. 2001 saw the great tragedy widely and simply referred to nowadays as "9/11". Terror struck the USA in an unexpected and phenomenal manner. Exactly 912 days after the 11th September terrorist attack on America in 2001, terror also struck in Europe when on the 11th March 2004 a series of coordinated bombings against the commuter train system of Madrid, Spain, killed 192 people and wounded 2,050. The next successful attacks in Europe were the London bombings which occurred in July, 2005.

The tension between two fundamental societal values is immediately evident: on the one hand, the right of the citizens to be protected from terrorism and the obligations of a sovereign State to fight against it and safeguard public security,

[14] Strasbourg, 28.I.1981; Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[15] Official Journal L 281, 23/11/1995 P. 0031 – 0050, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm

and on the other hand, the individual's right to personal data protection and privacy. With the declared aim of providing a vital tool against terrorism and serious crime in the hands of the law enforcement agencies across Europe, 2006 saw the finalization of the Data Retention Directive.[16]

R (87) 15 has, despite opposition, remained unchanged since its introduction in 1987. But are we in Europe in fact "killing [it] softly", as it begins to pass unobserved and legislation purportedly infringing on civil rights and in violation of the spirit, if not also of the word, of the said Recommendation is passed as if it were a simple matter of course? Before proceeding to see where this part of data protection law fits within successive cycles of domestic and international terrorism, it is worth examining its birth and development in some further detail.

2. The painful birth of R(87) 15

Fourteen months before Mr. Gorbachev had his fateful meeting with Mr. Bush in Malta but scarcely three years after the unsuccessful IRA attempt to blow up Margaret Thatcher, on the 17 September 1987 the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector. This Recommendation (hereinafter referred to as R (87) 15) was a victory for the basic principle of data protection of "purpose specification".[17] Principle 2 of R (87) 15 provides that *"the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation"* and later further provides that *"the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry*."

Principle 2.3 of R (87) 15 provides that "*The collection of data by technical surveillance or other automated means should be provided for in specific provisions*."

Principle 3.1 of R (87) 15 provides that "*As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law."*

---

16 Directive 2006/24/EC

17 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. Strasbourg, 28.I.1981 – in particular, Article 5.

These three key principles of R (87) 15 were not easily won. The Recommendation was born within the Council of Europe's Committee of Experts on Data Protection (CJ-PD) in Strasbourg during the years 1984-1986. CJ-PD was characterised by the strong leadership of Germany's Spiros Simitis, later involved in including data protection in the EU Charter of Fundamental Rights, and succeeded by Peter Hustinx, today EU Data Protection Commissioner. Many of the data protection experts at CJ-PD were accompanied by representatives of the police and security forces of their countries. The representatives of the police and security forces were asking for "general purpose" collection, as opposed to the position of the CJ-PD (as also of Convention 108) enlisting "purpose specification" as a basic principle of data protection. It was only as a result of very strenuous negotiations that it was possible to arrive at a consensus basis for the eventual text. The Police and security officials involved could draw upon the very recent memories of the Baader-Menihof and the Brigate Rosse campaigns in Germany and Italy not to mention the on-going campaigns of the IRA in mainland Britain[18] and their interventions before, during and after CJ-PD meetings were intended to minimise the effect of any eventual recommendation on Police operations but, on this occasion at least, they had to bow to the strength of the data protection lobby.

This was especially so when dealing with purpose specification. Convention 108 had created ambiguity by allowing an exclusion from its provisions for security purposes.[19] R (87)15 resolved this ambiguity by unambiguously subjecting police data to the same data protection regime as other data. R(87)15 thus scored a victory by entrenching the notion of purpose for collection and processing of data, even for police use.

[18] Though the mid-1980s saw a lull in IRA bombings in Britain until they commenced again in the early nineties.

[19] Article 9.

3. In the ascendant: the early years 1987 – 1993

R (87) 15 was never popular with the police in Western Europe, although it was greeted as a model for democracy and cited often, especially in the 1989-1992 period, in Central and Eastern Europe.[20] In the face of R(87)15 and then Directive 46/95, Police forces had to at least pay lip service to the principles of data protection.[21]

In the post-1989 surge forward for democracy, R (87) 15 was adopted as the data protection standard for the Schengen Treaty. In order to reconcile freedom and security in the Schengen area, freedom of movement was accompanied by so-called "compensatory" measures. This involved improving coordination between the police, customs and the judiciary and taking necessary measures to combat important problems such as terrorism and organised crime. In order to make this possible, an information system known as the Schengen Information System (SIS) was set up to exchange data on people's identities and descriptions of objects which are either stolen or lost.

In 2001 Switzerland was given the authority to negotiate for accession to the Schengen Convention. The Office of the Federal Data Protection and Information Commissioner then stressed, *inter alia*, that the problems connected with Switzerland's accession should not be seen as a weakening of data protection resulting from Switzerland's participation in an international system of co-operation. On the contrary, Switzerland's accession would in fact benefit data protection by imposing a clearly defined and delineated framework around the data processing operations required for the exchange of information with the contractual parties. This would ensure that standards are demanding and in conformity with the standard of European data protection legislation.

---

[20] An outstanding example of how security forces may indiscriminately collect data and, through the control of that information, control the society in which they operate is that of the Ministerium für Staatssicherheit (MfS / Ministry for State Security), commonly known as the Stasi, the main security (secret police) and intelligence organisation of the German Democratic Republic (East Germany). The Stasi amassed incredible amounts of data collected by all sorts of illegal and secretive means and was widely regarded as one of the most effective intelligence agencies in the world. Its influence over almost every aspect of life in the German Democratic Republic cannot be overestimated. Until the mid-1980s, a civilian network of informants called Inoffizielle Mitarbeiter grew within both East and West Germany. It is estimated that approximately one in fifty East Germans collaborated with the Stasi – one of the highest penetrations of any society by an intelligence gathering organization. During the 1989 peaceful revolution, the Stasi offices were overrun by enraged citizens, but not before a huge amount of compromising material was destroyed by Stasi officers. The remaining files are available for review to all people who were reported upon, often revealing that friends, colleagues, husbands, wives and other family members were regularly filing reports with the Stasi – a picture of a truly Orwellian society.

[21] There is disturbing anecdotal evidence (but no hard evidence as yet uncovered) that the respect of R(87)15 was patchy at best, with some forces in Europe trying to stick to the letter and spirit of the recommendation and others far more openly flaunting the rules on "purpose", remaining very happy to get hold of "interesting" personal data, never mind when it came from. Informal contacts between officers in different national forces appear to very often bypass any controls on personal data export across borders.

Switzerland's accession - *in particular on account of the strict limits imposed on the purposes and uses of the data* - would create a better set of conditions for flows of information and would thus provide better guarantees for the persons affected.[22]

On the face of it, there was no stopping R (87) 15 in the early years. In its **Recommendation 1181 (1992)1 on police co-operation and protection of personal data in the police sector**, the Parliamentary Assembly of the Council of Europe, recommended that the Committee of Ministers, among other things, draw up a convention enshrining the principles laid down in R (87) 15. It was noted that as a result of the Schengen Agreement, the European states co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. At that time, there was already an intensive exchange of data in the police sector among Council of Europe member states on a bilateral or multilateral basis and through Interpol. It was considered to be of vital importance for an efficient combat against international crime that it is fought at national and at European level. Moreover, an efficient fight against crime implies an exchange of data in the police sector. In this respect, it was considered useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member states of the Council of Europe regulating the use of personal data in the police sector. It was considered necessary, however, that there be adequate protection of personal data in the police sector. The Parliamentary Assembly therefore recommended that the Committee of Ministers:

i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;
ii. promote the application of these principles in the exchange of data in the police sector between member states and between member states and third countries via Interpol.

[22] The Schengen Convention from the Viewpoint of Data Protection (July 2002) – Available at http://www.edoeb.admin.ch/dokumentation/00445/00509/00513/00765/index.html?lang=en

4. The first skirmish: 1993

In 1993 the Project Group on Data Protection (CJ-PD) was requested by the Committee of Ministers of the Council of Europe to evaluate the relevance of R (87) 15 and in particular the need to revise the text, namely its scope and principle 5.4 (international communication), bearing in mind the principles set out in Assembly Recommendation 1181 (1992). The Project Group reached the conclusion that R (87) 15 gave adequate protection for personal data used for police purposes and that, at that stage, there was no need to revise it, or parts of it. The Project Group felt that Article 5.4 of R (87) 15, especially when read together with paragraphs 56-80 of the Explanatory Memorandum, appeared flexible enough to meet the foreseeable requirements of international agreements on the exchanges of data for police purposes.

In preparing for these conclusions, the Rapporteur[23] of the Group performed a qualitative analysis on all the national reports of the member states submitted. He reported that the response overview reinforced the impression that R 87 (15) continued to provide a sound basis for data protection in the police sector. The text of R 87 (15) was considered to be sufficiently elastic to permit the various interpretations that some member States may have wished to see specifically mentioned in the text or, more often, in the Explanatory Memorandum. This very fact would militate more in favour of maintenance of the current text rather than the re-opening of the Pandora's box that re-formulation of the text could have brought about. Moreover, several experts concurred "that the provisions of the Recommendation constitute an inalterable necessary minimum" (CJ-PD (93) 48). The number of requests for serious revision of the text, whether to strengthen or to weaken the provisions, was deemed to be too small to merit a re-opening of the discussion on R (87) 15 as a priority matter for the Project Group on Data Protection. With regard to the specific relevance of Article 5.4, it was considered that no overwhelming arguments had been advanced as to why the formulation of Principle 5 (Communication of data) and its accompanying Explanatory Memorandum failed in providing the most balanced formula capable of providing equitable provision for current requirements.

Finally, the Project Group nevertheless proposed that the relevance of R (87) 15 should become the subject of periodic review on a regular rather than an ad hoc basis. For this purpose, it further proposed that the next review be carried out and reported on by December 1998 and thereafter on a four-yearly basis.

[23] The 1993 Rapporteur to the CJ-PD was J.A. Cannataci, one of the co-authors of this present study.

5. Meeting the Internet: Cyber-crime vs. Privacy 1996-2001

For the more pessimistic observers, the first signs of a losing battle could probably be traced to the years 1996 – 2001 as the concern with cyber-crime increased in inverse proportion to the concern with privacy. Despite the long-standing tradition of the Council of Europe of developing data protection standards, the attempts by CJ-PD to insert breach of privacy as a substantive offence in the Cyber-crime Convention failed. The role of the US in the drafting process of the Cyber-Crime Convention was inestimable – in order to get the US on board a Council of Europe convention, the Committee of Experts on Crime in Cyber-space (PC-CY) was prepared to downplay Privacy as an issue. When negotiating the Cyber-Crime Convention, the US was mostly interested in agreeing minimum substantive offences, creating a 24/7 Network for collaboration for the purpose of investigations or proceedings concerning criminal offences relating to computer systems and data and creating a mechanism for the preservation of evidence and subsequent prosecution. Privacy was just not an issue that the criminal justice experts wanted to be bothered about at that stage.

6. The second report: 1998

Four years down the line, the CJ-PD had a number of other successes under its belt: it had completed a Recommendation on Medical Data,[24] a second on Statistical Data[25] and was working on a third recommendation: the Guidelines on Privacy on the Internet.[26] Despite this melee of priority work, the CJ-PD did not shirk its obligation for the four-year review of R(87)15 and indeed, the Rapporteur on this occasion was one of its most respected members, Mr. Alexander Patijn from the Netherlands Ministry of Justice. The 1998 Report by Mr Patijn – *the Second Evaluation of the Relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector* – thus followed the passing of the EU Data Protection Directive and was concurrent with the on-going discussions and negotiations on the Cyber-Crime Convention. The 1998 Report concluded that up till then no serious problems had been raised that would have necessitated changing the recommendation. The report proposed that the Committee of Ministers recommend that national legislators explicitly deal with certain questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure, or national or regional Police law.

The 1998 Report re-stated the case that police powers, to be adequate, necessarily interfere with the respect for private life and should therefore be

[24] R(97) 5
[25] R(97)18
[26] R(99) 5

restricted to the extent that is necessary. It was proposed that the Committee of Ministers of the Council of Europe change their original decision to evaluate the 1987 Recommendation periodically in the sense that periodically the question be answered whether any *additional international instrument* should be developed. The integrity of R (87)15 was thus preserved in this second mini-sub-cycle within a three cycle review process.

7. The third report: 2002

The report on the third evaluation of R (87) 15 was completed in 2002. The CJ-PD examined Recommendation R (87) 15 and agreed that "its principles are still relevant, continue to provide a basis for the elaboration of regulations on this issue and serve as a point of reference for any activities in this field and considered that it is not necessary to revise them at present. Furthermore, this Recommendation is referred to in other international instruments such as the Schengen Agreement and the Europol Convention". Therefore, CJ-PD would not recommend any revision of Recommendation No. R (87) 15 or the preparation of a new recommendation in the police field. The Report also recommended that the third evaluation should be the last of the periodic evaluations and that since the use of personal data in the police sector remains a continuing concern, where necessary further evaluations of specific issues arising in relation to the development of new techniques of processing police data could be carried out. Is the tone of the final evaluation an attempt at casting R(87)15 in stone in face of an increasingly hostile world?

8. Killing R (87) 15 Softly?

In the first evaluation report of R (87) 15 the Rapporteur quoted the stance typically expressed in the strongest terms by the Swiss Federal Data Protection Officer who "takes the view that these Regulations should not be weakened under any circumstances and that the principles set out in Recommendation R (87) 15 should be regarded as established". The CJ-PD appears to have remained consistent with this view over all three re-evaluation exercises but is this enough? Are we in fact killing R (87) 15 softly because while it was ultimately never revised, in whole or in part, other regulations and practices are in fact emerging that undermine the protection given by R (87) 15 for personal data used for police purposes?

9. Changing times – 9/11 – PNR data ….is the May 2006 ECJ decision a 'small' victory?

Terrorism presents our society with a real and pressing challenge. Governments must however respond to this challenge in a way that effectively meets their citizens need to live in peace and security while not undermining their fundamental human rights – including the right to data privacy – which are a cornerstone of our democratic society.

R (87) 15 was created when Europe had largely settled the terrorist issues which had plagued Germany and Italy in the '70s, though the IRA problem was far from solved for the British, the Belgians were in the grip of a terror rampage of their own while the Gladio scandal[27] had yet to explode fully in Italy. Yet, by the end of the 20th Century, while terrorism had become very common-place, almost part of daily life in Europe, this was not the case in the United States. 2001 brought with it 9/11 – a disaster which heralded much trouble for data protection. The first victim was the airline passenger lists resulting in a dispute between the EU and the US.

Following the terrorist attacks of 9/11, the United States passed legislation providing that air carriers operating flights to, from or across US territory have to provide the US authorities with electronic access to the data contained in their reservation and departure control systems, called 'Passenger Name Records' (PNR).

The Commission adopted, on 14 May 2004, a decision[28] finding that the United States Bureau of Customs and Border Protection (CBP) ensures an adequate level of protection for PNR data transferred from the Community. On 17 May, 2004 the Council adopted a decision[29] approving the conclusion of an agreement between the EU and the United States on the processing and transfer of passenger name records (PNR) data by air carriers established in the EU member states to the US customs and border protection. The agreement was signed on 28 May 2004 and entered into force right away.

---

[27] The Gladio scandal was the first official confirmation by a Head of Government that NATO has a secret plan of "stay-behind armies"…accompanied by many accusations that these "security forces" had actually run amok in some Nato countries, actually carrying out anti-democratic actions and even terrorist attacks. For a fuller account of this version of history, see Daniele Ganser, NATO's Secret Armies, Operation Gladio and Terrorism in Western Europe (2004) Zurich.

[28] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p.11).

[29] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, and corrigendum at OJ 2005 L 255, p.168).

In September 2004, the European Parliament brought a legal case against the Commission in the European Court of Justice (ECJ) on the EU/US passenger name records (PNR) agreement. Parliament accused the Commission of misuse of powers, breach of fundamental rights and of the principle of proportionality. The Parliament also appealed to the ECJ for annulment of the Council decision adopting the agreement. The European Data Protection Supervisor intervened in support of the Parliament in both cases, the first intervention before the Court by that authority since its establishment.

On 30 May 2006 the European Court of Justice ruled that "*neither the Commission decision finding that the data are adequately protected by the United States nor the Council decision approving the conclusion of an agreement on their transfer to that country are founded on an appropriate legal basis"*. The ECJ judgment thus annulled both the Commission and Council decisions on a technicality which did not address the substantive issues. The agreement as such was not annulled.

With regard to the Commission decision on adequacy, the Court held that in view of the fact that the first indent of Article 3(2) of Directive 95/46 excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law, and also in view of the fact that the transfer of PNR data to the CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law, the said decision on adequacy did not fall within the scope of the Directive. Therefore, the Court annulled the decision on adequacy and held that it is not necessary to consider the other limbs of the first plea or the other pleas relied upon by the Parliament.

With regard to Council Decision 2004/ 496, the Court held that the Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which are excluded from the scope of the Directive. The Court therefore also annulled the said Council Decision on the ground that it couldn't have been validly adopted on the basis of Article 95 EC as Article 95 EC, read in conjunction with Article 25 of the Directive, couldn't justify Community competence to conclude the Agreement. Once again, the Court held that it is not necessary to consider the other pleas relied upon by the Parliament.

Data transfers continued during a transition period until 30 September 2006, after which the ECJ judgment was to take effect. But the Commission quickly acted to remedy the situation in favour of data transfers: by the 6th October 2006 the United States and the European Union established a temporary arrangement for the transfer of personal information on European travellers that will expire in

July of 2007. The new agreement gives the Europeans greater control over the disclosure of passenger data to the United States. However, it leaves unresolved whether the United States has adequate privacy protections to safeguard the private information of European consumers.[30]

On balance, the decision of the ECJ cannot be considered to be much of a victory for the data protection lobby. On the contrary, as Peter Hustinx, EDPS, points out: "The judgment seems to have created a loophole in the protection of European citizens whereby their data are used for law enforcements purposes. This makes it all the more important that a comprehensive and consistent legal instrument ensuring the protection of personal data outside of the first pillar is adopted without delay".

This comment by Hustinx is especially interesting. The reference to first pillar is intelligible only in an EU context where security and crime prevention did not fall within the scope of the original EU treaty. Yet, most of the major players in the EU are also signatories of Convention 108, wearing their hats as member states of the Council of Europe, which is further amplified in R(87)15. So, while matters between the EU and the US may be currently falling into some form of legal limbo, at the level of individuals, anybody appealing to the European Court of Human Rights in Strasbourg (as opposed to the ECJ in Luxembourg) would be likely to have a court that will take both Convention 108 and R(87)15 into account.

To get to the Strasbourg Court however, an individual must exhaust all local remedies and the current frame of mind in European legislators across Europe is possibly making this more difficult. The recent case of Hungary perhaps illustrates this point best. On the 29th November 2006, the Hungarian President Laszlo Solyom returned to the Parliament the bill about the promulgation of the agreement on registration of travellers' data concluded between the European Union and the United States of America.

The Hungarian President Laszlo Solyom decided not to sign the national law regarding the promulgation of the EU-US PNR (Passenger Name Records) agreement and sent it back to the Parliament, considering that it can be improved. It has been claimed that "This is one of the few set-backs of the new EU-US PNR agreement concluded in October 2006, even though there have been numerous critics to the content of the new agreement that makes possible for air companies to send to US authorities the personal data of the passengers that were registered in the booking system".[31]

---

[30] It is only the Department of Homeland Security which is considered to offer adequacy in this agreement

[31] http://wwwkeh.hu/keh_en/news/20061129communique.html and http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3496

According to the Hungarian President "it is necessary that the Parliament make possible the forwarding of data in the act on promulgation of the international agreement only in case the person in question has explicitly approved of it. The President's opinion is that a regulation of such content would not be contradictory to the international agreement."

Therefore, Mr. Solyom asked the Parliament to re-discuss the bill and to complete it with a rule that stipulates for the explicit approval of the person in question to forward of his data abroad. However laudable the intentions of the Hungarian President may be, it is difficult to see how effective a protection of privacy this can be since most passengers will be compelled to give their explicit consent since they do not have much choice in the matter…unless they give their consent they won't get their air ticket![32] In other words, the protection offered by R(87)15, explicit consent of the data subject will not be worth much in real terms, the situation will be provided for by domestic law and the data subject will have no basis for appeal to the Strasbourg court.

As ever, there may be other issues which colour this cycle of developments: "The (Hungarian) Government might not push too much this issue since the U.S. President
promised last week that he will ask the Congress to waive the visa obligations of the new EU member states. Dr. Kinga Göncz, the Minister of Foreign Affairs was asked by journalists if the President's action could jeopardise Hungary's chances in obtaining a visa free status from the U.S. The minister replied she hopes the problem will be solved soon as it might cause problems in the long run."[33]

[32] Adam Foldes, the Data Protection Program Director within the the Hungarian Civil Liberties Union commented on the events: "Even if the Hungarian law on promulgating the PNR agreement includes provisions on asking for the passengers' consent for handling their personal data, it won't be very useful. How can anybody regard the consent as freely given when the passengers are not allowed to board or disembark the airplane without providing?" ibid.

[33] Ibid.

10. Traffic data & Electronic trails

Any type of data base that generates electronic trails (for e.g., the telecommunication networks, cellular telephone systems, consumer oriented funds transaction systems and automatic traffic control systems) can be used for surveillance purposes – the classical example is the use by the German police of the billing records of the Hamburg electrical board to locate the terrorist Rudolph Clemens Wagner. The police (especially in Germany) had been using traffic data to locate terrorists since the seventies. The lessons of the Clemens Wagner case from the Baader-Meinhof era were well-learnt.

Post-9/11 the police and security forces became more acutely aware of terrorist and crime uses of the Internet. To them the Internet is simply another communications system "to tap" and especially to provide "traffic data". One may consider however the distinction between the uses of data base surveillance for locating an individual (as in the case of Rudolph Clemens Wagner), and the use of surveillance for analysis with the objective of identifying a suspect population.[34]

"When the police are looking for a terrorist, any source of information may be relevant. There are traditional procedures to be followed for obtaining this information similar to those governing search and seizure procedures. The crime in known, the interest in solving the crime may be balanced against, for instance, the interest in privacy. This may be termed *individual data base surveillance*. More difficult is the *collective data base surveillance* situation where no suspect has been identified prior to the data base surveillance…"[35]

A regulation of the collective data base surveillance is not mainly an issue from the perspective of the individual data subject, but is part of a broader issue – the level of surveillance that should be accepted in a society, what procedures should safeguard against misuse of such methods, etc.[36] It is submitted that measures obliging telecommunications and Internet Service providers to store data on all telecommunications and Internet traffic for extended periods are disproportionate and therefore unacceptable. The European Data Protection Commissioners Conference meeting on 6/7 April 2000 in Stockholm stated that such retention of traffic data by Internet Service Providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights.[37] ()

---

34 Prof. Dr. Juris Jon Bing, Privacy and Surveillance Systems – available at http://www.jus.uio.no/iri/forskning/lib/papers/privacy/privacy.html

35 Quoted from the memoirs of Jan Freese, who was head of the Swedish Data Protection Inspection at that time, cf Den makfulkomliga oförmogan, Wahlström och Widstrand, Stockholm 1987:97.

36 Prof. Dr. Juris Jon Bing, Privacy and Surveillance Systems.

37 Cf. also Recommendation 3/99 of the Article 29 Working Party on the preservation of traffic data by Internet Service Providers for law enforcement purposes.

11. Data Retention – ignoring the principle of "purpose specification"

Discussions on regulating the retention of traffic data for law enforcement purposes go as far back as the G8 meeting in Moscow in 1999. By the year 2000, retention of traffic data was allowed for billing and interconnection payments. 9/11 speeded up the discussions and gave a 'justification' for retention of traffic data for longer periods.

The resistance of the Article 29 Working Party, the EDPS and civil society remained unaltered. Upon several occasions since 1997, the Article 29 Working Party and the Conference of European Data Protection Authorities have questioned the necessity of general data retention measures.

In several of its Opinions and Recommendations, the Article 29 Working Party has repeated, almost as a mantra, that retention of traffic data for purposes of law enforcement should be allowed only under strict conditions and that the retained data should only be kept for a limited period and only where necessary, appropriate and proportionate in a democratic society. In its **Opinion on the Draft Data Retention Directive**[38] the Article 29 Working Party questioned whether the justification for any compulsory and general data retention coming from the competent authorities in Member States had been clearly demonstrated and backed up with evidence and also whether the proposed data retention periods in the draft Directive were convincing. The Working Party also stated that in any case, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should be clearly spelled out. Yet, in spite of the Opinion of the Article 29 Group and protests form many other quarters, the European Union still brought into effect Directive 2006/24/EC – The Data Retention Directive.

This Directive forces, in an unprecedented manner, providers of publicly available communication services to store trillions of data relating to the communications of any and all citizens for investigational purposes. So, although it is submitted that the right to respect for private life implies that not everybody can indiscriminately become the subject of criminal intelligence, European law now makes it legitimate (indeed mandatory) to create the tool necessary to make everybody indiscriminately the subject of criminal intelligence-gathering activities.

In the aforementioned Opinion the Article 29 Working Party set out specific safeguards to be envisaged with particular regard to the requirements applying to recipients and further processing, the need for authorizations and controls, the

[38] Opinion WP113 of 21 October 2005

measures applying to service providers also in terms of security and logical separation of the data, the determination of the data categories involved and their updating, and the need to rule out contents data. One could say that the Article 29 Working Party's 'list of desirables' constitutes a return to basic data protection principles and in this sense preserve the spirit of R(87)15. *A contrariu sensu,* the extent to which the specific safeguards were addressed or ignored in Directive 2006/24, may be considered to be a measure as to how much R(87)15 is being "killed softly":

1. *Purpose specification* – Directive 2006/24 does not clearly define and delineate the specific purposes for which data should be retained. Rather, it mandates that the retained data must be made accessible to authorities investigating on non-specified "serious crimes". Thus, the sacred principle of purpose specification, so hard-fought to achieve in R(87)15, has been ignored.

2. *Access limitation* – Directive 2006/24 provides that the retained data is to be provided only to the competent national authorities, but it does not further provide that the competent national authorities should be specifically designated law enforcement authorities or that a list of such designated authorities should be made public. Neither does it clarify that other stakeholders, like the provider himself, do not have access to the data or that the data can only be provided if this is needed in relation to a specific criminal offence.

3. *Data minimisation* – Directive 2006/24 defines data categories in Art 5.

4. *No data mining* – The limitation in Art 4 of 2006/24 to "specific cases" seems to prohibit data mining activities. However (unlike much of the thrust in R(87)15) the Directive does not specify that the retained data can only be provided if this is needed in relation to a specific criminal offence.

5. *Further processing* – contrary ot the opinion of the Art 29 Working Party or the thrust of R(87)15, Directive 2006/24 contains no provision ruling out or limiting stringently further processing for other related proceedings.

6. *Access Logs* – Contrary to the opinion of Art.29 Working Party, the Directive 2006/24 does not create safeguards by providing that any retrieval of the data should be recorded and the records made available to the supervisory authority.

7. *Judicial / independent scrutiny of authorized access* – Once again, an important safeguard recommended by the Art. 29 Working Party is not mandated by the Data Retention Directive.

8. *Retention Purposes of Providers* – Yet again in breach of the advice of the Art.29 group, Directive 2006/24 does not provide safeguards by specifying that data should be retained by the service providers solely for public order purposes, and not for other purposes, especially their own.

9. *System Separation* – There is no specific provision in Directive 2006/24 mandating, in particular, that the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes and protected by more stringent security measures.

10. *Security Measures* – Although Article 7 of Directive 2006/24 lays down general requirements on minimum standards concerning the technical and organisational security measures to be taken by providers, these are not sufficient and in particular the relationship between the adequacy of safety-measures and the costs is not addressed in the text of the provision.

Thus, not only did the Data Retention Directive completely ignore the basic principle of purpose specification, on at least eight other counts, the Directive has been found to fail in providing important safeguards in what constitutes a huge new international collection of databases of transaction data.[39]

Directive 2006/24 has been the subject of harsh criticism, *inter alia* for the disproportionate nature of its measures, for the fact that the notion of purpose is not respected, not enough safeguards established and the cost-efficiency of data retention is nowhere demonstrated.

In its Opinion 3/2006 of 15 March 2006, the Article 29 Working Party remained critical of the Directive, particularly in view of the fact that it lacks some adequate and specific safeguards and leaves room for diverging interpretation and implementation by the Member States. The Working Party considered it crucial that the provisions of the Directive are interpreted and implemented in a harmonised way and that the Directive is accompanied in each Member State by measures curtailing the impact on privacy.

[39] Most of these deficiencies had also been anticipated by Hustinx. On 26th September 2005 Peter Hustinx, European Data Protection Supervisor (hereinafter referred to as the EDPS), issued his Opinion on the Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC39 (hereinafter referred to as the Opinion on the Proposed Data Retention Directive).

12. The Verdict: Is R (87) 15 dead or is it dormant?

It is submitted that the Data Retention Directive achieves the death (or at least a comatose state) of "purpose"…but only for traffic data. The respect for the principle of purpose for gathering data, in this case "traffic data", now takes second place to the notional usefulness of such data in the fight against terrorism and crime. The danger inherent in having whole masses of data preserved, for years and subject to the monitoring by the police and security forces for "their" purposes is being ignored. The Data retention directive lowers the standards by giving legitimacy to the opponents of "purpose" and creates new dangers in the form of large databases of traffic data which previously did not exist.

This being said, strictly speaking R(87)15 is neither dead nor dormant. It is still applicable in every area of personal data except communications traffic data. It still retains all its original strengths as well as its intrinsic weaknesses. As a mere Recommendation, it has no binding power on the member states of the Council of Europe. Quite simply, Hustinx is right in identifying a lacuna and the equivalent of R(87)15 needs to be written into EU law. For there can be no doubt that R(87)15 had achieved a degree of international consensus within Europe. Whether a renewed commitment to this consensus will take the shape of a new Convention of the Council of Europe or an Additional Protocol to Convention 108 incorporating R(87)15 or a new EU Directive adopting as much of R(87)15 as a fierce internal debate will allow (or at least two of the previous options) remains to be seen.

Whichever way it goes, it can also be viewed as being part of a cycle or even a cycle of cycles. The data protection debate is not dead either. While the wars in Iraq and Afghanistan have done much to keep international public attention focused on the so-called "war on terror" and this may have possibly contributed to the data retention directive being introduced in spite of it's clear incompatibility with key established principles like "purpose", there is no clear evidence that a "terror-weary" European public will not once again give prominence to the right to privacy. For the cycles in European history have shown that while terrorism cannot be defeated, nor can it be victorious for it can be contained.[40] In the carnage wrought by roadside bombs and suicide bombers in Iraq and Afghanistan, more Europeans will recall that many of these tactics had been perfected in the "culvert" bombs of the IRA which drove British troops off the road in areas like South Armagh and had forced a total reliance on helicopter transport until troop withdrawal in 2006.

Historical cycles have shown that while terrorist activities will not disappear, there will often be long patches when they fade into the background and new, fresher issues will take their place. Already, the Montreal 2007 Conference of

[40] A lesson learnt from the IRA struggle

Data Protection & Information Commissioners is set to focus further on the Surveillance Society and the ID card is possibly one of the issues that may take some of the limelight during the next national election in the UK. Fundamental Human Rights were one of the planks of Labour policy in the pre-1997 electoral campaign and privacy may yet return to a cycle of being in fashion. At this moment in time, much is being forgiven and/or forgotten in the name of security but when the public realizes or is persuaded that the very same security-measures may be posing a threat to cherished liberties, then we may be in for another cycle of change.

The future of surveillance technologies is probably rosy but not as clear-cut so as some may think. While the mayor of Chicago is promising a CCTV camera on every street corner by 2016, openly boasting that Chicago would rival London, on the other hand Detroit, Miami and Iowa have all abandoned their camera surveillance systems because they did not cut down on crime.[41] The future of R(87)15 will depend on another "battle for hearts and minds" – that of persuading voters that unregulated technological surveillance and unfettered police use of personal data cannot be tolerated. As in the case of R(87)15 in 1984-1986, this debate can be won if it is undertaken by the right people using the right means at the right time. In the same way that 9/11 lent fuel to the Data Retention Directive, it cannot be excluded that some other incidents will not lend themselves to advocates of a new EU Directive implementing R(87)15. There exists a precedent in the way that EU 46/95 practically legislated Convention 108 into being across Europe, in the teeth of some strong opposition, particularly from the UK. A repeat performance with R(87)15 would help temper but possibly never completely exclude the nightmare scenario painted by Richard Thomas i.e that of our sleepwalking into a surveillance society..

It is interesting to speculate on the effect that a resurrected European constitution could have on the fate of R(87)15. The recent "yes" vote in Luxembourg and German premier Merkel's undertaking to resurrect the constitution may lead to developments favourable to R(87)15 if the constitution were to retain its current positive bias towards data protection ruled. In such an eventuality, there is a case to be made for the Data Retention Directive to be un-constitutional, provided always that by the time the Constitution comes into being, EU 2006/24 would not have been scrapped on account of its not being cost-effective.

[41] http://www.epic.org/privacy/surveillance/

Part 2 – Tools

Plagiarism and Fraud in Education: The Importance of Monitoring and Supervision

Kees van Noortwijk and Richard V. De Mulder
Erasmus University Rotterdam

Abstract

This paper is about monitoring and supervision in educational environments. The problem of plagiarism and fraud by students has become significant in the past decade. Information technology plays an important role here. It provides techniques that make it possible to copy text, images and other materials almost effortlessly. Educational institutions are aware of this, and try to halt this undesirable development. IT can play a role here as well, with new applications that can identify plagiarism and / or fraud. Conventional measures as well as a firm and determined anti-fraud policy are a necessity too, however.

1. Introduction

Educational institutions expect their students to work hard and to produce original work, suitable for assessing the progress they make during the curriculum. Students, of course, want to graduate, but are not always convinced of the necessity to do all the work themselves. Why spend effort in doing something that somebody else has already done before you? Copying strategic parts of existing work can seem much more appealing then. And this is even more the case if the subject is difficult or does not interest you all that much.

Several terms are used to describe this undesirable – at least to the educators – student behaviour. 'Plagiarism' is defined in the Oxford Dictionary of English as "the practise of taking someone else's work or ideas and passing them off as one's own".[1] It is a broad term, indicating any copying of the work of another author without giving proper credit and /or specifying the source, therefore making it appear as if he who has copied the work is the author himself. Sometimes this happens unintentionally. For example, an author simply forgets to acknowledge one of his sources.

When the term 'fraud' is used, however, the intention to copy without the readers noticing this dominates. 'Fraud' includes any form of plagiarism in situations where this is expressly forbidden, for instance during examinations or when completing an individual assignment. Certain forms of (unintentional) plagiarism can be overcome by providing proper instructions on how students

[1] *The Oxford Dictionary of English*, second edition, Oxford University Press 2003.

should refer to sources. Identifying and preventing fraud, however, should be a top priority for every educational institution. Legal options for this can for instance be found in the official university regulations regarding education and examinations. It could even be contended that fraud in examinations should be seen as forgery, as the fraudulent actions serve the intention to obtain an official diploma (which can be used as proof of abilities).

2. Types of plagiarism

Several forms of plagiarism can be distinguished.[2]

- Plagiarism of ideas, claiming credit for someone else's thoughts, ideas of inventions. An example of this would be if a student writes a thesis, but copies a line of thought or an important insight from a book he or she has read, without mentioning that book. This form of plagiarism is sometimes difficult to avoid, as people are not always consciously aware of the source of an idea. Here, we put emphasis on forms of plagiarism where this consciousness *does* exist.
- Word for word plagiarism, literally copying parts of someone else's work without indicating this. This happens when a student reproduces phrases from someone else's work without using quotation marks. If the original author is not mentioned either, this can also be called plagiarism of ideas.
- Plagiarism of sources, copying citations from another author without mentioning that the citations were brought together by him. A more serious form is when the references are simply copied, while the publications were in fact not read by the new author at all. This form is often found in conjunction with the previous two.
- Plagiarism of authorship, which involves claiming to be the author of a whole work that was in fact written (at least for a substantial part) by someone else. This happens when a student copies (important parts of) a thesis, written by a fellow student (possibly in another university). But it is also possible that a student pays someone else to write the work for him, which falls into the same category.

Of these, word for word plagiarism is usually the easiest to identify. Information technology can be of assistance here, as will be discussed in the next paragraph. Unfortunately, students are increasingly aware of that and in response attempt to mask their copying activities, for instance by substituting synonyms for certain terms or by rearranging the words. They are often surprised when they learn that even the copying of ideas can already be plagiarism.

---

[2] Martin, B., *Plagiarism: policy against cheating of policy for learning?*, University of Wollongong 2004, p. 2-3.

Plagiarism of authorship has been in the news recently[3] because it is exploited commercially nowadays. On internet sites such as www.ukessays.com, tailor-made essays and dissertations can be ordered by everyone willing to pay for them. These sites officially do not advocate plagiarism (in fact they guarantee the originality of the essays they sell!), they state that the texts can be used as examples, or to improve the contents of the work the student has written himself. But if students feel the same about this remains to be seen. That they would be willing to pay £ 400,- or more for something they only use 'as an example' seems unlikely.

This example clearly illustrates that it is absolutely necessary to monitor student activities these days, such as the production of essays and other assignments. IT provides students with new tools and options, many of which can be used in fraudulent actions. As educational institutions have an important responsibility to make sure that students who graduate indeed possess the required knowledge and skills, they must take action.

This responsibility of educators has a wider significance than just the reliability of the diploma and the reputation of the institution providing it. Unqualified professionals could easily inflict major damage. Therefore, certifying that future engineers, doctors and lawyers are indeed qualified is in the interest of society as a whole and has a clear relationship with public safety and security as well.

3. Information technology as source of problems

Information technology (IT) plays an important role when dealing with plagiarism and fraud nowadays. To students, it provides the tools to copy and paste large amounts of text or other data almost effortlessly. The results of this are noticeable at all different educational levels. For instance in first-year education, where in a recent take-home assignment at the School of Law, Erasmus University Rotterdam, more than 10% of all students were found to have copied each others work (word for word plagiarism). But even at the graduate level, a number of Master theses were identified as complete copies of someone else's work in the past few years (plagiarism of authorship).

The scale on which copying can now take place has also grown tremendously by the use of information technology. The internet can serve as a global source of almost unlimited size. Furthermore, when suitable source materials have been found, IT can provide tools to mask the copying. For instance, word processing functions and automatic synonym substitution or (in case of graphics) tools to remove author-specific elements in pictures can be used.

[3] For instance Taylor, M. and Butt, R., 'How do you make £1.6m a year and drive a Ferrari? Sell essays for £ 400', The Guardian, July 29 2006.

4. Using information technology to fight plagiarism

IT can play a role in fighting plagiarism and fraud as well, however. Tools exist to identify fraudulent work in several different ways. Three main categories can be distinguished.

- Checking student work 'externally', i.e. comparing it with every other available piece of work.
- Checking student work 'internally', i.e. comparing it with the work of fellow students who did the same assignment or examination.
- Checking the 'consistency' of the written work by a certain student.

4.1. External checking

To check student work externally, a basic requirement is that all documents (both the student work and the external work) are available in electronic form (a computer file). For assignments and 'take home exams' this is usually not a problem nowadays. Most students use word processing software for the production of any substantial piece of text anyway. For most written examinations, taken by groups of students in examination rooms, however, the use of computers to type the answers is still rather uncommon.

External checking typically involves a comparison of the student work with either all documents that are available on the internet (an 'unlimited check') or with a particular subset of these (a 'limited check'). The simplest way to achieve an unlimited check is by using an internet search engine such as Google or Yahoo. An advantage of this approach is that no special software or license is necessary. The precision[4] of a general internet search operation is usually low, however, which means that a considerable number of documents must be opened and inspected manually. Furthermore, a disadvantage is that only generally accessible or 'open' sources can be searched in this way. Copying from commercial databases, to which students often have access because their institutions hold a license, therefore remains unnoticed when using general search engines.

Commercial plagiarism detection services, a number of which have emerged in the past few years, often do not have that drawback. These services tend to operate on a subscription basis; if an institution wants to make use of it, it has to pay an annual fee and sometimes also a fee that is dependant upon the amount of requests. In return, the services offer some advantages, such as:

[4] The precision of a search operation is in this case defined as the ratio of the number of useful documents (documents from which parts were copied) divided by the total number of documents that were retrieved, Salton, G., *Automatic Text Processing, the Transformation, Analysis and Retrieval of Information by Computer*, Massachusetts: Addison-Wesley 1989, p. 248-249.

- the possibility of searching in certain 'closed' data collections, such as commercial databases;
- the possibility to include certain 'private' document collections (such as sets of student assignments) in the search operation;
- the option to operate interactively (for a single file) or to process batches (for a whole set of assignments, to be checked overnight).

Examples of commercial services are SafeAssignment (www.mydropbox.com), Turnitin (www.turnitin.com), Urkund (www.urkund.com) and Ephorus (www.ephorus.nl). Although all of these services are relatively user-friendly, the procedure to check one or more documents varies considerably. Some services depend almost completely on e-mail for file uploading and for the reporting of results, which can be problematic when larger numbers of files are involved. Other services can only be accessed through a 'Network Learning Environment' (NLE) such as Blackboard (www.blackboard.com). At the Erasmus University, where the authors of this paper do their work as teachers and researchers, this is the case with SafeAssignment. To use this plagiarism detection system, the Blackboard user interface must be used, which still a lot of teachers are not familiar with. As it seems, there is not a single system that is fit for every purpose. A teacher should make his own choices, based on the intended use.

A characteristic these services share with software that performs 'internal' checking is that in fact only *similarities*[5] between documents are identified and reported. It is always the teacher who has to decide whether these common phrases (or perhaps paragraphs, or even pages) constitute plagiarism or not. Basically, similarity between documents (available in electronic form) can be calculated completely automatically from for instance the *word use* in the documents. How this can be achieved is explained in the next section, parts of which are based on [Van Noortwijk & De Mulder 1997].

4.2. Calculating Similarity

The simplest method to calculate the similarity of two documents utilizes just the presence or absence of word types[6]. This method will be described here. A more sophisticated approach could also take into account the frequency of a word type within each document. With the simple method, only the number of documents in which a word type appears plays a role. This characteristic, the 'document frequency', has a strong relation to the dispersal of word types over the documents.

---

5 See for example Meadow, Ch. T., Boyce, B.R & Kraft, D.H, *Text Information Retrieval Systems*, San Diego (Ca): Academic Press 2000, p. 221-224 and Noortwijk, C. van & Mulder, R.V. De, 'The Similarities of Text Documents', in: *JILT – Journal of Information, Law and Technology*, Issue 2/1997, Coventry: University of Warwick 1997.

6 Word types are the different words used in a certain document, also referred to as the vocabulary in that document. The term word token, on the other hand, is used to indicate one occurrence of a certain word type.

When we determine the similarity of two documents by means of the word types present in these documents, two situations seem to be possible at first sight:

- a word type is present in both documents; because this means that the documents have a common characteristic, it should increase similarity. For this situation the term 'hit' has been introduced.
- a word type is present in one document, but not in the other; at this point the documents differ from each other and therefore similarity should decrease. This situation is called a 'miss'.

The 'misses' in fact come in two different types. With two documents X and Y there could be

- a 'type 1 miss' (in short, 'miss1') if a word type is present in document X, but not in Y; and there could be
- a 'type 2 miss' (in short, 'miss2') if a word type is present in document Y, but not in X.

With these three characteristics, the number of hits, miss1's and miss2's, the relationship between two documents can be effectively established. However, when the documents do not stand on their own but are part of a database containing many other documents, there is a fourth characteristic. The other documents will probably contain quite a number of word types which are neither present in document X nor in Y. The absence of such a word type in both documents can even be considered a point of *resemblance*, which should increase the similarity of the documents. Therefore, this is also a kind of 'hit', just like in the situation where a word type is present in both documents. This means that next to two types of misses, two types of hits are also possible:

- a 'type 1 hit' (in short, 'hit1') if a word type is present in both documents; and
- a 'type 2 hit' (in short, 'hit2') if a word type is absent in both documents, but is used in other parts of the database.[7]

The number of documents in which a word type is present (the 'document frequency' of a word type[8]) differs from the number of documents in which other word types appear, this can have an influence on similarity. For the probability that a word type with a high (document) frequency is present in a certain pair of documents, and therefore is responsible for a 'hit1', is much higher than the probability that this happens with a low frequency word. Conversely, the probability of a 'hit2' is higher with word types of a low frequency. For the two types of misses an analogue conclusion can be drawn.

---

7 See for example Batagelj, V. & Bren, M. *Comparing Similarity Measures*. University of Ljubljana, Ljubljana 1993.

8 As this 'document frequency' is the only frequency considered here, from now on we will refer to it simply as 'frequency'.

That means that not every hit or miss can be considered to be of equal significance. When a word type with a frequency of only 2 (when the number of documents is high, say 20000) is found in a pair of documents, this gives us much more information than when a high frequency word type (for instance 'the', 'it', etc.) is found, and the similarity of the documents should therefore increase more in the first situation than in the second. This means that we have to take into account the probability that the hit or miss occurs in a certain database. The probability to *encounter* a word type is equal to the (document) frequency of the word type divided by the number of documents in the corpus. The probability to *miss* a word type is equal to the difference between the number of documents and the (document) frequency of the word type, divided by the number of documents in the corpus. The weight (indicating the significance) of a hit or miss of a certain word type is the complement of this probability (1-P(i)). Using these weights, the similarity between two documents could be calculated by adding the weights of the word types that constitute a hit1 or a hit2 in this particular document pair and subtracting from that the weights of the word types that constitute a miss1 or miss2. As not all documents are of equal size, however, these added weights of hits and misses should be made relative to the *maximum* weights that could have been achieved with that particular document, i.e. to the total weight of all words present or absent in it, respectively. A relatively simple similarity score, taking into account just the hits,[9] could then be calculated in the following way:

$$S = \frac{\sum_{i=1}^{m}(1 - P(i_{hit1})) + \sum_{i=1}^{n}(1 - P(i_{hit2}))}{Hit1_{\max} + Hit2_{\max}}$$

where m stands for the number of hit1s, n for the number of hit2s, P for the probability that a particular word i constitutes a hit1 or a hit2, respectively. $Hit1_{\max}$ is the maximum total hit1 weight for a particular document (= the total weight of all word types present in it) whereas $Hit2_{\max}$ is the maximum total hit2 weight (= total weight of word types absent in it). For more information on this, see Van Noortwijk & De Mulder 1997.

For a set of documents, this can lead to a series of similarity scores for every possible combination of two documents (i.e. every document pair) from the set. The highest ranking pairs, or pairs of which the score exceeds a certain threshold value, are candidates for closer inspection by the teacher. To support this inspection, some plagiarism detection services provide reports that list the common characteristics or highlight these in the original documents. This can speed up the process of assessing similar documents considerably.

---

[9] In fact, misses *are* taken into account here, as they influence the relative values; see Noortwijk, C. van & Mulder, R.V. De, 'The Similarities of Text Documents', in: *JILT – Journal of Information, Law and Technology*, Issue 2/1997, Coventry: University of Warwick 1997, p. 8.

Even with sophisticated report generation, however, assessing the originality of a set of, say, 400 documents can be quite a task. In such a set, it is not uncommon that 20 to 40 document pairs are reported as containing suspicious similarities. This means that the teacher must (re)read and compare 40 to 80 student assignments. If plagiarism is indeed confirmed, follow up must be given to this (for instance in the form of messages to students or to the examination board), which again could take a considerable amount of time and has other drawbacks as well, as will be discussed in section 5 of this paper.

4.3. Internal checking

For the internal checking of documents, IT can again only play a role if all documents are available in electronic form. When this requirement is met, the documents can be compared using a 'plagiarism detection' or 'fraud finder' program installed on a local PC. An important advantage of such a program is that, when a license for it has been obtained, usually no subscription to any commercial service is necessary. The software can be used for an unlimited number of checks, until the licence expires.

Programs that perform internal checking are usually intended to be used on a 'closed' group of documents, for instance all completed student assignments from a particular course or part of a course. Actually, this can be an advantage for the detection of similarities. This is because in a closed set, it is possible to take into account *omissions* of certain words (i.e. a word is not used in the two documents that are compared, but is present in other documents). As is explained in [Van Noortwijk & De Mulder 1997],[10] such a word that is omitted in two documents can be seen as a point of resemblance, which should increase the calculated similarity score. Including this characteristic when calculating a similarity score usually improves results considerably; documents with identical parts get relatively higher scores which makes it easier to distinguish them from the rest. This is especially true if all documents are of more or less equal size (as is often the case with for instance student assignments). When document size differs a lot, however, calculating similarity from just the common (present) words could yield better results.[11] Having the possibility to choose one of these (and possibly also other) options while determining similarity and to observe which one works best can be a considerable advantage.

Several software packages are available to perform internal document checking. Examples are WCopyfind (www.copycatchgold.com), Pl@giarism (www.plagiarism.tk) and Codas Fraud Finder (www.andromatics.com). Some of

[10] Noortwijk, C. van & Mulder, R.V. De, 'The Similarities of Text Documents', in: *JILT – Journal of Information, Law and Technology*, Issue 2/1997, Coventry: University of Warwick 1997, p. 4.

[11] Noortwijk, C. van & Mulder, R.V. De, 'The Similarities of Text Documents', in: *JILT – Journal of Information, Law and Technology*, Issue 2/1997, Coventry: University of Warwick 1997, p. 8.

these programs are offered free of charge (sometimes with certain limitations, or for an evaluation period). They usually have a graphical user interface and are easy to operate. Using this kind of software is therefore one of the easiest countermeasures against unauthorised copying within a group of students.

4.4. Consistency checking

One major drawback of both external and internal plagiarism checking is that the original work must be available for comparison. But what if a student copies substantial parts from a book that is unknown to the teacher and has never been published in electronic form? This type of plagiarism is difficult to detect using the techniques described in the previous sections.

There is another option, however. A student who copies substantial amounts of text from external sources (i.e. written by others) mixes his own style of writing, word use etc. with that of other authors. This means that a number of characteristics of the language in the new text will be different from those in other texts produced by the same student. This difference can be detected. Several techniques to accomplish this have been developed in the past decades, for instance in order to find out if a particular text could be attributed to a certain author. Several researchers[12] have used *word frequency* data from texts that were already known to be written by a certain author to construct a unique 'fingerprint' of that particular author. The same can be done for other texts (for instance, texts of unknown origin). When the key characteristics match, the texts can be attributed to the respective author.

To apply this principle in education, databases containing a broad selection of earlier work of each individual student must be compiled. One way to establish this is to make use of electronic 'portfolios', in which every piece of written work of a particular student is stored from the moment he commences his studies until the moment he leaves the institution. This material is usually well suited to construct a 'fingerprint' from, which can then be compared to that of any new production. The more documents the portfolio contains, the more reliable the fingerprint will be. Of course, to most teachers this is not an entirely new technique. When they know their students well, they tend to 'feel' that something is wrong if a mediocre student hands in productions that considerably exceed his usual level. Using a computer to compare linguistic fingerprints, however, makes it possible to apply the method with more precision and in educational situations where the number of students is too high to know the individual work of each of them.

---

[12] For instance Ellegard, A., *A Statistical Method for Determining Authorship: The Junius Letters 1769-1772*, Gothenburg Studies of English no. 13, Gothenburg: University Press 1962 and Kenny, A., 'A stylometric study of Aristotle's Ethics', in: Lusignan, S. and North, J.S. (eds.), *Computing in the Humanities*, Waterloo, Ontario: University Press 1977.

5. Conventional measures against plagiarism

Even though technology brings us powerful new tools to fight plagiarism, conventional measures against this undesirable phenomenon are still just as important. This is especially true in education, as discussed in this paper. It is vital that students are taught the importance of producing their own, original work and the need to handle sources correctly. As stated earlier, certain forms of plagiarism are far from obvious to many students. Therefore, they could apply these forms unintentionally, unless taught otherwise.

Therefore, plagiarism should be a subject that is dealt with explicitly, starting from the first year of education. The different forms of plagiarism and the ways to avoid them should be explained. Furthermore, students should be taught the guidelines for the proper acknowledgement of sources, using a generally accepted method. Using plagiarism detection software can then be a logical complement to this education. It can be used to check that all students have understood and implemented the guidelines correctly. If done in this form, students will probably accept it more easily, as they will recognise that everyone is treated equally in this respect and that only original work is accepted and rewarded.

Another important reason to take plagiarism seriously and to counteract against it is the fact that the institutional reputation depends on it. If standards for student work are maintained, this reputation will be reinforced. Students who have become used to this, will probably see this advantage as well, and hopefully will communicate this point of view to other, for instance first-year students.

This approach, which puts emphasis on alerting and prevention, is preferable to one that mainly focuses on repression not only from the educational point of view, but for practical reasons as well. For detecting that students have cheated is one thing, but proving it beyond doubt and documenting it in such a way that it will hold in appeal procedures – and even in court, if a student wants to take it that far – is a lot more difficult. For a student, a lot can be at stake when he or she is accused of fraud, which makes it appealing not to acknowledge the copying, but to deny everything. Appeal procedures, especially external ones, can be costly and time consuming for both parties and could damage the institution's reputation. Furthermore, proving that a student has copied work of others can be difficult, even in seemingly clear cases, as there is always the possibility that the similarities are caused by discussions between students that are, in themselves, allowed.

Conclusions

As has been argued in this paper, plagiarism is a serious problem in modern education. Information technology makes it easier for students to find and copy work of others. Many students are so used to looking up information on the internet, that they do not even realise that what they find should not just be copied, but should be properly acknowledged as work performed by someone else. While in High School, many were even praised for handing in extended project reports containing lots of copied material. For these students, making them aware of the problem and teaching them the right methods might suffice. But those who deliberately copy the work of others and present it as their own should definitively be identified and helped to end this behaviour.

Fortunately, IT can play a role to counteract against plagiarism as well. Several tools exist, to compare student work with external sources (documents available on the internet) as well as with internal sources (essays or assignments from other students in the same group). The effectiveness of these tools differs, as it depends on the number and the quality of the sources that are used for comparison. Internal checking can be very effective in a closed group, for instance to check the originality of take-home assignments.

Teaching students not to plagiarise and educating them to use sources properly should of course lay the foundation. But to make sure that they have understood the lesson and really do not cheat, technical means have in fact become indispensable. These tools should be embedded in the whole institutional policy against plagiarism and fraud. Doing so is vital to the reputation of the institution and to that of students.

Safe and trustworthy access in a working environment: the MoodlePKI Project

L. Catalinas, F. Galindo & P. Lasala [1]

Abstract

We set out in this paper the possibility of using the Internet to satisfy two basic requirements: (1) the publication of information that its creators wish to be present on the Internet and to be freely available to all interested users, and (2) respect for the wishes of those who want information to be accessible and usable in particular ways for different groups of people. In order to exemplify these potentialities, the design and test of a website (http://www.lefis.org) has been carried out, with the help of cryptographic access techniques, in particular, a public-key infrastructure. Both the possibility of supervising and guiding access to information on the Internet, and that of safeguarding fundamental rights such as freedom of speech, freedom of access to information, data protection and information security have been illustrated in this way.

1. Introduction

The Internet is an especially appropriate environment for presenting information, opinions and knowledge about any matter. It is perhaps no exaggeration to assert that the Internet is progressively becoming one of the ultimate communication channels.

This characterisation requires us to recognise that in the publication of information, opinions and knowledge via the Internet, just as in the case of publication by other means (the press, television, books and documents in paper format), the rights that are attributed to the originators and receivers (authors and readers) of information in democratic societies must be respected. The rights of citizens to be respected are those related to the handling of their personal data and the rights that citizens 'transfer' by means of constitutional documents to public authorities. Those authorities must preserve the personal security of all citizens; and citizens' beliefs, no matter what those beliefs may be or what view of reality particular citizens may have, provided that they do not violate the Declarations of Human Rights, must also be safeguarded.

[1] University of Zaragoza, Spain. The research supporting this paper is financed by the Spanish Ministery of Education and Research, Project 'Governance and regulatory strategies in the knowledge society' (SEJ2004-00747), and by the European Commission, Socrates Thematic Network Legal Framework for the Information Society (225990-CP-1-2005-1- ES-ERASMUS-TN).

This implies that we must recognise that freedom of speech, and the control or supervision of ideas expressed on the Internet or by any other means, may be compatible rather than contradictory principles, as opposed to what the use of certain techniques that facilitate the use of the Internet seems to suggest.[2] The LEFIS public-key infrastructure provides a practical example of the possible compatibility between freedom of speech and control or supervision mechanisms on the Internet,[3] as we shall show in this paper.

The Legal Framework for the Information Society (LEFIS) network is an organisation of universities, companies, public institutions and private organisations, located in Europe, South America, the United States and Russia, that, with participation by its members, is developing content of a certain type (a didactic model). At the same time, it is producing teaching materials and conducting research and development projects, focused on proposing juridical solutions to problems originating in the information society. The LEFIS network uses the Internet as a tool to develop and communicate its proposals. Its members use the Internet to communicate with each other and to work on joint projects; they also use the same means to make public their conclusions.[4]

To this effect, a website (http://www.lefis.org) makes known the composition of the network (members, addresses, occupations, …) and the results of, advances in and content of their work, which is expressed in a standard programming format that allows the use of Moodle. Moodle is a tool dedicated to distance learning, and for this reason is of particular interest for the communication and joint work carried out among the LEFIS members, who are working in all of Europe, mainly on models and concrete teaching content in the area of the regulation of the information society. At the same time, this content is especially appropriate for demonstrating and reflecting on what public-key infrastructures allow: the delimiting of the rights of access to and of contribution of content, for those who are integrated into the LEFIS network and for other interested parties who are participating or merely wish to know about the activities of LEFIS. It is for this reason that, given the characteristics and objectives of the Internet,

2 "What is special about the Internet is the way it mixes freedom with control at different layers. The physical layer of the Internet is fundamentally controlled. The wires and the computers across which the network runs are the property of either government or individuals. Similarly, at the content layer, much in the existing Internet is controlled. Not every thing served across the Net is free for the taking. Much is properly and importantly protected by property law". Lawrence Lessig, The future of Ideas, New York , Vintage Books, , 2002, p. 25.

3 It is an ideal proposal to generalize the use of the PKI. See: Lawrence Lessig, El Código y otras leyes del ciberespacio, Madrid, Taurus, 2001, p. 86.

4 From a political perspective the purpose of LEFIS is to build, with moderation and in the limits of the objects of discussion, some kind of "discursive' procedures" to make "egalitarian decisions dependent on prior argumentation (so that only justified decisions are accepted); they are furthermore inclusive (so that all affected parties can participate); and they hold the participants to assume each others' perspectives (so that a fair assessment of all affected interested is possible)". Jürgen Habermas, "The Kantian project of the constitutionalisation of international law, does still have a chance?", in Law and justice in a global society, Granada, Anales de la Cátedra Francisco Suárez, 2005, p. 126.

LEFIS provides a good example of what we wish to demonstrate in practice here: the possibility to make freedom of speech and control or supervision of activities on the Internet compatible.

We present the following items in this paper. In section 2, the work environments required on the Internet to place and gain access to information are exemplified, satisfying requirements aimed at guaranteeing the security of information in general on the Internet and of access to that information, and at guaranteeing freedom of speech . In section 3, the work environment chosen in LEFIS to present and provide access to information generated by the network, using the possibilities offered in this respect by public-key cryptography, is specified. In section 4, the form in which information is presented and organised using Moodle, an especially appropriate tool for use in the academic environment, is summarised. In section 5, some new steps to be taken in the development of the network, in relation to the establishment of security measures, are outlined. Finally, some conclusions are presented.

2. Working environments

When we want safe and trustworthy access to a working environment on the Internet, there are three problems to be solved:

1. The server must know who wants to be connected: to read information, to download files, to put news up, to upload files, etc. This is the *user identification problem*.
2. The users must know that they are really connecting to the correct server: they must be sure where they are uploading their documents to and where they are downloading information from. This is the *server identification problem*.
3. The communications between the users and the owners of the information on the Web must be guaranteed to be secure. This is the *communications security problem*.

2.1. Solutions to the user identification problem

Information on the Internet may be open to all users interested in it or only to certain users. In the first case it is not necessary in general to have explicit user identification, that is, to require users to give their forename and surname or their email address. The operation of the Internet ensures that, in general, the IP (Internet Protocol) address, the number that identifies the particular computer from which a visit to any given Web page is made, is recorded in the registration system of the server (the computer that holds the page that is open to all users of

the Internet). On the LEFIS website, information about accesses to pages is given publicly, at addresses that provide statistics about those accesses.[5]

The administration of LEFIS does not carry out verification of the identity of the holders of the computers whose IPs are recorded in these statistics. On the other hand, the possibility of consultation of these statistics is open to all users of the Internet who want it, which reminds users that, as soon as the statistics are located on secure pages (https), it will be possible to know the IPs of those who have carried out such consultation. The administration of LEFIS does not in fact make use of this last virtuality.

In the case where access to information is restricted to certain users, several identification systems exist. The most commonly used are those that require a username and a password, which are provided by the manager of or person responsible for the information system, to allow access to the information system. In such cases, the identification is clear and direct, unless someone impersonates the holder of the username and the password by using both.

It is for the latter reason that in many environments, authentication systems based on the username/password pair are insufficient and do not really guarantee the user's identity (e.g. workers may use the usernames of others for convenience, there may be shared access, etc.). Furthermore, on many occasions, those simple authentication systems are used on insecure communication channels (HTTP), using neither authentication nor encryption. In these situations, it is very easy to 'hunt' for usernames and passwords. Having the necessary technical knowledge (it is not necessary to be an engineer; knowing how to use a program is enough)[6] and being in the appropriate place is enough to carry out this 'hunt'. In contrast, the use of identification systems based on public-key cryptography gives enough guarantees, at least for the moment, about user identification.

No less important than knowing with security the user's identity is to set down the operations that the user will be able to carry out and what resources the user will be allowed access to. This is performed by means of ACL (access control list) systems implemented in applications to help to distinguish types of users (anonymous and identified, for example), operations that they can carry out (reading of information and modification of that information, for example), and resources that they can access (informative pages, generic databases and personal databases, for example).

5 There are two addresses: https://admin.lefis.org:446/awstats/ and https://admin.lefis.org:446/webalizer/.

6 If you are interested, you can try searching with Google on terms that identify suitable programs, such as 'dsniff', 'sniffit' or 'ethereal'.

2.2. Solutions to the server identification problem

This is the problem of knowing that one is accessing the 'correct' server, that is, the computer where the information is stored and accessed via the Internet. The current avalanche of 'phishing' attacks demonstrates that confusion is very easy. These 'phishing' attacks are aimed mainly at banks, but can be easily extended to any other environment; their intention is to lead an Internet user to a falsified destination, different from that which the hyperlink apparently shows,[7] with the purpose of obtaining information from the user that allows a third party, the sender of the false e-mail, to impersonate a legitimate user in order to gain access to the correct server and to carry out bank transactions, for example, that a legitimate user can carry out.

A server, service or system in general that works with authenticated users should always be identified with sufficient technical and legal guarantees. These should not leave any space for doubt, but at the same time they should be easy to use and to interpret by the average user. This can be achieved by means of cryptographic public-key techniques, specifically, a public-key infrastructure (PKI).

2.3. Solutions to the communications security problem

To establish an appropriate work system in the Internet environment, it is necessary to add to the above-mentioned requirements that a system, which allows access to authenticated users and allows them to carry out data creation and modification operations should offer guarantees that the modifications have been carried out in a legitimate way. That is, there should be no doubt about who the author of the modifications is; this can be guaranteed by means of the concepts of authentication and non-repudiation offered by the technique of digital signatures.

Besides the above requirement, the issue of data privacy must be addressed. It would be ideal if, in a support system for group work, it was possible to send information to other collaborators or leave information for them in such a way that only they could make use of it; and even more, that these data could be published or sent through insecure channels (web, e-mail, …) with the reassurance that only the legitimate recipients could interpret them. This is technically possible also, through the use of public-key cryptography.

7 This is possible because of bugs in Web and email applications and the use of HTML and Javascript in emails.

3. The LEFIS working environment

The principles set out above in section 2 are being put into practice in LEFIS. We describe in this section the methods to ensure safe and trustworthy access to the LEFIS website that are under development at the moment and have been partially implemented.

3.1. User identification

The server allows anyone to navigate through the Web pages, but it will only let LEFIS members access restricted zones. LEFIS members must be identified with LEFIS digital certificates. As has been said before, the simplest solutions (such as the username/password pair) are the simplest to implement and use but they have problems (it is easy to use another person's identity). It is better to use another solution, such as authentication access using digital certificates; and better still if cryptographic and biometric devices are also used, for convenience and security. LEFIS uses cryptographic devices only, for the moment. The LEFIS certificates are generated and negotiated by our own PKI, which offers us a very high level of control and flexibility inside our own organisation, without depending on anyone else. We have also performed tests that have correctly identified external certificates to the LEFIS PKI, although this functionality will not be implemented until a later phase.

A PKI public interface exists, where the effective and revoked certificates, as well as the certificate revocation list (CRL), are published and can be downloaded. Through the public interface, any LEFIS member can request a certificate. The generation of keys is carried out on the user's own system in a secure way; the Spanish LEFIS members can even use cryptographic devices for key generation homologated by FNMT-RCM and CERES, the public certification authority authorised by the Spanish government.

The identity verification tasks for an applicant for a certificate are carried out by a specific application, the registration authority (RA), and by qualified personnel (RA operators), to decide whether a request is accepted. The operators apply the LEFIS certification policy, which specifies the procedures to be followed. The function of digitally signing the approved requests (once the applicant's identity has been checked by the RA) is carried out by another specific application, the certification authority (CA), and by a technician (the CA operator), who verifies the correctness, at a technical level, of the request and generates the certificates and the CRL, following the LEFIS certification policy. Once the procedure has been completed correctly, the certificate is sent to the user, already signed, by e-mail and is incorporated into the list of valid certificates in the public interface. When the user receives this e-mail from the LEFIS PKI server, he/she only has to click on a link and the LEFIS certificate will be installed automatically in his/her computer browser.

These advances have been possible because we had already developed, by the beginning of 2005, a modified version of our intranet (an application web programmed in Java) that was able to identify users through digital certificates from the LEFIS PKI. Initially, the intranet allowed access with a username and password. With the installation of the PKI version of our intranet, users can enter in a more secure way and without having to remember passwords, because they are recognised automatically on the basis of their LEFIS certificate. We have made successful use of cryptographic devices, namely CERES smartcards; we have also performed tests with eTokens, which we discarded because they were much more expensive. At the moment, we are investigating the possibilities for using the Spanish @firma and DNI-e projects with our platform.

3.2. Server identification

In order for LEFIS members to know that they really are working with the LEFIS server, the LEFIS server has a digital certificate from our own PKI, and the communications are encrypted to ensure users' privacy (with secure protocols such as https) and to safeguard them against spying attacks (which are easy to carry out for a technician with a 'sniffer' utility). LEFIS members can know in this way that they really are working with the LEFIS server. They need only to install in their Web browsers the APTICE and/or LEFIS certificates to be used as certification authorities. If they do not do this, an error occurs in the browser, warning that it does not trust the CA that has signed the certificate of the site.

3.2.1. The LEFIS PKI

The LEFIS PKI has an internal or private character, that is to say, it is not designed so that everybody trusts it automatically. To be able to trust and to operate correctly with the PKI of LEFIS, it is necessary to carry out a simple operation: to install the certificate of the APTICE or LEFIS CA.

To meet legal requirements and for reasons of technical flexibility, we decided not to create a simple autonomous PKI but to go a little further, and created the certification authority of a legal entity, APTICE (ca.aptice.es, www.aptice.org). The APTICE CA has the ability to sign CA (or SubCA) certificates that can be used to create complete, functional PKIs in a more flexible and secure way, such as the LEFIS PKI and others that we can create to implant PKI in other organisations.

Therefore, the best solution for a user who wishes to trust the LEFIS PKI is to install the APTICE CA root certificate; this provides enough guarantees to establish the root trust and to certify the CA of the LEFIS PKI, in order to lay the foundations for trust in its PKI environment.

3.2.2. Technical characteristics of the PKI

The PKI uses the standard X.509v3 architecture for certification authorities and registration authorities, with separation of the signature and verification functions, the management of digital certificates, and the certification revocation list. Public-key encryption with the RSA algorithm allows the use of encryption and digital signatures. The LEFIS PKI was built using open-source software (adapted to our needs by modifying source code), attending to the need to provide these characteristics and functions:

- use of Linux as the operating system;
- use of Apache as the Web server, with SSL;
- use of OpenCA for the PKI;
- use of OpenSSL as the SSL engine (for cryptographic libraries and extensions);
- use of Java and Perl as programming languages;
- interoperability (information interchange among applications from different sellers by means of a standard);
- cross-certification (we plan to be able to identify users in the future with certificates that come from other certification authorities);
- design of the PKI using a hierarchical structure.

3.2.3. How to get a LEFIS certificate

LEFIS members can enter http://pki.lefis.org and choose the 'PKI Sign Up' option in the left menu. There are several options for generating a certificate sign request (CSR):

- For first-time users, we advise them to read the detailed guide to completing the sign-up process.
- For non-first-time and advanced users, they can go directly to the 'CSR Generation Wizard' option. On choosing this option, users get a user-friendly Web interface, adapted for the LEFIS network. The key generation process is done on the user's computer so that the keys do not travel through the Internet. This is the most secure way.
- There is also a guide for users who have a CERES cryptographic device (available only to Spanish users), which details the process of generation of a CSR with an RSA key pair inside this cryptocard[8] for great security of key protection. Furthermore, using these cryptocards allows LEFIS PKI users also to store other personal certificates, such as the FNMT Personal Certificate, in the same card and use them on many computers, without the

8 Smartcards are a kind of microcomputer, able to perform cryptographic operations and store keys protected by integrated hardware/electronic security measures.

need to install their certificates in those computers. Obviously, this is more secure and convenient.

The LEFIS PKI is based on a multiplatform system, compatible with the PKI-X standard X.509v3, although we use only Internet Explorer in Windows XP at the moment, to avoid support work.

3.2.4. What does the user get with a LEFIS certificate?

Users who have a LEFIS certificate installed have identified access to LEFIS Web resources, documents and e-mail digital signatures, and are able to use public/private keys to sign and/or encrypt documents on their own computers, if they are interested.

3.3. Communications security

The documents and resources uploaded to and downloaded from the LEFIS website can be digitally signed to ensure their integrity and legitimacy, and to detect illegitimate handling of LEFIS documents. Since we have fully functional and compatible digital certificates, we have the capacity to work with digital signatures using applications that allow it, namely Microsoft Office 2000 and OpenOffice.org 2, Adobe Acrobat 6 and newer versions; also, for Spanish users who have CriptoKit FNMT-RCM, it is possible to sign/encrypt any file with the utilities that it installs. We also have the capacity to publish all the LEFIS documents (in supported formats) with a digital signature. This can be the digital signature of the person responsible or of the editor of the document (a LEFIS member certificate); later, this could be a component digital signature (a certificate installed in a program on the server that signs files automatically).

In a later phase, we shall integrate into the LEFIS website some options (Java applets) that will allow users to sign files digitally on their own computer and to send them to the server, to store them already signed. This covers a very important field in which we have not yet worked. Some similar functionalities exist in the Spanish @firma platform and the DNI-e project that we are studying, with the intention of making use of them to create compatible and interoperable systems.

4. The MoodlePKI Project

The Moodle tool is the mechanism used by the LEFIS network to present the information and knowledge whose study and design it is in charge of. Moodle has functionalities very near to the satisfaction of the immediate needs of the LEFIS project: to develop models and content that can be used for teaching purposes. In this section, we summarise the main functionalities that Moodle provides for LEFIS from the point of view of PKI technologies.

4.1. Characteristics

The LEFIS website is being built using Moodle. We have called the development process the MoodlePKI project, because the main goal is to integrate PKI technologies with the Moodle environment. Moodle is an acronym for 'Modular Object-Oriented Dynamic Learning Environment'. It is an open-source e-learning platform that we are adapting to support the activities of work groups, dynamic content and other functionalities for the LEFIS network.

4.2. PKI functions

To integrate PKI technologies into the LEFIS–Moodle environment, we are working in three ways in relation to Moodle:

1. In order that the server should allow access to only LEFIS members, the solution chosen is the following:

- An external validation component (a Java Web application) able to obtain a digital-certificate request from the user over a Web connection (https) and to check its PKI validity. This validation component plays the role of an interface between Moodle and the PKI, and is being developed in Java for maximum flexibility.
- A new authentication module for Moodle written in PHP (the programming language in which Moodle is written) that validates users against the LEFIS PKI using the above validation component.

Moodle is designed to support multiple authentication mechanisms of very different nature (username/password, POP3, ldap, etc.), and does not only support them by default incorporated mechanisms. It has been possible to develop a new authentication module adapted to our PKI to identify users via their digital certificates. This proves that the possibility of modifying software to adapt it to concrete needs without being tied to a specific company is one of the many advantages of free software.

2. In order that LEFIS members should know that they are really working with the LEFIS server, we have generated a digital server certificate with our own PKI for www.lefis.org (cheaper and more flexible than a server certificate from a recognised CA during the development phase). We plan to purchase a public CA signed Web server certificate for the www.lefis.org site for use in the production phase.

3. To ensure that the documents available from LEFIS are those which the LEFIS members originally generated, the solution adopted is that we shall

provide LEFIS members with digital user certificates, which also will allow them to carry out digital signing of objects such as documents (in supported formats), besides Web authentication, email signing, etc.

5. Future extensions

Once the basic nucleus of applications or programs has been developed that allow the identification of users and of the server and guarantee that various sets of people can gain access only to the information assigned to them on the LEFIS website, we shall immediately carry out work on developments and applications.

The efforts will be focused on the following aims:

- to simplify and polish the working systems;
- to allow limited access to the personal databases of LEFIS members;
- to allow limited access to the teaching material developed by the LEFIS members;
- to try to ensure that validation of the public-key certificates issued by the APTICE and LEFIS certification authorities is carried out by an agency of the Spanish government.

5.1. Personal databases

The MoodlePKI applications developed so far allow users to obtain public keys and corresponding certificates through the procedure presented above in section 3. By means of these certificates, it is possible to access documentation on the LEFIS website that cannot be consulted without having these certificates. This information is, at the moment, the chapters of a book *Gobierno, derecho y tecnología: las actividades de los poderes públicos* (*Government, Rights and Technology: the Activities of the Public Powers*), located on the LEFIS website. The access security mechanism developed ensures that only the authors of the book chapters are able to access this content; they need to have the public key, issued for them by the LEFIS certification authority, installed on the computer from which they carry out the query.

The next step is to allow access, by means of LEFIS certificates, to personal information collected in the LEFIS database of members, stored on the computer dedicated to the administration of the project. This personal information is composed of a forename, last name, electronic mail address and other personal data stored in the LEFIS database; this information does not have the character of public information, nor is it accessible on line through the Internet.

Since the public key can be used to access the database if its holder's identity is known, the personal database will be located on line and will be accessible to those LEFIS members with a LEFIS certificate. In the future, the database will

also be accessible with a public key certified by a certification authority that the LEFIS member that uses it trusts, and that also offers sufficient guarantees as specified by the LEFIS website personal-information access policy.

5.2. Teaching materials

LEFIS members, especially those working in educational institutions, are developing an appropriate model for use with the teaching provided in the various centres where they work. This model fits the educational standards promoted and approved by European Union institutions and those of the member states in the Bologna process to establish a European area of higher education. These reform proposals are especially aimed at promoting learning-oriented teaching, particularly to train professionals so that they are able to exercise their profession in all European Union countries, independent of their birthplace. This means that the teaching in European universities must consider the requirement that professionals should have European titles whose content and training are understandable and homologable in all of the European Union countries. The model under development is included in the LEFIS Tuning template published, as a draft at present, on the LEFIS website (http://www.lefis.org/outcomes/t_template/lefis_tuning.pdf).

LEFIS members are developing appropriate teaching materials for this training. The professions at which these studies are particularly aimed are those in the areas of the administration of justice, public administration and what is known as Internet governance, the laws and codes of practice used for management of the Internet. This teaching material will be located on the LEFIS website in a double way: on one hand, as an organised database with the aid of a documentation access tool, such as Greenstone, to put it into the form of a document library; and, on the other hand, as teaching materials accessible through MoodlePKI to all those LEFIS members holding a LEFIS certificate.

The information in the document database will be freely accessible. The information located in MoodlePKI will have restrictions. So, only some of the LEFIS members will be able to place information, namely professors provided with LEFIS certificates. Other LEFIS members will only be able to access it and to give their opinions: these will be students and other interested people, also provided with LEFIS certificates.

5.3. Validation of APTICE and LEFIS certificates

Another step to be carried out is the validation of APTICE and LEFIS certificates by the Validation Authority of the Spanish Ministry of Public Administration (MAP). To this effect, we are carrying out pertinent tests with programs developed by the MAP.

5.4. Other actions foreseen

By the halfway point of the project, we want to have carried out the following activities in the area of the security of the LEFIS electronic communications:

- a test of signing documents using LEFIS certificates;
- a test of sending encrypted electronic mails using LEFIS certificates;
- development of the various possibilities that the APTICE Certification Authority offers;
- joining the RedIRIS PKI hierarchy;
- providing access for users to the LEFIS website using the Spanish electronic DNI and other electronic certificates.

6. Conclusions

We have presented various practical examples of the rights to freedom of speech and of access to information, taking account of the virtualities and limits of the Internet and starting from our experience with LEFIS. We have also described effective safeguards that the use of the Internet should and may offer, which are similar to what happens with regard to the established relationships among citizens when they publish their opinions by means other than the Internet, such as the press, television and radio. We have presented programs designed to allow and promote this freedom of speech.

It has also been shown that it is possible to establish the security measures required by law, in this case by use of technical measures to safeguard the use and communication of personal data, the security of stored information and the free expression of ideas, without violation of other rights such as internal security or the public competences of public authorities.

Our use of technical measures has shown, in any case, that people, in this case those responsible for the design and administration of the www.lefis.org website, must make decisions paying attention to the characteristic norms and principles of democratic societies. A tool such as the Internet that is not used with such precautions, by virtue of the characteristics of its principles of operation, can favour damage to the rights of its users recognised by democratic legal systems.

7. Bibliography

General Information about PKI

Peter Gutmann, *'Godzilla' Crypto tutorial*, (consulted 12th September 2006) http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html .

Peter Gutmann, *Everything you Never Wanted to Know about PKI but were Forced to Find Out* , http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf (consulted 12th September 2006).

Symeon (Simos) Xenitellis and the OpenCA Team, *OpenSource PKI Book: A Guide to PKIs and Open-Source Implementations*, http://ospkibook.sourceforge.net/, (consulted 12th September 2006).

Books

Raúl Durán, Luis Hernández and Jaime Muñoz, *El criptosistema RSA*, Paracuellos de Jarama, Ra-Ma, 2005.

Jürgen Habermas, "The Kantian project of the constitutionalization of international law, does still have a chance?", in *Law and justice in a global society*, Granada, Anales de la Cátedra Francisco Suárez, 2005.

David Hook, *Beginning Cryptography with Java*, Indianapolis, Wrox-Wiley, 2005.

Lawrence Lessig, *El Código y otras leyes del ciberespacio*, Madrid, Taurus, 2001.

Lawrence Lessig, *The future of Ideas,* New York , Vintage Books, , 2002.

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone*, Handbook of Applied Cryptography*, http://www.cacr.math.uwaterloo.ca/hac/ (consulted 12th September 2006).

Jason Weiss*, Java Cryptography Extensions*, San Fracisco, Morgan Kaufmann, 2004.

Software

Apache Web Server with OpenSSL, http://www.apache-ssl.org (consulted 12th September 2006).

GNU/Linux SmartCard Libraries, http://www.opensc-project.org (consulted 12th September 2006).

Moodle, http://www.moodle.org (consulted 12th September 2006).

PKI Package, http://www.openca.org (consulted 12th September 2006).

SSL Libraries, http://www.openssl.org (consulted 12th September 2006).

Tomcat Java Application Server, http://tomcat.apache.org (consulted 12th September 2006).

Hardware

CryptoCards for the Spanish FNMT-CRM, http://www.c3po.es/ (consulted 12th September 2006), http://www.cert.fnmt.es (consulted 12th September 2006).

Development and Standard Definitions

BouncyCastle CryptoAPI, http://www.bouncycastle.org/ (consulted 12th September 2006)

IETF Group, http://www.ietf.org/html.charters/pkix-charter.html (consulted 12th September 2006)

Java Security and Cryptography Extension, (consulted 12th September 2006) http://java.sun.com/javase/technologies/security.jsp; (consulted 12th September 2006) http://java.sun.com/j2se/1.5.0/docs/guide/security.

Ambient Intelligence: Monitoring and Supervision of New Type

P. Mikulecký, K. Olševičová & D. Ponce

Abstract

The concept of ambient intelligence provides a vision of information society of the future which anticipates that people will find themselves in an environment of intelligent devices, represented by intuitively usable interfaces incorporated into all kinds of objects. Such an environment will be able to recognize the presence of different individuals, and react to it in a non-disturbing, and often invisible way, frequently fully integrated into a particular situation.
The devices can be understood as relatively independent entities, which are instantly monitoring or supervising activity of a human in such an environment. These intelligent entities are supposed to co-operate mutually, and all of them will co-operate also with humans. We shall discuss the co-existence of intelligent entities of various types (artificial or living) in the real world.
In the paper we discuss sources of possible ethical and legal problems of such a co-existence, and we wish to stress a number of potentially important consequences for human lives.

1. Introduction

It is well known, that the concept of *ambient intelligence*, created in the ISTAG research group reports, provides a vision of information society of the future, in which maximum emphasis is placed on user friendliness, effective and distributed support of services, reinforcement of the user's resources, and support for interactive work. This vision anticipates that people will find themselves in an environment of intelligent, intuitively usable interfaces incorporated into all kinds of objects. Such an environment will be able to recognize the presence of different individuals, and react to it in a non-disturbing, and often invisible way, frequently fully integrated into a particular situation.

However, there is another view of the *ambient intelligence*. This view should be focused on the problem arising from the relatively simple fact that humans in their environments of a new, more intelligent type will be surrounded by various information devices integrated into people's everyday life. These devices will be represented with their intelligent interfaces capable to communicate with people as well as mutually. These can be understood as relatively independent entities with certain degree of intelligence**,** which are instantly monitoring or supervising each human's activity in such an environment. Their intelligence

vary, of course, from rather simple level of one-purpose machines (e.g., an "intelligent" toaster capable to adapt the heating to the level appropriate to requirements of its individual users) to relatively intelligent and complex systems (e.g., an "intelligent" building, or a car with many features of artificial intelligence). These intelligent entities are supposed to co-operate one with another, and all of them are expected to co-operate from time to time with humans.

Considering humans also as to be another entity with various degree of intelligence, we can discuss the co-existence of intelligent entities of various types (artificial or living) in the real world. This will lead to an investigation of a number of interesting aspects of such co-existence, among them also instant monitoring as well as supervising of human entities by artificial ones in such a world. We shall discuss some sources of possible ethical and legal problems of such a co-existence, and we wish also to stress a number of potentially important consequences for human lives.

2. Ambient Intelligence – The Basic Vision and Technology

The novel concept of *ambient intelligence (AmI)*, firstly introduced in the ISTAG research group reports, provides a vision of society of the future, where the people will find themselves in an environment of intelligent and intuitively usable interfaces, in which maximum emphasis is placed on user friendliness, effective and distributed support of services, reinforcement of user's resources, and support for interactive work. This environment is able to recognize the presence of different individuals, and react to it in a non-disturbing, almost invisible way, frequently fully integrated into the particular situation.[1]

It is straightforward, that the vision of *AmI* anticipates a shift in the usage of information technology from desk computers to various devices involved in people's everyday life. At the same time, it is anticipated that the prevailing technological aspects of computing and information technology shall be moved to the background, while intelligent interfaces of an environment would become more prominent. This shift is strongly emphasized in the working programme IST in the 6th Framework Programme of the EU for 2003 - 2006, where *AmI* is highlighted as one of the main topics of the research.[2]

Insofar *ambient intelligence* is *"a set of properties of an environment that are in the process of creating"*, therefore it is impossible to define this concept

[1] See *IST Advisory Group: Scenarios for Ambient Intelligence in 2010*. Edited by Ducatel, K.; Bogdanowicy, M., Scapolo, F., Leijten, J.Burgelman, J-C. IPTS (Institute for Prospective Technological Studies) - ISTAG, EC: Luxembourg 2001. Also in *IST Advisory Group: Strategic Orientations and Priorities for IST in FP6*. Luxembourg: Office for Official Publications of the European Communities 2002.

[2] *6th Framework Programme of the EU, Working Programme for 2002 / 2006*. European Commission 2002.

explicitly. According to the ISTAG,[3] fulfilling the *AmI* vision depends on numerous research domains and components, including:

- sensor technology, bridging the physical world and the cyberspace,
- embedded systems development technology,
- ubiquitous communication including networks for active and passive tagging or internet access,
- adaptive software that is self-managing and self-adjusting,
- media management and handling supporting ”produce one, present anywhere”.

Nearly synonymous concepts of *disappearing computing* or *calm computing* express the technology diffused into everyday objects and settings.[4] From the technological point of view, *AmI* bears ship to the conception of *ubiquitous computing* (*UbiComp*), the term firstly used by Mark Weiser in 1998.[5] *UbiComp* is defined as the use of computers everywhere and is determined by interactions that are not channelled through a single workstation. It is characterized by interactions, that are not channelled through a single workstation. Technical features of *UbiComp* systems include:[6]

- *’invisible’ file systems*, so user can access data without knowing specific file names, locations or formats,
- *automatic installation and optional migration* of programs from a computer to another without requiring fundamental changes in configurations,
- *personalized information* that is tailored to the user’s requirements. AmI environment is characterized by merging of physical and digital space tangible objects and physical environments are acquiring a digital representation.

AmI artifact (also *smart object, smart device*) is an element of *AmI* environment which process information, interacts with environment, is autonomous, collaborative, composeable and changeable.[7]

---

3 ISTAG: Ambient Intelligence: from Vision to Reality. In: Riva, G.; Vatalaro, F.; Davide, F. Alcaniz, M. (eds.): *Ambient Intelligence*. IOS Press, 2005. Availaible on *http://www.ambientIntelligence.com*.

4 Russell, D. M., Streitz N. A., and Winograd T., 2005. Building Disappearing Computers. In *Comm. of the ACM, Vol. 48*, No. 3, pp. 42-48.

5 See, e.g., Alcaniz, M., Rey,B.: New Technologies for Ambient Intelligence. In: Riva, G.; Vatalaro, F.; Davide, F. Alcaniz, M. (eds.): *Ambient Intelligence.* IOS Press, 2005. Availaible on *http://www.ambientIntelligence.com*, or Bohn, J. et al. Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In *Ambient Intelligence*, Springer-Verlag, 2005, pp. 5-29.

6 Alcaniz, M., Rey,B.: New Technologies for Ambient Intelligence. In: Riva, G.; Vatalaro, F.; Davide, F. Alcaniz, M. (eds.): *Ambient Intelligence.* IOS Press, 2005. Availaible on *http://www.ambientIntelligence.com*.

7 Kameas A., Mavrommati I., Markopoulos, P.: Computing in Tangible: Using Artifacts as Components of Ambient Intelligence Environments. In: Riva, G.; Vatalaro, F.; Davide, F. Alcaniz, M. (eds.): *Ambient Intelligence*. IOS Press, 2005. Availaible on *http://www.ambientIntelligence.com*.

The vision of *AmI* is often communicated through illustrative scenarios that are related to certain domains. General scenarios of application *AmI* vision in context of everyday life were offered by ISTAG.[8] Other scenarios can be proposed for more specific domain, such as e.g., a university, that represents a variable environment where many people interact with numerous systems and devices. These interactions can be understood from the perspective of optional application of different *AmI* sub-solutions. Here we present the main areas of meaningful utilization of *AmI* principles and technologies. Some more detailed visions of *AmI* application in virtual environments such as learning management systems were discussed elsewhere.[9]

Recognition of person
The recognition of person is essential for any service personalization. The user identification mechanism can be based on biometrics or voice recognition and enabled by electronic cards, RFID, mobile phones. This process has to involve fast loading of the user profile. Leaving the environment (classroom, library) is similar to logging off the virtual environment: user profile is updated (including e.g. the list of borrowed books from the shelves) and user preferences settings are stored (including e.g. the setting of the presentation, illumination, air-conditioning technology of the classroom).

Context-based services, omnipresent monitoring, customization and personalization
Most of activities inside complex environments (e.g., a university environment) are related with delivery of data, information or knowledge. All accessed content and also its presentation should be automatically tailored both to the particular user and to the device used for accessing it. This tailoring expects processing of data from user profile, deriving of recommendations, etc. The context-based services have to build at least on following abilities:

- to recognize and interpret information and knowledge needs of individual,
- to update user's profiles with respect to information and knowledge needs, that newly appear, or that become irrelevant,
- to customize information and knowledge delivery to language and format preferences given by user, including optional machine translation,
- to exchange data with remote systems and external resources, with respect to security and privacy restrictions on both sides of communicating systems.

---

8 *IST Advisory Group: Scenarios for Ambient Intelligence in 2010.* Edited by Ducatel, K.; Bogdanowicy, M., Scapolo, F., Leijten, J.Burgelman, J-C. IPTS (Institute for Prospective Technological Studies) - ISTAG, EC: Luxembourg 2001.

9 Olševičová, K., Mikulecký, P., : Learning Management System as Ambient Intelligence Playground. In: *Proc. of the IADIS International Conference Web Based Communities 2006* (Ed. by P. Kommers, P. Isaas and A. Goikoetxea), IADIS Press, 2006, pp. 12-18, ISBN: 972-8924-10-0

For example, the same event *"scheduling a lecture of the foreign visiting professor"* will thus trigger different context-based actions for different users in the *AmI* environment: a Czech student, whose profile informs that he is interested in a theme of lecture, will get e-mail in Czech; an Erasmus exchange student will get e-mail in English; a polite acceptance letter of the lecture proposal will be sent to the lecturer; an invitation to lecture will be generated for the purpose of university website.

Innovated hardware and new types of devices
Apart of PCs, there are also other personal digital devices, servers, data projectors, printers or copy machines used within the environment. *AmI* applications and *UbiComp* systems can monitor and manage their functioning, control their communication, manage optimal usage of resources, organize repairs. The remote access to applications installed in centralized client-server model and central storage of data would mean that e.g. in a university environment students could run programs on any type of device connected to the university network and anywhere in the university campus, not only in given computer labs. Printing job could be automatically sent to the most suitable printer (e.g., the closest or less loaded one).

Intelligent interfaces, processing implicit inputs and interactions
User-friendly, intuitively usable interfaces are one of the most challenging parts of the *AmI* research. From a world where one user is sitting in front of a single computer there is a shift to another world, with users living, working, and solving problems in an environment full of interfaces with various degree of embedded intelligence.

An intelligent interface may have form, for example, of a virtual personal assistant managing for the user execution of tasks on regular basis (searching digital libraries for new publications, keeping track of submission deadlines), interaction with other personal assistants (arranging administrative actions prior to conference journey, setting up a selection of user's latest publications for the purposes of grant proposal), co-operation with other personal assistants (brokering timing of a meeting, rescheduling a postponed lecture).

Support of communication inside the community
The *AmI* vision can be also seen as something what will facilitate better communication and improve interpersonal contacts. Much more technical equipments ensuring the communication services will be physically spread over the environment. Instead of user attaching himself to a technical device (sitting at a computer connected to intra-net, wearing a mobile or hand-held), the user will freely move around in the physical environment and the communication act can be realized at a communication point best fitting the user's location, timing (synchronous/asynchronous) and expected reaction as well as urgency, privacy and security level.

For example, a communication channel similar to instant messengers may evolve such that is not restricted to computer network and keyboard/screen interface (while copying on copy machine, the user may receive an urgent message from a colleague; during the user's identification after his/her morning arrival at the university campus he/she may receive daily instructions from the boss).

Invisible file systems
The concept of invisible file systems would minimize the necessity to remember artificial paths to e-content, the need to construct and share acronyms and file names.

Accessing repositories of digital content from different devices, the user should always meet the same organization of the content. This is important especially in case of shared digital content, e.g. educational materials used by teaching assistants of the same course.
Affective computing
Affective computing is supposed to work with emotions of humans. Some authors[10] explicitly talk about tutoring systems as typical applications for utilization of students' emotional states by measurement of psychological signals.

Recognizing and anticipating the emotional state and impact (mood, tiredness, stress) will enable to adapt the *AmI* environment action towards the user. Suggesting the user appropriate action: *"take the rest, you start making errors"* is one of possible reactions of an intelligent environment to the user's emotional state.

Privacy issues
At the university, different information systems are used for management of personal data to be at the disposal of teachers and administrative staff. In an *AmI* application, large amounts of transaction data will be collected which characterize the spatio-temporal-action profile of user existence in the *AmI* environment. Data mining of these transaction data (e.g., revealing user's daily habits) must be regulated with respect to the security and privacy issues. New methods for protecting data in *AmI* environments are necessary, and their research should be one of highest priorities for the *AmI* research. Significant results in this direction certainly can contribute to building trust in new technologies among their potential users.

[10] Alcaniz, M., Rey,B.: New Technologies for Ambient Intelligence. In: Riva, G.; Vatalaro, F.; Davide, F. Alcaniz, M. (eds.): *Ambient Intelligence*. IOS Press, 2005. Availaible on *http://www.ambient Intelligence.com*.

New business models
Commercial providing of educational services opens the door to application of new business models, reflecting the ideas of *real-time economy*. *Pay-per-use* models, offered in relation to software licenses, could be applied here, e.g. for getting experiences with its practical realization and with users' response.

Interaction of AmI subsystems
The important fact is that the previously mentioned *AmI* sub-solutions can interact and can form the full-featured *AmI* environment. The exploring of this environment, whose all characteristics and total functioning cannot be easily predefined and anticipated, can bring new insights, utilizable in other complex situations (e.g., intelligent houses).[11] Future *AmI* technologies include also new, efficient algorithms for driver and compiler independent parallel and/or distributed processing of terabytes of data collected during the continuous user activity monitoring.

3. AmI – Economic, Social, Ethical, and Legal Aspects

There are three main dimensions to the problem of *ambient intelligence*:

- technological
- social
- political

Within the *technological dimension* it is necessary to study and develop technical devices, information, knowledge and communication technologies which will make the implementation of the vision of ambient intelligence possible. Key technologies might, among others, include also knowledge management, artificial intelligence, user interfaces, communication and network services, as well as solution to the problems of security and protection of data and information.

The *social dimension* focuses on studying the influences of social, economic and geopolitical trends on the quality of everyday life and the acceptance of using solutions employing information and communication technology (*ICT*) for solving problems accelerated by the above mentioned trends. Areas of problems of more global nature include for example ageing of society, multicultural society, the EU enlargement, lifelong education, the problem of consumer society, globalization, anti-globalization, etc. The *societal acceptance* of *AmI* vision depends on such features of *AmI* applications as ability to facilitate human contact, orientation towards community and cultural enhancement, ability to inspire trust and confidence, supporting citizenship and consumer

[11] *IST Advisory Group: Scenarios for Ambient Intelligence in 2010*. Edited by Ducatel, K.; Bogdanowicy, M., Scapolo, F., Leijten, J.Burgelman, J-C. IPTS (Institute for Prospective Technological Studies) - ISTAG, EC: Luxembourg 2001.

choice, consistence with long term sustainability both at personal, societal and environmental levels, as well as controllability by ordinary people.

The *political dimension* of the problem of ambient intelligence has its starting point in the resolution adopted at the Lisbon congress of the EU in 2000, on the basis of which the European Commission resolved to secure Europe's leading role in the field of generic and applied technologies for creation of knowledge society, and thus increase Europe's ability to compete successfully, and enable all European citizens to take advantage of the merits of knowledge society. To this effect, the new technologies must not be the cause for excluding some groups of citizens from society, but must ensure universal and equal approach to its - both digital and therefore also knowledge - sources. The most controversial, breath-taking implications of the *AmI* vision, especially those that seem to attack the freedom of choice of humans, or to increase our dependence on the correct functioning of numerous artificial systems are logically related to its psychological dimension and represent the main barrier that can at least slow-down the acceptance of *AmI* approach.

The concept of *AmI* is strongly motivated also by *economic aspects* – probably economic motivation is the most significant incentive in this area. A discussion about *real time* or *now-economy* has been presented by Bohn and his colleagues,[12] where more and more entities in the economic process, such as goods, factories, and vehicles, are being enhanced with comprehensive methods of monitoring and information extraction. The authors point out how two technologies, the ability to track real-world entities and the introspection capabilities of smart objects, will change both business models and consumers' behaviour.

There is also another dimension to the problem of ambient intelligence. Let us call it the *co-existential dimension*. This co-existential dimension should be focused on the problem arising from the relatively simple fact that various information devices integrated into people's everyday life represented with their intelligent interfaces capable to communicate with people, can be understood as relatively independent *entities with certain degree of intelligence.* Their intelligence varies, of course, from rather simple level of one-purpose machines to relatively intelligent and complex systems (e.g., an intelligent building, or an intelligent vehicle). These intelligent entities co-operate one with another, and all of them from time to time have to co-operate with humans.

Considering humans also as to be another entity with various degree of intelligence, we are able to study the co-existence of various intelligent entities in real world. This will lead to an investigation of a number of different

[12] Bohn, J. et al. Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In *Ambient Intelligence*, Springer-Verlag, 2005, pp. 5-29.

interesting aspects of such co-existence, and also to a number of potentially important consequences for human lives.

The *psychological theories* of different types of intelligence can help to understand human reasoning, and human interaction with machines. Each individual possesses diverse intelligences (see e.g. logical, linguistic, musical, spatial, interpersonal and other intelligences provided by Gardner,[13] or analytic, creative and practical intelligences offered by Stemberg)[14] in different percentages. As Bettiol and Campi[15] notices, this mixture of intelligences determines the learning style and motivations of each individual; therefore an *AmI* application must adopt itself dynamically to peculiarities of its users. Other psychological factor that has to be taken into account when designing *AmI* environments is that people tend to continue their habits, therefore the applications should respect the natural behaviour patterns of humans.

When taking into account such artificial entities with a certain degree of intelligence and with a mechanism for the initiation of its activity, where the activity is oriented on certain benefit (or service) to human beings, we are able to investigate the following basic problems related to them:

- various types or levels of such artificial entities,
- their mutual relationships as well as their relationships with humans,
- their communities (virtual as well as non-virtual),
- their co-existence, collaboration and possible common interests,
- their co-existence and collaboration with humans,
- antagonism of their and human interests,
- ethical aspects of the previous problems, etc.

All of these are interesting sources of a plethora of serious scientific questions. We shall try to discuss some of them in more detail now.

Ambient Intelligence as a virtual community of various entities
The first impression from the *AmI* idea is, that humans are surrounded by an environment, in which there are microprocessors embedded in any type of objects – in furniture, kitchen machines (refrigerator, coffee maker, etc.), other machines (e.g., washing machine, etc.), clothing, toys, and so on. Of course it is depending on the type of the particular environment, there are clear differences between an environment in a hospital when compared with a luxurious private house, or in comparison with a university environment.

---

[13] Gardner, H. *Frames of mind: the theory of multiple intelligences*. New York: Basic Books Inc., 1985.
[14] Stemberg, R.J. *Beyong IQ: A Triarchic Theory of Human Intelligence*. New York: Cambridge Unviersity Press, 1985.
[15] Bettiol, C. and Campi, C. Challenges for Ambient Intelligence: Empowering the Users. In *Ambient Intelligence*. IOS Press, 2005, availaible on *http://www.ambientintelligence.com*.

It is straightforward that when speaking on intelligent artificial entities able to communicate mutually, we could certainly expect some relatively intelligent behaviour of such a community. We can speak about the emergent behaviour of such a community that can be modelled e.g. as a multi-agent system, serving to some purpose considered beneficial for humans. However, the emergent behaviour of such an artificial community can be potentially dangerous – if the possible goal of the community differs from the human interests, or if the community is simply unable to serve to the human being goals from various (maybe also technical) reasons. We certainly have to take into account such questions, like:

- How to tune all the emergent behaviour of the particular environment to be able to serve the particular human being goals?
- What to do if the emergent behaviour of the environment is not in accord with the human aims, or even if it is contradictory?
- How the privacy of a particular human will be respected?
- Is the particular information about the concerned human safe from being exploited by another person?

Of course, these are just a few of possible questions which could arise in relation to the first attempts to introduce the *AmI* idea into the life. Some of other issues we will mention below.

Privacy of humans under ambient intelligence

The notion of privacy and its content in an environment with *ambient intelligence* seems to be a very delicate as well as complicated problem. Some authors have already mentioned possible problems and risks in the area.[16] As a matter of fact, the main common objective against the *AmI* concept seems to be, that it is possibly a basis for a very sophisticated and potentially dangerous surveillance system, in a sense a kind of a new *"Big Brother"*.

The personal privacy can be viewed from various standpoints.[17] Privacy is considered to be a fundamental requirement of any modern democracy. According to Lessig[18] it is possible to distinguish among the following motives for the protection of privacy in today's standards:

---

[16] See, e.g., Bohn, J. et al. Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In *Ambient Intelligence*, Springer-Verlag, 2005, pp. 5-29; or Mikulecky, P. Ambient Intelligence and the Co-existence of Humans and Machines. In *Interdisciplinary Aspects of Human – Machine Co-existence and Co-operation, Czech – Argentine Biennale "e – Golems"*, Prague, 2005, pp. 106-109.

[17] Bohn, J. et al. Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In *Ambient Intelligence*, Springer-Verlag, 2005, pp. 5-29

[18] Lessig, L. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

- *Privacy as Empowerment* – privacy mainly as informational privacy, giving people the power of controlling the publication and dissemination of information about themselves. This leads to a recent discussion, whether personal information is a private property, or intellectual property. From the *AmI* point of view, especially the right to control the dissemination or exploitation of the information about a particular person, collected about him/her by the intelligent environment, could be endangered seriously. New legal norms in this direction are necessary.
- *Privacy as Utility* – the focus is on minimizing the amount of disturbance for the individual (no unsolicited emails or phone calls). Technologically it is feasible to tailor an intelligent environment so that it is not disturbing for the human surrounded by the environment. However, there could be a complicated task of tailoring the environment to be suitable for two, three, or more persons at the same time. If their goals are contradictory, whom should be the preference given? What should be the rules for that?
- *Privacy as Dignity* – this is not only about being free from unsubstantiated suspicion, but also about equilibrium of information available between two people. The balance (equilibrium) of information between a person and the surrounding intelligent environment could be a serious problem because of their conflicting aims: the environment in a sense "wishes to know" everything about the human in order to serve him efficiently, while for the human it is usually not necessary to be aware what the environment is about. The problem of unsubstantiated suspicion seems to be much more serious one, as the vast information about the concerned person will be collected somewhere in the common memory of the intelligent environment, which can be considered, from the previously mentioned point of view, to be a sophisticated surveillance system. New legal norms are here more than necessary.
- *Privacy as Regulating Agent* – privacy laws and moral norms can also be seen as a tool for keeping checks and balances on the powers of decision-making elite. In an intelligent environment it will certainly be easy to gather information of certain type enabling to limit or prevent the society from certain type of improper behaviour. On the other hand, there should be a subtle borderline between the information necessary for the social prevention and information potentially endangering the human right for privacy.

Social acceptance

As Bohn and his colleagues pointed out,[19] the fundamental paradigm of *ambient intelligence*, namely the notion of *disappearing computer* (computers disappear from the user's consciousness and recede into the background), is sometimes seen as an attempt to have technology infiltrate everyday life unnoticed by the

[19] Bohn, J. et al. Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In *Ambient Intelligence*, Springer-Verlag, 2005, pp. 5-29

general public in order to circumvent any possible social resistance.[20] However, the social acceptance of *ambient intelligence* will depend on various issues, sometimes almost philosophical ones. The most important issue seems to be our changing relationship with our environment.

Historically, a few years ago only a couple of people expected personal communicators, but recently the penetration of mobile phones hardly surprises anyone. Some more years ago, computers needed a separate room to be installed. Recently, anyone uses personal computers, PDAs, smart phones, and other kinds of computing devices without any problem. We can extrapolate, that in the near future people would not be surprised by a smart car (first intelligent vehicles of this type already appeared), intelligent house (these are available recently as well), but also by various kinds of other intelligent environments. We can mention intelligent environments helping handicapped people, or intelligent environments in hospitals, or even intelligent academic environment at universities.[21]

We would not be surprised by a broad social acceptance of this new, recently developed phenomenon in a short horizon of a few years. According to Dryer et al.[22] *"our inevitable future is to become a machinelike collective society. How devices are used is not determined by their creators alone. Individuals influence how devices are used, and humans can be tenaciously social creatures."* Actually, based on our experience, we cannot agree more, however, social consequences that *ambient intelligence* may have will certainly be addressed in a broad debate and a deep and focused research.

4. Conclusions

Different technologies help us to preserve data and information and cover more and more aspects of our lives in quite complex ways. While in the ancient times a traveller had to simply remember all his experiences and still one century ago he could only take written notes and optionally photos, today it is possible not only to catch all audio-visual experiences continuously, using numerous portable, easy-to-use technologies, but also to process data in different ways and to distribute them around the planet in few seconds. All those devices and methods for data collection, capturing, manipulating and reuse bring new challenges that are explored under the context of ambient intelligence; we have technologies that were developed for particular objectives, but also can be

---

[20] Araya, A.A. Questioning Ubiquitous Computing. In: *Proc. of the 1995 ACM 23rd Ann. Conf. on Computer Science.* ACM Press, 1995.

[21] Olševičová, K., Mikulecký, P., : Learning Management System as Ambient Intelligence Playground. In: *Proc. of the IADIS International Conference Web Based Communities 2006* (Ed. by P. Kommers, P. Isaas and A. Goikoetxea), IADIS Press, 2006, pp. 12-18, ISBN: 972-8924-10-0

[22] Dryer, D.C., Eisbach, C., Ark, W.S. At what cost pervasive? A social computing view of mobile computing systéme. *IBM Systems Journal, 38(4)*: 652-676.

combined in new, unanticipated ways or can be applied in formerly improbable contexts.

It is hard to predict the evolution of *ambient intelligence* environments and mainly, and it is impossible to try to manage this evolution in any way. The vision of ambient intelligence is as exciting as the vision of the *Golem* was nearly five centuries ago, in the times of the *Emperor Rudolf II*. The lack of idea about real power of Golem is similar to our current lack of knowledge about real possibilities that will grow up as side-effects or emergent effects of particular *AmI* subsystems and applications at the moment of their uncontrolled interacting. All that will need a broad debate, focused research, as well as completely new legislative framework.

5. Summary

The paper is focused on a new phenomenon – *ambient intelligence* – which seems to be not only a technological problem, but also a new paradigm which requires new social, legislative, etc. attitudes. The technological background is described shortly, and a discussion about some problems, related to privacy and social acceptance is presented.

The research has been partially supported by the Czech Grant Foundation, Grant No. 406/04/2140, as well as by the Grant No. 402/06/1325.

Part 3 – Theory

Monitoring and supervision in the economic analysis of safety and security

L.T. Visscher
Erasmus University Rotterdam

Abstract

Monitoring or supervision in the sense of observing behaviour to establish whether the observed party has acted according to the applicable norms or standards of behavior is one of the many possibilities to influence behaviour. In this paper, several legal instruments (tort law, regulation and criminal law) are analysed as instruments to induce parties to behave according to the rules. Those instruments are divided on the basis of when the norm is formulated (before or after the externality is caused), who initiates enforcement of the norm (individual people or the government), how the instrument works (directly or indirectly) and the stage of legal intervention (preclusion, act-based sanctions and harm-based sanctions). It is argued that all instruments have strong and weak points, and that a combination of instruments is necessary. The costs of monitoring and supervision are relevant in determining the optimal mix of enforcement instruments, but are not all-decisive.

1. Introduction

In this paper, I will discuss the topic of monitoring and supervision from an economic point of view. The *Pocket Oxford English Dictionary* defines to monitor as 'observe someone or something in order to record or regulate their activity or progress', and to supervise as 'watch and direct the performance of a task or the work of a person'.[1] For the purpose of this paper, I will use both terms as synonyms, denoting the situation where an actor observes the behaviour of another actor, in order to establish whether the latter has acted according to the applicable norms or standards of behaviour.
Given the focus of this workshop on safety and security in society, I will limit myself to insights from Law and Economics that deal with safety and security. In economic terms, I will link the issue of monitoring to the problem of *internalization of negative externalities* (section 2). Different legal instruments exist with which this internalization can be strived for. I will treat three of such instruments (tort law, regulation and criminal law) and I will compare these instruments on their relative strengths and weaknesses (section 3). Subsequently, I will treat the literature on the topic of 'optimal enforcement' (section 4). It will become clear that society should not aim for a *minimum* level of violations of

[1] C. Soanes, S. Hawker and J. Elliot (Eds.), *Pocket Oxford English Dictionary*, 10th Edition, Oxford: Oxford University Press, 2005.

standards and norms, but an *optimal* level. The benefits of more enforcement have to be weighed against the costs of the measures that are taken to improve enforcement. Monitoring contributes to those costs, so that a decrease in those costs due to e.g. new technology affects the optimal level of enforcement and the optimal mix of instruments to attain this level. In section 5, I will discuss economic literature regarding monitoring and enforcement of environmental policy, because this provides a clear and interesting example of the previously developed insights. Section 6 contains the conclusions.

2. Safety and security in society: internalization of negative externalities

In the economic analysis of law it is assumed that when people are confronted with different possible actions, they choose the one of which they believe that it is best for them, given their information. This is the so-called rational choice theory.[2] Therefore, if someone has to choose between obeying a legal rule or breaking it, he makes an assessment of the consequences of both actions, and chooses the action which yields the best results. The legal rules influence this process.
If, for example, I have to choose between keeping to the speed limit or driving with excessive speed, I weigh my private benefits of speeding (saving time, enjoying the speed, *et cetera*) against the possible costs thereof (more use of gasoline, the possibility of a fine, *et cetera*). The higher the possible fine or the greater the likelihood that I will indeed be fined for speeding, the less attractive speeding becomes. My final decision whether or not to speed therefore is influenced by the likelihood of being sanctioned and the severity of the sanction.

If people undertake activities, they might cause possible negative consequences for others. If I speed, I cause more pollution and create more risks for others than if I keep to the speed limit. If a factory produces, it might create noise, smell and pollution for the people in the vicinity. It might also endanger the employees working with dangerous machines.
If the party who causes these negative consequences for others does not have to pay for them, he creates a *negative externality*. This party does not incorporate *all* costs of the activity in his decision whether to participate in the activity and if yes, to what extent. The private costs of the activity therefore are lower than the social costs. From a social point of view it is desirable that one only engages in an activity if the full costs are lower than the full benefits. If the actor does not have to bear all the costs himself, he engages in the activity too often. Part of the costs is born by others, and these costs lower social welfare. Only by weighing the full costs and benefits of the activity, welfare can be maximized.

---

[2] See e.g. J. Elster, 'Introduction', in: J. Elster (ed.), *Rational Choice*, Oxford: Basil Blackwell 1986, p.3; E. Mackaay, 'Schools: general', in: B. Bouckaert & G. De Geest (eds.), *Encyclopedia of Law and Economics. Volume II. Civil Law and Economics*, Cheltenham: Edward Elgar 2000, p. 408.

If the actor who causes the externality is forced to pay for it himself, he will make the correct cost/benefit analysis. He has then *internalized* the negative externality. Different methods of internalization exist. First, in situations where the parties involved can cheaply negotiate with each other (in economic terms, the *transaction costs* are low), they can reach an agreement on the price that the polluter has to pay in order to be allowed to produce, or alternatively on the price that the other party has to pay to the polluter to stop him polluting.[3] In reality, these situations of low transactions costs are scarce, and other instruments are needed.

The use of taxes, the second method to be discussed, is such an alternative. If the factory that pollutes the surroundings has to pay a tax that covers the costs of cleaning up the pollution, the factory has internalized the negative externality. The costs of the tax will be passed on to the consumers, who face a higher price. They will buy less of the product and maybe switch to a cheaper product. The producer therefore gets an incentive to reduce the pollution, if the costs of avoiding (part of) the pollution are lower than the decrease in taxes that it causes. However, it might be very difficult to exactly calculate the optimal tax, because each additional unit of production should be taxed by the additional pollution that this unit has caused.

Third, fines and non-monetary sanctions can in theory lead to internalization of externalities, if they are based on the negative effects of the behaviour on others.

Forth, tort law can lead to internalization. If the damages that the injurer has to pay are based on the losses he has caused to the victim, the injurer is confronted with the negative consequences of his behaviour. He will take care measures that cost less than the losses they avoid, and he also might reduce his activity level.

Finally, negative externalities can be avoided if regulation exactly describes the way in which a certain activity has to be undertaken. If a factory e.g. needs a permit to produce, and if this permit requires the manufacturer to take measures that avoid or reduce pollution, the factory is confronted with the costs of these measures, and therefore it cannot externalize pollution on the people living nearby. The consumers will pay for the measures through the price, and a correct weighing between costs and benefits is made.

3. Relative strengths and weaknesses of tort law, regulation and criminal law

3.1. Introduction

The different instruments for internalizing externalities can be divided on the basis of at least four criteria.[4] First, it can be asked if the norm is formulated *ex*

---

[3] R.A. Coase, 'The Problem of Social Cost, (3) *The Journal of Law and Economics* 1960, p. 1-44.

[4] S. Shavell, *Economic Analysis of Accident Law*, Cambridge, Massachusetts: Harvard University Press 1987, p. 278 ff.; S. Shavell, 'The Optimal Structure of Law Enforcement', (36) *The Journal of Law*

ante (so before the externality is caused) or *ex post* (after the externality is caused). Ex ante formulation is often done on a very detailed level, so that the norm exactly describes how the actors should behave. On the opposite, ex post formulation implies that an open norm is used, which is specified ex post on the basis of the circumstances of the actual case at hand.
Second, enforcement of the norm can be initiated by the *government* or by *individual people*. In private law, it is often the individual that starts a case, e.g. by suing the person who has committed a tort or who breached a contract. In criminal law, on the other hand, it is often the government (through the public prosecutor) who initiates the case.
Third, the way in which the externality is combated can be *direct* or *indirect*. If an indirect method is used, the actor receives incentives to change his behaviour, e.g. by the prospect of having to pay a fine if he acts wrongly or damages if he causes losses. Also imprisonment, taxes and subsidies are indirect ways to influence behaviour. Direct methods, on the other hand, exactly describe the way in which the actor has to act, and also enforce this. For example, the government can issue detailed norms for maximum emission of pollution, and close down a factory that exceeds the limits. Also an injunction directly combats the externality.
The fourth distinction partially overlaps the distinctions ex ante/ex post and direct/indirect. Legal intervention can take place at three stages. When it takes place at the earliest possible stage, the harmful act is *precluded*. This is ex ante intervention in a direct manner, e.g. a police officer that stops an actor from committing a crime. Preclusion occurs through the use of force or physical barriers. Legal intervention may also result after the act has been committed, but before harm results or irrespective of whether it does. E.g. a speeding ticket is issued on the basis of speeding, irrespective of whether the speeding motorist caused losses. Such *act-based sanctions* are ex ante, indirect methods. Finally, legal intervention might be triggered by causing harm. E.g. tort damages can only be sued for after losses already have occurred. These *harm-based sanctions* are ex post and indirect. The difference between act-based and harm-based instruments can also be characterized as *input monitoring* versus *output monitoring*.[5]
Tort law, regulation and criminal law can be categorized on the basis of these criteria. It is important to realize that the first three criteria are not binary in character, but rather form three continuums. For example, tort law is *mostly* ex post (by applying the open due care norm, which is specified after an accident), but rules of strict liability are formulated ex ante. When discussing the relative strengths and weaknesses of the different instruments, this characteristic of continuums should be kept in mind.

---

and Economics 1993, p. 257 ff; S. Shavell, *Foundations of Law and Economics*, Cambridge, Massachusetts: The Belknap Press of Harvard University Press 2004, p. 572 ff.

5 D. Wittman, 'Prior Regulation versus Post Liability: The Choice Between Input and Output Monitoring', (6) *The Journal of Legal Studies* 1977, p. 193.

As explained above, internalization of externalities increases welfare, because the actors make a better weighing between the costs and benefits of their activities. This avoids a too high activity level and a too low care level, which would cause negative consequences for third parties. However, the instruments that can achieve internalization might be more or less costly themselves. These costs of internalization should be taken into account when deciding which instrument(s) to use. The costs also influence the optimal level of enforcement: it is socially desirable to allow a certain degree of norm breaking behaviour (even though this causes negative externalities), because the costs of avoiding these violations are higher than the benefits of additional deterrence. Furthermore, information on the behaviour of the actors and the consequences thereof is needed to internalize externalities. It is more or less costly to acquire and process the necessary information, and these costs also have to be taken into account when choosing the internalization instrument(s) and when determining the desired rate of compliance.

3.2. Tort law

3.2.1. The criteria applied

Tort cases are primarily initiated by the victims, so that the initiative lies with individual people instead of with the government. The most important tort is negligence, hence the violation of an unwritten, open norm of due care. Therefore, tort law is primarily ex post. However, in situations of strict liability, or when the tort consists of violating a statutory duty, ex ante features are dominant. In most cases, plaintiffs sue for damages, so that tort law primarily is an indirect way of fighting externalities. In the more exceptional cases where plaintiffs ask an injunction, it is direct. Tort law mostly uses harm-based sanctions (damages), although an injunction is an instrument that precludes the damaging act.

3.2.2. The economics of tort law in a nutshell

Law and economics scholars argue that tort law can lead to the internalization of externalities, because the tortfeasor is confronted with the negative consequences of his behaviour for others. This result can be achieved through negligence and strict liability.
Under negligence, an injurer is only liable for the losses if he did not take enough care. In formulating the level of due care, the court should compare the costs and benefits of care measures that the injurer could have taken. If the costs of an additional care measure are lower than the benefits thereof (the reduction in the accident probability and/or the reduction in the losses if an accident occurs), yet the injurer did not take this measure, he should be deemed negligent.[6]

[6] This is the so-called *Hand formula*, named after judge Learned Hand who applied this line of reasoning in the case *United States v. Carroll Towing Co.*(159F.2d 169 (2d Cir. 1947)). He argued that an

This induces the injurer to take the care measures that cost less than they yield, so that social welfare is maximized. Under strict liability, the injurer is always liable, irrespective of his care level. He will therefore take all the care measures that he himself thinks are cost justified.
A major difference between negligence and strict liability therefore is, that under negligence the court decides the due care level and the injurer adapts his behaviour to it, while under strict liability the injurer chooses his care level himself. The quality and costs of information for courts and injurers therefore form an important aspect in the choice between the two rules.
In addition, under strict liability the injurer will engage less often in the activity, because he has to bear the full costs thereof. Hence, he will only engage in the activity if the utility that this yields exceeds the full costs of the activity. This leads to an optimal activity level, because the costs and benefits are weighed properly. Under negligence, however, the injurer only has to bear the costs of due care, so that he already engages in the activity as soon as it yields him more utility than those care costs. The activity level under negligence will therefore be too high.

3.2.3. Relative strengths of tort law

First, tort law predominantly applies open norms, which are easy to formulate. The costs of norm formulation therefore are low. The disadvantage of open norms (they do not give clear guidelines for behaviour) will be limited, because over time, legal verdicts specify the open norm for different types of situations.
Second, only in cases where harm occurred and a suit is filed, the open norm has to be specified. Given that many cases are settled outside of court, or are dealt with administratively by insurance companies, the system costs will be relatively low. The system costs are presumably lower under strict liability than under negligence, because the court does not have to investigate whether the injurer was at fault. Each case is therefore less complicated under strict liability. The possible result that more cases might be filed is more than offset by the fact that more cases will be settled, due to the higher degree of predictability of the courts' decision.
Furthermore, courts are less sensitive to the influence of interest groups than legislators, and the open norms in tort law limit the possible benefits of influencing decisions anyway.
Fourth, tort law utilizes the information that is available to the parties involved. In typical tort cases, the victim knows who injured him, so the costs of identifying the injurer are relatively low.[7] In the choice between strict liability and negligence, information is relevant as well. Under negligence, the court has to

injurer was negligent if the burden of adequate precautions (B) was lower than the product of the probability of an accident (p) and the gravity of the resulting injury if an accident occurs, so if $B < pL$.

7 W.M. Landes and R.A. Posner, 'The Private Enforcement of Law', (4) *The Journal of Legal Studies* 1975, p. 31; Shavell 1993, op.cit. (note 4), p. 267.

weigh the costs and benefits of care measures in formulating the due care level. Under strict liability, the injurer himself decides which level of care to take. If the injurer has better information about the costs and benefits of taking care (e.g. because he is a specialized manufacturer of complicated products), strict liability is preferable, because it makes use of the superior information of the injurer.

3.2.4. Relative weaknesses of tort law

The indirect approach, using tort damages as instrument, requires that victims indeed bring suit and that all injurers who committed a tort indeed pay damages. There are many factors that lead to a too low 'probability of conviction'. Victims might decide not to bring suit because the costs are higher than the expected benefits (which is especially problematic with losses that are spread over a large group of people, so that each individual victim only bears a small loss, but the total loss can be substantial),[8] or they might face problems in proving fault or causation. In principle, increasing the amount that the injurer has to pay, so that the expected damages (i.e. the probability of having to pay damages, multiplied by the magnitude of these damages) again equal the expected losses caused by the injurer, can offset this too low probability of conviction. However, many countries do not accept such punitive damages, and high levels of damages might lead to the *judgment proof problem*.

An injurer is said to be judgment proof, if he does not have enough assets to pay the damages. Tort law then cannot provide correct behavioural incentives, because an injurer will not be deterred by damages that he cannot pay anyway. Vicarious liability might solve this problem. This implies that someone else is held liable instead of the actual tortfeasor. From an economic point of view, vicarious liability makes sense if the liable party has more assets than the actual tortfeasor (so that the judgment proof problem is avoided) and if the liable party has other instruments to provide care incentives for the tortfeasor. For example, an employer is often vicariously liable for the torts committed by his employees. The employer presumably has more assets, and he can provide care incentives through the labour relation (granting or withholding promotion, wage raises, terminating the contract, *et cetera*). Of course, vicarious liability creates monitoring costs, because the principal has to supervise the agent in order to be able to determine his care level.[9]

Finally, the tendency in tort law to protect the victim ex post inefficiently increases the standard of care for the injurer, while simultaneously decreasing the standard of care for the victim himself.

---

[8] See e.g. Landes and Posner 1975, ibid., p. 33.

[9] R. H. Kraakman, 'Vicarious and Corporate Civil Liability', in: B. Bouckaert & G. De Geest (eds.), *Encyclopedia of Law and Economics. Volume II. Civil Law and Economics*, Cheltenham: Edward Elgar 2000, p. 670, 671.

3.3. Regulation

3.3.1. The criteria applied

Regulation makes use of detailed rules that describe the way in which actors should behave. It is therefore an ex ante and direct method of dealing with externalities. The government is the dominant actor, in issuing the regulation, in monitoring whether actors obey it and in enforcing the regulation by the use of force and/or fines. The timing of legal intervention can be at the earliest stage (e.g. not allowing a factory to produce before it adheres to the requirements posed by regulation), but regulation also uses act-based sanctions (e.g. imposing a fine if a building does not have proper fire exits). If costs of monitoring compliance are high, harm-based sanction can be chosen, because the occurrence of harm can provide information on possible wrongful behaviour.

3.3.2. The economics of regulation in a nutshell

For the purpose of this paper, the notion that the regulator can provide and enforce norms and standards for behaviour to fight negative externalities suffices.[10] If the regulator defines the norms and standards on the basis of a weighing of costs and benefits of possible care measures, regulation can provide actors with incentives to behave optimally. Obviously, in order to induce actors to obey the norms or standards, they have to be enforced, which causes enforcement costs. Monitoring and supervision, as well as execution of sanctions are sources of such costs. The complications that arise if the regulator does not possess adequate information, or that pressure groups try to influence the regulator so that regulation does not primarily serve the general interest but the private interest of the pressure group, are treated in the subsequent sections.

3.3.3. Relative strengths of regulation

If the regulator has better information than courts or the parties involved, it is best that he formulates a clear norm on desirable behaviour. In formulating this norm, the regulator weighs the costs and benefits of possible care measures. Given his superior information, this will lead to a better rule than under negligence (where the courts formulate the rule) or strict liability (where the injurer himself decides which measures to take).[11] An additional advantage is, that regulation can be applied to *all* actors, so that regulation can benefit from economies of scale. The regulator e.g. can analyze the possible dangers of work-

---

[10] See e.g. J. den Hertogh, 'General Theories of Regulation', in: B. Bouckaert & G. De Geest (eds.), *Encyclopedia of Law and Economics. Volume III. The Regulation of Contracts*, Cheltenham: Edward Elgar 2000, p.229; R.G. Noll, 'Economic Perspectives on the Politics of Regulation', in: R. Schmalensee and R.D. Willig (eds.), *Handbook of Industrial Organization. Volume II*, Amsterdam: North Holland 1989, p. 1256.

[11] S. Shavell, 'Liability for Harm Versus Regulation of Safety', (13) *The Journal of Legal Studies* 1984, p. 359 ff.

ing with toxic chemicals, heavy equipment *et cetera*, and issue regulation on working conditions that affects all firms using these materials.
Furthermore, the ex ante character of regulation solves the judgment proof problem, by either using instruments that preclude the act from being carried out altogether, or by using act-based sanctions instead of harm-based sanctions. Act-based fines can be (much) lower than harm-based fines/damages, because they can be discounted by the probability that the act leads to harm.[12]
Finally, because the government is the predominant actor, the problem that potential victims might decide not to bring suit because their private costs are too high, is solved.

3.3.4. Relative weaknesses of regulation

Public Choice theory argues that the regulator is susceptible to the influence of interest groups. Therefore, regulation need not be the result of a correct weighing of costs and benefits of possible measures to internalize negative externalities. It might, on the other hand, be the result of a successful lobby, thereby promoting the interests of specific pressure groups instead of increasing social welfare. In order to issue regulation, the government often has to rely to a certain extent on information issued exactly by the parties that are being regulated. These parties will have an incentive to provide information in such a manner that it furthers their goals. This problem is known as *capture*.[13]
Regulation resembles fault liability in the sense that an injurer that keeps to the norms might not be subjected to sanctions. As explained in section 3.2.2, this leads to a too high activity level, compared to strict liability.
An important drawback of regulation in the context of this paper, are the high system costs. Issuing detailed regulation is more costly than issuing open norms. This problem is worsened because regulation can be issued by different agencies, so that problems of consistency occur (e.g. the doors of a day-care centre have to be locked due to regulation concerning the safety of children (it prevents them from running onto the street), but they have to be unlocked due to fire regulation).
More importantly, because regulation is ex ante, the costs of monitoring can be very high. After all, monitoring occurs before it is clear if externalities exist. If administering speed controls, *all* motorists are monitored, not only those who are speeding. And if restaurants are (randomly) checked for their hygiene, also restaurants that obey all regulations are visited. Ex post measures do not have these high monitoring costs, because the victim of an accident might have enough incentives to respond to the externality after it has occurred, and in any case the measure is only applied in the exceptions where harm was caused. The costs of monitoring can theoretically be lowered by decreasing the level of monitoring (and thereby the probability of being caught), while simultaneously

---

[12] Shavell 1993, op.cit. (note 4), p. 262.
[13] M.E. Levine, 'Regulatory Capture', in: P. Newman (ed.), *The New Palgrave Dictionary of Economics and the Law*: Volume 3, London: Macmillan 1998, p. 267-271.

raising the fine. The expected sanction remains the same, yet the costs of enforcement decrease.[14] However, the increased fine in itself could again cause the problem of judgment proof.

3.4. Criminal law

3.4.1.. The criteria applied

In criminal law, the government is the predominant actor in issuing the rules and in enforcing them, although in some cases the public prosecutor can only try a case after a complaint of the victim. The rules are formulated ex ante, but enforcement is mostly ex post (preventive detention is an exception to this). Criminal law can be applied before and after the criminal act, and also after harm has occurred. The applicable sanctions (fines or imprisonment) are indirect methods to internalize externalities, but if a person is detained, this directly prevents him from committing other criminal acts.

3.4.2. The economics of criminal law in a nutshell

In his seminal article from 1968, Becker gave an economic analysis of crime and punishment. His main purpose was to determine how many resources and how much punishment should be used to enforce different kinds of legislation. Several factors are relevant in answering this question.
The first factor is the harm caused by norm violations, which increases with the number of offences.[15] Of course, the offenders yield gains by their offences, and these gains also increase with the number of offences. Becker defines the net cost or damage to society as the difference between harm and gain.[16] These net costs probably increase if the number of offences increases.
The second factor is the cost of apprehension and conviction. The more is spent on police, courts, *et cetera*, the easier it is to discover offences and convict offenders. The lower these costs, e.g. due to technologies such as fingerprinting, wiretapping, computer control and lie detecting, the cheaper a given level of apprehension and conviction would be.
The third factor, the supply of offences, depends on the probability of apprehension and conviction and the severity of the sanction. It appears that an increase

---

[14] See e.g. A.M. Polinsky and S. Shavell, 'Public Enforcement of Law', in: B. Bouckaert and G. De Geest (eds.), *Encyclopedia of Law and Economics. Volume V. The Economics of Crime and Litigation*, Cheltenham: Edward Elgar 2000, p. 312.

[15] G.S. Becker, 'Crime and Punishment: An Economic Approach', (76) *Journal of Political Economy* 1968, p. 173.

[16] Shavell does not incorporate the gains that injurers get from committing intentional norm violations in the social welfare function. He regards their utility as 'social illicit'. Friedman does not agree with this method, because by labeling certain activities as social undesirable, even if they yield more gains to the injurer than they cause losses for the victim, the conclusion that these acts are undesirable is presumed instead of proven. See Shavell 1987, op.cit. (note 4), p. 147 and D.D. Friedman, *Law's Order. What Economics Has to Do with Law and Why it Matters*, Princeton, New Jersey: Princeton University Press 2000, p. 229 ff.

in the probability has a greater effect than an increase in the punishment.[17] Also other factors, such as income and law-abidingness due to education, are relevant.
The last factor concerns punishments, which differ in the costs they impose on the offender. They also affect other members of society. The total costs of punishment are the cost to offenders plus the cost or minus the gains to others. Fines produce a gain that equals the cost to the offender, aside from collection costs. Imprisonment, on the other hand, also causes costs to others, e.g. the need for guards, buildings, *et cetera*. Imprisonment is therefore more expensive than the use of fines.
According to Becker, the criminal justice system should aim to minimize the total social costs. This implies that the severity of a sanction should depend on the harm caused, but also on the probability of apprehension and conviction. Furthermore, imprisonment should be replaced by fines whenever possible, due to the lower social costs. Finally, one should not aim for maximum deterrence, but optimal deterrence. The enforcement costs are one of the factors determining the optimal level of enforcement.[18]

3.4.3. Relative strengths of criminal law

Criminal law can make use of non-monetary sanctions such as imprisonment. These methods can offer a solution to the judgment proof problem. Even if an actor has limited assets so that the financial threat of fines or damages does not provide adequate behavioural incentives, the possibility of being detained might provide enough incentives after all.
Criminal sanctions are regarded as relatively heavy, due to a negative reputation effect and the consequences they might have for employment or personal relationships. This offsets the low probability of conviction, because the expected sanction can still be high.
The negative association that people generally have with criminal activities in itself can already prevent them from engaging in such activities, so that these norms do not cause high enforcement costs. However, this requires that criminal rules remain exceptional. The more types of undesired behaviour are treated as crimes, the less this 'self-enforcement' will occur.

3.4.4. Relative weaknesses of criminal law

Criminal law is an expensive instrument to control externalities. The punitive element essentially lowers social welfare because it imposes costs on the convicted offender without offering offsetting gains elsewhere. This problem is larger with imprisonment than with fines, because a fine is a transfer of money, while the imprisonment creates additional harm.
This also implies that the consequences of a wrongful conviction are much greater than the consequences of a wrongful acquittal, so that the legal proce-

[17] Becker 1968, op.cit. (note 15), p. 176.
[18] Becker 1968, op.cit. (note 15), p. 207 ff.

dure needs many safeguards against wrongful convictions. This increases the system costs and reduces the probability of conviction. It also might cause high monitoring costs, because it is only worthwhile to start the costly criminal procedure if there is enough evidence to sustain the charge.
Furthermore, imprisonment is a costly sanction, when compared to fines and damages, not only because of the stigmatizing character, but also because of the high costs of guards, buildings *et cetera*.
Finally, the officials in the whole process have to be monitored themselves, to avoid abuse of power *et cetera*. This introduces a new type of monitoring costs, because not only actors who might not act according to the norm have to be monitored, but also the officials in the criminal procedure.

3.5. Conclusion

Tort law, regulation and criminal law all have their strengths and weaknesses. Depending on the circumstances, one instrument might work better than the other, and in economic theory it is well established that a combination of instruments is needed to optimally internalize negative externalities.[19] If e.g. the legislator has the best information on the costs and benefits of certain types of behaviour, regulation is preferred over tort law. On the other hand, negligence is superior if courts have the best information, and strict liability if the injurer is the most informed party. Regulation might offer minimum safety rules, thereby profiting from economies of scale, but under specific circumstances, tort law might induce actors to take additional care measures. The use of ex post monetary sanctions is problematic if the injurer is judgment proof, so that ex ante regulation or ex post non-monetary sanctions are more appealing in cases where optimal tort damages would be so high that they indeed cause judgment proof problems. Criminal law has high system costs due to e.g. the penalizing character, but the non-monetary sanctions might be necessary to solve the problem that tort law does not provide adequate incentives in cases of widely spread losses.
Generally speaking, Law and Economics has a preference for tort law. Private parties know their own preferences best and they can act accordingly. They often possess adequate information on costs and benefits of care measures and on the identity of the injurer. The system costs of tort law are relatively low, due to the ex post, harm-based sanctions and the open norm character. In cases where tort law does not work properly, due to informational problems, judgment proof injurers or too low probabilities of conviction, regulation and criminal law become more important. Due to the high system costs, criminal law should serve as an *ultimum remedium*.
The list of relevant factors in deciding the optimal mix of the different instruments is long, and many interrelations between them exist. The costs of monitoring are one of those factors. It is therefore important to realize that one should not solely focus on these costs, but has to embed them in the broader framework.

[19] See e.g. Shavell 1984, op.cit. (note 11), p. 365.

The costs should not be neglected either, because changes in the costs of monitoring, e.g. due to technological changes, influence the optimal mix of instruments. In the next paragraph, I will therefore analyze the optimal mix of instruments in general, and I will pay specific attention to the role of the costs of monitoring and supervision.

4. Optimal enforcement and the influence of monitoring and supervision

4.1. The choice between preclusion, act-based and harm-based sanctions

Several factors influence the choice between the different instruments to control risk. If the possible sanctions are only small, they might not be able to deter undesirable behaviour, so that preclusion through force or physical measures is the only possible alternative. As the magnitude of potential sanctions increases, act-based sanctions become available as well, and if the magnitude becomes sufficiently high, harm-based sanctions can be used. Shavell gives a clear numerical example regarding this relationship.[20] Suppose that a person obtains a benefit of 50 from an undesirable act that causes high losses with a probability of 20%. Also suppose that the highest possible sanction is 100, that there is a 30% chance that an act-based sanction will be applied and that there is a 30% chance that a harm-based sanction will be applied if harm occurs. Neither type of sanction can deter this person, because the expected act-based sanction is 0.3*100 = 30 and the expected harm-based sanction is 0.2*0.3*100 = 6, while the private benefits where 50. The only way to avoid the undesirable act therefore is preclusion by force or physical measures. The sanction has to be at least 166.67 for act-based sanctions to work (because 0.3*166.67 = 50) and 833.33 for harm-based sanctions to work (because 0.2*0.3*833,33 = 50). The possible magnitude of sanctions is determined by the wealth of the party involved, or with imprisonment by his remaining life. Also, notions of fairness can limit sanctions (e.g. life imprisonment for shoplifting would be considered as being unfair), and in the economic analysis of criminal law it is well established that the magnitude of the sanction should rise with the size of the harm (*marginal deterrence*). These limits on the magnitude of the sanction can lead to the necessity of increasing the probability of sanctioning, thereby probably increasing the costs of monitoring, to offset the limited size of the sanction.[21]

Second, the probability of sanctioning is relevant. If it is difficult to preclude by force or physical measures, act-based or harm-based sanctions become more appealing. If monitoring of behaviour is difficult, preclusion or harm-based sanctions become more attractive. If it is difficult to establish a causal relation between certain harm and the possible acts that have caused them, preclusion or act-based sanctions are better. It should be noted that improvements in monitor-

[20] Shavell 1993, op.cit. (note 4), p. 261 ff.

[21] See e.g. A.M. Polinsky and S. Shavell, 'The Fairness of Sanctions: Some Implications for Optimal Enforcement Policy', (2) *American Law and Economics Review* 2000, p. 232.

ing techniques can increase the probability of sanctioning, but this might induce actors to spend resources in order to evade being detected. For example, radar controls have increased the probability of being caught when speeding, but devices such as a radar detector or see-through covers for license plates that cause a picture of the license plate to be illegible could offset this increase (just as the mere destruction of camera poles would). Also, devices that scramble the signal of mobile phones or computer data reduce the effectiveness of monitoring these forms of communication. This can lead to a costly alternation of measures and countermeasures, which lowers social welfare.

Third, the level of information is important. If parties have good information on the dangerousness of their behaviour, harm-based sanctions can provide correct incentives. If they lack this information but they know that certain behaviour is not allowed, act-based sanctions could deter adequately. If the actor is unaware of the dangers of his actions, he might not realize that his act is forbidden, so that neither harm-based nor act-based sanctions work. Preclusion then is the only option. This of course assumes that the social authority has better information regarding the true dangers.

Also the enforcement costs are relevant. If it is relatively cheap to deter people by using physical measures (e.g. fencing an area in which they otherwise might dump toxic waste), sanctions become less attractive. However, if preclusion requires the use of officials who constantly have to monitor the behaviour of actors, it might become too expensive so that sanctions have to be used. Harm-based sanctions then have an advantage over act-based sanctions, because they are applied less often. In some circumstances it may be easier to impose act-based sanctions (e.g. determining whether oil tanks of ships are properly maintained might be easier than detecting whether a ship has leaked oil into the ocean),[22] in other circumstances harm-based sanctions could be easier (e.g. determining whether a driver who caused an accident made a wrong turn as opposed to constantly observing all drivers on their turns).

Finally, determining the expected harm of an act might be much more difficult than ascertaining the actual harm if an accident has occurred.

Technological developments can change the relative attractiveness of preclusion, act-based sanctions and harm-based sanctions. For example, if speeding of motorists could only be detected by police officers that subsequently would have to chase the speeding motorist to fine him, act-based sanctions would be very expensive. The use of radar and photo cameras decreases these costs substantially, so that act-based sanctions become feasible. Recent developments in so-called *Intelligent Speed Adaptation* (ISA) might even preclude speeding altogether. With an ISA system, an onboard computer can, by the use of GPS, determine the position of the vehicle. The computer checks whether the local speed limits are exceeded. If they are exceeded, the driver is warned by a signal, or the device even reduces the speed of the vehicle automatically. Detection of shoplifting through the use of electromagnetic gates instead of personnel that

[22] Polinsky and Shavell 2000, ibid., p. 315, 316.

constantly scans the shop is another example. Also the way in which drunk driving is combated might change, e.g. if *alcohol locks* become cheaper to manufacture. This way, a drunk driver *cannot* drive his car and this act is therefore physically precluded.[23] This might be better than act-based sanctions (a fine and/or confiscation of the driver's license) or harm-based sanctions (civil or criminal liability after an accident is caused due to drunk driving). At present, the alcohol lock is sometimes installed to avoid repeat offences. The higher probability of drunk driving of someone who was already convicted for this offence, justifies the still substantial costs of applying the technique. The mere probability of act-based and harm-based sanctions are too low for repeat offenders, compared to the externalities they are likely to cause.[24]

Wittman analyzes the complicated relationship between act-based and harm-based sanctions. In essence, the monitoring actor has four methods of control available: (1) the probability of detecting and sanctioning the act, (2) the sanction when the act is detected, (3) the probability of detecting and sanctioning harm and (4) the sanction when harm is detected. If a change in technology decreases the costs of detecting an act (e.g. the introduction of radar to monitor speed), act-based monitoring becomes more attractive compared to harm-based monitoring. The severity of the punishment will decrease, because the higher rate of detection leads to more convictions, thereby increasing the social costs of

---

[23] It is possible that a passenger takes the breath test, so that a drunken person can still drive. To decrease this problem, the test has to be repeated with random intervals (while driving) and taking the test for someone else is considered as a criminal offence.

[24] A recent Dutch situation provides an example regarding the relation between available information, technical measures, public or private initiative and the probability of 'being caught'. One of the many tasks of the General Inspection Service ('Algemene Inspectiedienst AID') is to monitor cattle markets on cruelty to cattle. In 2005 the AID received information from vets and cattle traders that in some instances animals were mistreated, and therefore additional supervision is executed. On August 24, 2006, the foundation Animalrights Netherlands ('Dierenrecht Nederland') has published photographs and videos which were made with the use of hidden cameras, which show that mistreatment of cattle still occurs. The foundation has pressed charges against the persons involved. The Dutch Minister of Agriculture has responded that supervision by the AID has to be improved and increased.
In terms of this paper, vets and traders possessed private information regarding cruelty to animals, and after they conveyed this information to the AID, supervision was increased. Obviously, the idea behind increased supervision is to increase the probability of getting caught and hence the expected sanction. Apparently, the increased supervision did not solve the problem. This could very well be explained by the high costs of supervision (due to the costs of monitoring one should aim for optimal rather than maximal deterrence) and the fact that the AID has to supervise other activities as well. Private entities such as the foundation Animalrights are able to provide additional information, e.g. by using instruments which public bodies are not allowed to and by the fact that they can operate incognito (cattle traders who see the AID inspector will probably behave according to the rules, just as many motorists will reduce their speed when they see a police car). As a result of the new information, public monitoring might increase.
Obviously, the increase in public monitoring is not necessarily desirable. The AID might have to reduce supervision in other areas, which might lead to more problems in those areas. Cruelty to animals is an area where the public opinion is an important factor. From the perspective of Public Choice theory it is therefore not surprising (especially if one considers that general elections were scheduled to take place three months later!) that on the same day that Animalrights Netherlands published the evidence, members of Parliament have confronted the government with this issue, and the Minister of Agriculture has already promised increased supervision. It is noteworthy that in the general elections, the Party for the Animals ('Partij voor de Dieren') has won two seats in Parliament.

sanctioning. The expected act-based sanction increases, because the increase in probability outweighs the decrease in magnitude of the sanction.[25]

4.2. The role of information

In section 3 it is already discussed that in setting the standard for behaviour, regulation makes use of the information of the government, negligence of the information of courts and strict liability of the information of the injurer.
It is also mentioned that tort law uses the information that the victim has regarding the identity of the injurer, because it requires the victim to bring suit against (a) specific defendant(s). Also the desire not to be harmed (again) and to see the injurer suffer sanctions can induce the victim to use his information to identify the injurer.
In situations where the victim does not possess information on the identity of the injurer, public enforcement activity may be necessary. Private parties might not have enough incentives to identify the injurer, e.g. because they bear the full costs of identification but only expect little benefits. The private benefits of finding the injurer can therefore be lower than the social benefits, which consist of the possibility to confront the injurer with the negative externalities he has created. It can also be the case that it is socially desirable that information systems or other enforcement technologies are developed, but that it is not worthwhile for individuals to do so. Fingerprint records or DNA databases, shared information systems, satellite surveillance for environmental pollution *et cetera* are so-called *natural monopolies*. This means that they can be most cheaply produced on the largest possible scale, because they have huge fixed costs and low marginal costs. New information sharing technologies, e.g. through the Internet, can change this character, so that smaller units of information gathering might become optimal, and private initiatives again become feasible.
From an economic point of view it is - all else being equal - desirable to use the instrument for internalizing externalities that retrieves the necessary information at lowest cost. Monitoring is a relatively expensive method to collect information, especially compared to tort law. After all, under a regime of tort law the victim has an incentive to sue the injurer, so that the behaviour of potential injurers need not be constantly monitored to discover harmful behaviour. Strict liability, moreover, induces the injurer to utilize his information in determining which care measures to take, because he always bears both the costs of those care measures and the expected losses. This reduces the need to monitor the injurer for possible norm violating behaviour, as well as the need for the courts (negligence) or regulator (regulation) to attain the necessary information. Obviously, the relative weaknesses of tort law limit its information cost saving potential, so that regulation and/or criminal law might be necessary as well.

[25] Wittman 1977, op.cit. (note 5), p. 196.

4.3. The framework applied to the legal instruments[26]

In tort law, harm-based monetary sanctions are applied. Direct prevention would be impossible in many of the types of accidents that tort law seeks to deter. It is e.g. not possible to monitor many of the measures that motorists can take to avoid accidents, such as paying adequate attention to traffic instead of changing a CD, starting the journey on time so that time pressure is avoided, not driving when one is tired, *et cetera*. Act-based sanctions are also too costly, because many acts can cause losses. Monitoring all these types of behaviour and sanctioning them is very costly, while in most cases no harm occurs. Harm-based sanctions are therefore the only feasible instrument to provide incentives for better behaviour. The mere fact that harm actually occurred can provide information on the dangerousness of the activity, although it is important to keep in mind that also an injurer that takes due care can cause losses. Monetary sanctions are often enough to provide the necessary incentives. In cases where the injurer deliberately reduces the chance that he will be identified (e.g. by leaving the scene of the accident that he has caused), non-monetary sanctions from criminal law might be used to provide adequate incentives after all.
Regulation comes into play if the regulator has superior information, or if the harm-based sanctions of tort law do not adequately deter, e.g. due to the judgment proof problem or a too low probability of being held liable. Shavell provides the examples of regulation to avoid a fire in a restaurant (large expected losses), health-related losses (difficult to establish causation, thereby lowering the probability of being held liable) and environmental losses (problems with causation and possible widely dispersed losses, which both lead to a too low probability of being held liable).[27] Under these circumstances it is better to prevent the act in the first place. When this is impossible or too costly, e.g. due to costs of monitoring, act-based sanctions are used. Obviously, these also require monitoring in order to detect the acts. If the probability of detection, combined with the possible fine, is not high enough to deter, criminal law might be needed.
Criminals often try to avoid being detected and being caught. This reduces the probability that act-based or harm-based sanctions can be applied, so that the magnitude of the sanction has to be increased to offset this. This, together with the often limited assets of the criminal and the gains he expected to yield, explains the use of non-monetary sanctions. It also clarifies why criminal law sometimes tries to prevent the crime in the first place, and why attempts that do not succeed are punished nonetheless. Furthermore, people that committed crimes have shown that they were not deterred by the expected sanctions (‘*gen-*

[26] Shavell 1993, op.cit. (note 4), p. 271 ff.
[27] Shavell 1993, op.cit. (note 4), p. 279. Also see M. Boyer and D. Porrini, ‘The Choice of Instruments for Environmental Policy: Liability or Regulation?’, in: R.O. Zerbe and T. Swanson (eds.), *An Introduction to the Law and Economics of Environmental Policy: Issues in Institutional Design*, Volume 20, Elsevier Science Ltd., p. 246.

eral deterrence'), and imprisonment might be the only way to prevent them from committing further crimes ('*specific deterrence*').

Polinksy and Shavell distinguish between fixed and variable enforcement costs.[28] The fixed enforcement costs are independent of the number of violations of a standard and are incurred to reach or maintain a certain probability of detection. The variable enforcement costs on the other hand depend on the number of violations and are made in order to actually fine the violator. The optimal fine equals the harm, corrected for the probability of detection, as well as the variable enforcement costs. This implies that the optimal fine will increase if variable enforcement costs rise and/or if the probability of detection decreases due to higher fixed enforcement costs. The optimal probability of detection decreases if fixed and/or variable enforcement costs increase. It simply becomes too expensive to detect violations and/or to impose the sanction on violators.
Monitoring concerns fixed enforcement costs. Therefore, if technological changes decrease these costs, the optimal probability of detection increases, and the optimal magnitude of the fine decreases. These changes increase the attractiveness of regulation *vis-à-vis* tort law and criminal law.

4.4. Liability of monitoring agencies

An interesting and actual topic where several of the abovementioned insights are relevant is liability for monitoring agencies.[29] In many fields of public safety, governments make use of monitoring agencies that have to check whether actors in the relevant field behave according to the applicable regulation. Examples can be found regarding the quality and safety of food, medicines, consumer goods, safety of the workplace, *et cetera*. These agencies should contribute to public safety by responding to observed norm violating behaviour through e.g. imposing fines, withdrawing permits or even forcefully correcting dangerous situations.
If an actor violates the rules and thereby causes losses, the monitoring agency cannot be automatically held liable for these losses. Only if the supervision was inadequate or if the agency did not respond to a situation where it should have responded, liability can be an issue. It is important to note that the monitoring agencies have a certain degree of freedom in determining their policy, so that courts will act reservedly in establishing liability.
The supervisors experience the so-called supervisor's dilemma: if they are not active enough, third parties might start a tort suit against them for the resulting losses. However, if they take measures that in hindsight were not necessary (e.g. withdraw a permit or close an installation), they can be held liable for the negative consequences by the affected actors. Obviously, if the supervisor is held

[28] A.M. Polinksy and S. Shavell, 'Enforcement Costs and the Optimal Magnitude and Probability of Fines', (35) *The Journal of Law and Economics* 1992, p. 133.
[29] See e.g. C.C. van Dam, *Aansprakelijkheid van Toezichthouders*, British Institute of International and Comparative Law 2006 (www.wodc.nl/images/1189_deel1_volledige%20tekst_tcm11-112960.pdf).

liable for the losses caused by a rule violating actor, the supervisor might take recourse on the actual injurer. The administrative costs of such recourse actions, however, can be substantial.[30]

Most monitoring agencies have reported that they are not influenced in their policy by the possible liability claims from third parties. The explanation for this is, that they base their decisions on their ideas of professionalism. The agencies themselves do not plea for abolishment of liability, because they regard the liability claims as a test for their professionalism and quality.[31] Obviously, liability *can* influence monitoring policy, because agencies pay attention to case law in determining their policy. It is not the *fear* of liability, but the possible impact of liability cases of e.g. standards of care that indirectly can influence supervisors.[32]

Kraakman argues that while most legal devices for recruiting private enforcement rely on rewards, this is impossible with 'gatekeepers' (an actor that can prevent misconduct by withholding support, such as not issuing a permit). Their efforts to withhold support from wrongdoing are invisible and difficult to verify, so that we can only observe ex post the occasions where the gatekeeper fails to prevent misconduct ex ante.[33] Imposing liability on failing gatekeepers creates administrative costs. Whether or not these costs are worthwhile depends on the extent in which the threat of liability improves the supervision by the gatekeeper. It is difficult to draw general conclusions on this issue.

5. Monitoring and enforcement of environmental policy as an example

Cohen has given an extensive overview of economic literature on monitoring and enforcement of environmental policy.[34] In this section I will sketch the results of this survey that are most important for the topic of this workshop on monitoring and supervision, and add insights from other relevant literature.

An important way to improve the effectiveness of monitoring is to divide firms that were monitored into two groups. The first group consists of firms that complied at the last inspection and the second of firms that did not comply. Firms in group 2 are subsequently monitored more often, the regulatory standards for them might be tougher and/or the sanctions more severe, as compared to group 1. It appears that this scheme leads to a higher rate of compliance than subjecting all firms to the same monitoring regime.

If firms differ in the effectiveness of an audit, meaning that norm breaking behaviour of some firms is more difficult to detect than such behaviour of other firms, it is best to first audit the firms that are easiest to audit. As the budget for

---

30 W.M. Landes and R.A. Posner, 'Joint and Multiple Tortfeasors: An Economic Analysis', (9) *Journal of Legal Studies* 1980, p. 529, 530.

31 See Van Dam 2006, op.cit. (note 29), p. 72.

32 See e.g. Van Dam 2006, op.cit. (note 29), p. 137, 138.

33 R.H. Kraakman, 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy', (2) *Journal of Law, Economics, and Organization* 1986, p. 60.

34 M.A. Cohen, *Monitoring and Enforcement of Environmental Policy*, 1998.

audit increases, more firms can be monitored. The firms most difficult to audit might not be monitored at all, which could induce them to pollute as much as they like. This problem might be limited, however, by the fact that a high level of pollution in itself can attract the attention of the auditing agency. Furthermore, firms that value pollution the least should be audited first, because they can be deterred relatively easy. A low probability of detection might already be enough to deter these firms, so that the costs of monitoring them are low.[35] The general insight that monitoring costs lower the optimal rate of compliance, so that one should not strive for maximum but optimum compliance, is also present in the literature regarding enforcement of environmental law.[36]

In the above sections it already became clear that the optimal magnitude of the sanction and the probability of conviction are interrelated. It is possible to save monitoring costs by increasing the magnitude of the sanction, because the lower probability is offset by the larger magnitude of the sanction. However, the possible magnitude of the sanction is limited by the wealth of the offender, ideas of fairness, the need for marginal deterrence and risk aversion. This last argument implies that actors prefer a larger probability of a small loss to a smaller probability of a large loss, the reason behind it being that a twice as large loss in money leads to a more than twice as large loss in utility. After all, actors spend their first euros on the most important needs, and subsequent money is spent on lesser needs. Larger losses therefore also endanger the more important needs. Hence, a tradeoff exists between the desire to lower monitoring costs (by increasing the fine and decreasing the probability of being caught), and the decrease in welfare it causes due to risk aversion.[37]

Another way to decrease the costs of monitoring is to induce *self-reporting behaviour*.[38] This instrument shifts (part of) the monitoring costs onto firms (who now have to investigate whether pollution occurs), which is socially desirable if firms can monitor at lower cost than the government. It is possible to require firms to report violations of environmental standards and to base the possible sanction for violating behaviour on whether the firm indeed reported this. Firms that did report will be subjected to lower sanctions than firms that did not report, to induce them to self-report. Failure to report or submitting false reports could even be labelled as crimes, to make this kind of behaviour very unattractive. Obviously, the higher the sanction for pollution, the more resources firms might spend on trying to evade detection, so that the quality of the self-reports might decrease. Self-reporting introduces new monitoring costs, because the self-reports have to be audited. The total costs decrease if the costs of monitoring behaviour are high and/or the maximum feasible fine is limited. However, self-

---

35 I. Macho-Stadler and D. Pérez-Castrillo, 'Optimal Enforcement Policy and Firms' Emissions and Compliance with Environmental Taxes', *UFAE and IAE Working Paper 612.04* 2004, p. 13, 14.

36 See e.g. C. Arguedas, 'Pollution Standards, Costly Monitoring and Fines, *CentER Discussion Paper No. 2005-09* 2005, p. 4, 16, 17.

37 See e.g. A.M. Polinksy and S. Shavell, 'The Economic Theory of Public Enforcement of Law', (38) *The Journal of Economic Literature* 2000, p. 53, 54.

38 See e.g. L. Kaplow and S. Shavell, 'Optimal Law Enforcement with Self-Reporting of Behavior', (102) *Journal of Political Economy* 194, p. 583-606.

reporting probably increases costs if the costs of collecting penalties are high or if the regulator's monitoring technology is very accurate.
Cohen discusses the scarce empirical literature regarding environmental enforcement. Monitoring oil transfer operations and random port patrols designed to detect spills are found to be effective, but routine inspections that are designed to determine if vessels are in compliance with oil spill prevention regulations has no significant effect on spill size.[39] This implies that harm-based sanctions are more effective than act-based sanctions. Furthermore, the implemented change in monitoring policy of the U.S. Coast Guard to classify ships into 'low risk' (infrequently monitored) and 'high risk' (always monitored) turned out to reduce the costs of enforcement, without having a negative effect on the environment. This offers an empirical corroboration of the theoretical idea described above: decreasing monitoring costs by supervising high risks more intensively than low risks. Research on monitoring and fines regarding industry emissions in the U.S. and Canada shows that both methods reduce the levels of pollution, although a 10% increase in fines appears to have a larger impact than a 10% increase in monitoring activity. Most researches also show that firms that were monitored and that complied are less likely to be inspected in the next period.

6. Conclusion

In this paper I have discussed the literature on the economic analysis of optimal law enforcement and the role of monitoring and supervision. Tort law, regulation and criminal law are different instruments for the internalization of negative externalities. These instruments all have strengths and weaknesses, and optimal enforcement requires a mix of all instruments.
Monitoring and supervision in this paper regard the situation where an actor observes the behaviour of another actor, in order to establish whether the latter has acted according to the applicable norms or standards of behaviour. Tort law, which has an ex post character, does not rely on monitoring and supervision in this sense, with the possible exception of vicarious liability, where the principal (e.g. an employer) has incentives to monitor the behaviour of the agent (e.g. the employee), in order to be able to induce him to avoid losses.
Within the context of monitoring, it is possible to distinguish between input and output monitoring, where the former relies on act-based sanctions and the latter on harm-based sanctions. Furthermore, it is possible to preclude damaging acts from occurring in the first place, by applying physical restrictions or force.
A general preference for tort law exists, due to the relative low costs of this instrument. However, problems of judgment proof and a limited probability of being convicted limit the possibilities of tort law. Criminal law has to be used as *ultimum remedium*, due to the high system costs and social costs.
If input and output monitoring are very costly, preclusion is attractive. If input monitoring becomes cheaper (e.g. speed control by radar), act-based sanctions

[39] Cohen 1998, op.cit. (note 34), p. 33.

become more attractive. If output monitoring becomes cheaper (e.g. due to the possibilities of satellites to detect dumping of toxic waste), harm-based sanctions become more important.

The costs of monitoring are just one of the many factors that determine optimal enforcement, so it's importance should not be overstressed. However, because the costs are substantial, they should not be neglected either. Technological changes that decrease the costs of certain monitoring devices leads to a higher level of optimal enforcement, but also to a shift between the different instruments to internalize negative externalities.

Surveillance technology, Constitutional rights and the 'Monitoring Power'

Richard V. De Mulder & Pieter Kleve
Erasmus University Rotterdam

Abstract

Surveillance techniques have become embedded in modern society. Their applications are diverse. The ease of use and the diminishing costs of this technology have led to a substantial growth in monitoring. This is of particular importance because of the impact of surveillance technology on certain constitutional and legal rights. This article reaches the conclusion that with the increasing significance of surveillance technology, the need to monitor those carrying out the monitoring will increase as well.

1. Introduction

Surveillance and monitoring technology has become commonplace throughout the world. It is used to supervise both social and physical processes, and to monitor individual behaviour. This technology is constantly being refined. For example, speeding, as an offence that forms a risk to public health, has for some time been dealt with by technology. The standard approach has been to have a camera that takes a photograph of the car once a certain maximum speed has been exceeded. Having established the level of the speeding, the car owner is then sent a notification of the appropriate fine. However, in this set up the camera can only register the offence if it takes place where the camera is located To remedy that deficiency, a new form of surveillance has made its appearance: it is now possible to follow the car along a section of the road. If the average speed is too high, notification of a fine will be sent. For the road user, this development means that it is pointless just to slow down at the location of the first camera; speed must be kept down for the whole stretch of road between the two cameras.[1]

In the above example, there are legitimate legal grounds for the use of surveillance technology; the law has already laid down what constitutes the maximum speed and the carrying out of the procedure is the responsibility of the state. This surveillance technology has led to a certain conditioning of driving behaviour. However, road cameras have stimulated some drivers to find means of evasion. One such technique is the radar detection device, which warns of the vicinity of radar controlled speed measurement equipment. That has led some

[1] It should perhaps be pointed out that this technology will not catch the driver who only speeds for a very short time on that section of road.

authorities to demand that such detection devices be made illegal (and consequently some manufacturers have developed detection devices that do not fall within the category of 'illegal radar detection devices'). This is only a confirmation of the well-known fact that a rule of law does not, of itself, produce compliance. Individuals will act in their own self-interest, as they see it.[2] This action/ reaction phenomenon draws attention to the relationship between a rule of law and the enforcement of that rule of law. The use of technology may promote compliance with the law, although that is not always necessarily the case.

Surveillance by camera is, of course, not confined to traffic situations. The use of camera surveillance is common in shopping centres, petrol stations and industrial areas, to name just a few examples. Although camera surveillance is an obvious example of making people feel that they are 'being watched', it is by no means the only form of surveillance. It is already the case that foreigners who wish to enter the USA must provide fingerprints of both index fingers and a passport photograph. Other personal data is provided by the charter company.

Internet is not as anonymous as its users have long presumed. Surfing on the net leaves countless tracks, which can be picked up by businesses that chart users' Internet behaviour. Given the state's monopoly on coercion, it is not difficult for the state to obtain access to these 'tracks'. There was considerable consternation when the press revealed the existence of the Echelon program of the American National Security Agency (NSA). This controversial program could monitor (or tap) data exchange on the Internet and thus, in effect, worldwide.[3]

2. Surveillance techniques

From the above examples, it is clear that technology plays an important role in surveillance. Surveillance is not exclusively aimed at conformity with certain legal requirements. Nor is it restricted to use by governmental agents. Surveillance by the authorities is often the starting point of a process that leads to tracking down offenders and prosecution. IT (information technology) has become a major means for implementing all the stages in that process. Various examples of this type of technology are presented below.

[2] C.f. M.C. Jensen & W.H. Meckling, 'The Nature of Man', *Journal of Applied Corporate Finance* 1994-2, p. 4-19.

[3] However, the question must also be raised as to whether the consternation would have been greater if it had appeared that the NSA did not carry out such monitoring. C.f. O.S. Kerr, 'Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't', *Northwestern University Law Review*, Vol. 97, 2003, http://ssrn.com/abstract=317501.

2.1. Camera surveillance in public and non-public places.

The use of audio-visual equipment (cameras) is closely connected to surveillance. Cameras allow real time surveillance as well as retroactive surveillance. It has been argued recently that it is the real time surveillance that makes cameras in public places particularly effective, as action can be taken directly once a situation appears on camera.

With respect to surveillance in real time, the role of IT in the process may not be immediately apparent: in principle what is involved here is a screen that must be monitored by a human supervisor. However, these days the video signal is often not recorded and broadcast in an analogue form but in a digital form. That opens up various new possibilities. These video images can be more easily stored and transmitted to differing locations. That is particularly the case if the camera has a network connection and can communicate via the Internet protocol. These images could then, in principle, be accessed via any computer connected to the Internet. Digital image processing is now also a possibility, allowing the computer to analyse and process the material at various levels. The following examples illustrate this technique (ranked, more or less, according to the complexity of the operations):
- Motion detection or similar techniques that make sure that only the recordings in which something has happened are shown or stored (for example, where there has been movement or sound).
- Increasing the sharpness and contrast of a recording, so that it is possible to zoom in on details (such as a number plate or a person's face).
- Facial recognition: identifying a person by recording that person's face. Great steps forward have now been made in the application and processing of this form of biometric information[4]. With this technique, it is already possible to identify someone in a crowd (although the person's face must, at a certain moment, be visible). The technique has not encountered much resistance, probably because recording someone's face is seen as less threatening and less intrusive than, for example, an iris scan.
- Where cameras are positioned at more than one location, it becomes possible to track and trace people for a certain distance and over a certain period of time on the basis of facial recognition. This technology means it is possible to make a detailed analysis of where a given person is at any given time in the area covered by the cameras.
- Object pattern analysis: this system makes it possible to look at images where something out of the ordinary is considered to be taking place. This system makes it possible to track deviant behaviour, for example, where someone remains motionless at a particular location for a much longer period than average. The technique also makes it possible to isolate deviant patterns, for example cars or lorries that exhibit an unusual route pattern.

[4] This is dealt with in more detail below.

- The use of images from special satellites which have advanced cameras and sensory equipment making it possible to localize, identify and follow people or goods.

It is clear from the above examples that the 'traditional' form of camera surveillance, whereby analogue imaging is relayed via specific, separate infrastructure to a location where the pictures can be seen or recorded, has been overtaken by new forms of technology. In particular, the fact that digital cameras based on Internet technology do not need a separate infrastructure, such as specific cables, is a great advantage. It is, therefore, expected that this technique will supersede the analogue version in the years to come.

2.2. Surveillance of telecommunication

As well as extensive camera surveillance, the monitoring of all forms of telecommunication has also become large-scale. That monitoring applies not just to telephone and fax messages, but also, and increasingly, to data traffic on the Internet.

From a technical viewpoint, in most cases it no longer matters what sort of communication is involved; even speech can often be directly digitalized and then transmitted. Furthermore, there is little point in monitoring or tapping data on the basis of which type of communication is going to be the subject of the surveillance. It is usually not possible to distinguish these types before the data has been received and decoded. The decoding establishes, inter alia, what type of data is involved (digitalized speech or computer data etc). However, it is also quite likely that the sender of the data has sent them in an encrypted form. This is, in principle, very easy where digital data are involved. Trying to decrypt without the right key can be extremely difficult and time consuming, in particular when a so-called strong form of encryption has been used. Even the use of technology does not mean this problem can be easily solved. This is why authorities have considered placing encryption under legal regulation. In the Netherlands, an attempt was made to make the users of encryption provide the data for decryption where a criminal investigation was concerned.[5]

A specific form of surveillance, entailing the surveillance of people rather than of telephone or data traffic, allows people to be located, based on their mobile phone data. This information can be derived from one or more transmitters for mobile phones. It makes it possible to determine who was where (in the vicinity of one of these transmitters) at a certain time, at least if the mobile phone was on. This technique is now used regularly to follow a suspect. However, the use made of this data by the Rotterdam police, to send sms messages to all those

[5] This provision never became law. Nor did the rule that encryption keys had to be deposited with 'Trusted Third Parties' (TTPs).

who had been in the vicinity of the football stadium at a certain time, was new, at least for the Netherlands. Of interest here is that the data of bystanders was used for the purposes of a criminal investigation, not just the data of those suspected of a criminal offence. In itself, this may not seem so spectacular, its effect was arguably no different from the traditional door-to-door police inquiry, but the scale of the application and the infringement of the privacy of those bystanders led to a heated discussion in the Netherlands.

For this sort of location data, as well as data traffic itself, it is obvious that the registration and storage of such data can be of great important for retrospective monitoring. European law has already been introduced to make this possible.[6] Nonetheless, its introduction has met resistance from providers and Internet user organisations, such as 'Bits of Freedom'.

2.3. Entry control; identifying persons and goods

The time that entry would be granted to a person based on no more than an identification card, specifying the carrier's name and photograph, is drawing to an end. The traditional identification papers are simply too easy to copy. It is, therefore, not surprising that measures have been taken to make passports, driving licences and similar forms of identification more difficult to forge. The newest weapon against forgery is the use of digitalized biometric information as a means of identification.

Biometrics (literally 'measuring life') has quite a long history. The use of the finger and handprint for identification was known in China in the 14th century. In Europe, fingerprints have been used as a means of identification since the end of the 19th century, based on a system developed by Richard Edward Henry of Scotland Yard.[7] Fingers are not the only parts of the body, however, that can be used for identification purposes: hands, eyes (the iris and retina), the face, the voice and the DNA itself can be used. However, they all require specific technology. The certainty of identification they provide may vary. DNA is generally regarded as being the most accurate and reliable biometrical method. The disadvantage of using DNA for identification is that the process requires considerable time and cost, whereas an iris scan, a face scan or a fingerprint can be carried out quickly and cheaply. It is for these reasons, that the latter techniques are the ones used at entry points.

IT plays an important role in the use of biometric techniques. For example, the characteristics of a fingerprint are normally stored in the form of a so-called

---

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[7] A. K. Jain, L. Hong, S. Pankanti & R. Bolle, 'An identity authentication system using fingerprints', *Proceedings of the IEEE* 85 (9) (1997) 1365-1388.

template. The accuracy with which that process takes place determines the dimensions of the template and also its reliability. The template can be stored in a memory chip which, for example, can be used in an identity card.

Not only persons, but also goods can be identified and traced. One traditional form is the traditional metal detector, for example a screening doorway at airports, which makes use of a magnetic field. Other techniques that are increasingly being used include MRI scans, microwave radar registration and microwave dielectrometrics, each of which are capable of detecting specific types of objects, for example in baggage. Explosives can be detected by, inter alia, 'Explosives Trace Detection' (ETD), a relatively cheap system in which traces of explosive materials are traced by way of samples, and by 'Explosive Detection Systems', which uses expensive automated scanners with x-ray capacity in order to analyse the content of packages and suitcases. Similar techniques are available to detect biological weapons.

All these techniques have in common that they make use of the existing characteristics of persons or goods. It is, however, possible to track a person or goods by means of a tagging system. With respect to goods, a good example of this form of surveillance is the security barcode label that is now found on many products. A similar application can be found in cars and scooters, enabling stolen items to be returned to their rightful owners. One technique that is of much interest at the moment is RFID, 'Radio Frequency Identification'. It functions in the same way as the security bar code, but it is so cheap and so small that it can be inserted during the manufacturing process of virtually any product. This technique could replace the barcodes as an effective means of preventing shoplifting as it could be used to trigger an alarm once the exit has been passed. The privacy aspect of this development, as it is, in principle, possible to collect information unobtrusively about what products a person has, has led to much discussion.[8] An example of persons being tagged is the electronic ankle tag connected to the telephone to enable electronic house arrest.

Finally, mention must be made of the GPS, the 'Global Positioning System'. Apart from being used for navigational purposes, this system can also detect the precise location of a person or a thing, for example a car. If this information is then passed on to the police, such as via a GSM connection, it makes it much simpler to track down persons or stolen goods. When this system is applied to persons in the form of an ankle tag, new possibilities arise enabling the detection of a person's movements who is subject to electronic house arrest.

[8] About RFID: Government Accountability Office (GAO, *Information Security, Radio Frequency Identification Technology in the Federal Government*, WWW, <www.gao.gov/new.items/d05551.pdf>, 12 October 2005.

2.4. Techniques for the detection and prosecution of crimes

Many of the techniques described above are suitable not just for the purposes of crime prevention, but also for detection and prosecution when a crime has been committed. For example, cameras can be used for face recognition, data from data exchanges and location data can be stored by computer and biometric methods can be used. Such techniques affect criminal procedure; evidence obtained through the use of highly advanced technology[9] must comply with the same standards of validity and reliability as evidence obtained in a more traditional way, for example by witness statements. The use of new technology can cause problems for judges; their lack of familiarity with the technology involved means they have to rely heavily upon the expert opinions of those familiar with the technology. It is of great importance to deal with this problem as it is likely that the use of evidence obtained by technology will increase rather than decrease.

3. Constitutional rights

The democratic, constitutional state is the most common form of authority in the modern Western world. Possibly the main principle is that of the rule of law: the authorities are subject to the law and may only act within the existing legal framework. Constitutional rights are protected through the separation of powers. Ultra vires actions by the authorities may be investigated and held up to judicial review. In the following sections, attention will be paid to some of the constitutional rights issues which have arisen because of the application of surveillance technology.

3.1. Privacy versus safety?

One opinion that is often voiced is that people find it unpleasant to be spied on and to know that their movements can be monitored later. However, when members of the public are asked if they would like to see more CCTV or more uniformed policemen on the street, the vast majority answer in the affirmative; most people apparently find a police presence on the streets reassuring. Is it, then, a question of finding the right balance: yes to surveillance in itself but no to surveillance in an extreme form? If that is the case, it implies a remarkable conclusion; that we actually want a certain level of uncertainty. It is clear that the public estimates risk not just in terms of the chance of something happening or the effect of that something happening; other considerations must also play a role. It is otherwise not possible to understand how some people behave in traffic or why they smoke.

[9] C.f. B. Budowle, G. Carmody, R. Chakraborty & K.L. Monson, 'Source attribution of a forensic DNA profile', in: *Forensic Science Communications*, July 2000, ISSN 1528-8005.

With respect to the relationship between privacy and safety, the question seems to be: "How much privacy are people prepared to surrender in order to increase their safety?" These two basic rights, the right to privacy and the right to protection, seem to be uneasy partners. However, the question is not as straightforward as it may seem. Why is it that most of us are perfectly prepared to have our baggage examined in airports but resent our past being looked into? Privacy is not a clear concept. It may encompass various dimensions, such as the spatial dimension. This spatial dimension is concerned with our freedom of movement: if there were no controls at airports would we feel freer or less free to go as we pleased? And if our past is looked into, would the examination of our baggage no longer be necessary? Privacy and safety do not have to be opposites, but the one can affect the other. It would be hard to think of something that was a greater infringement of a person's privacy than having to undergo a body search, or having personal belongings searched, or even the threat of it. Nevertheless, people accept all these infringements in airports and many other situations where the person and personal belongings are inspected.

3.2. Who threatens constitutional rights?

Constitutional rights have a special place in the relationship between the authorities and members of the public. Rights and freedoms have been formulated to protect citizens against the arbitrary use of power by the authorities. In the course of time, the concept of the horizontal working of constitutional rights has developed. The right to personal privacy is not just operative between the authorities and the public, but also between members of the public themselves. In former times, it was necessary to protect citizens from the arbitrary behaviour of the authorities (or the monarch). Today, in the developed democratic states of the West, the authorities are subject to public review and may be held responsible for infringements. It would seem that the danger to constitutional rights emanates not so much from the authorities but from those who reject authority. Fear restricts the movements of citizens, either because they are not sure if it is safe to take an airplane or the local metro, or to voice a possibly controversial opinion. It would now appear that it is often the authorities that have become the champion of constitutional rights, rather than the body suspected of flouting them.

The question now before us is which aspects of privacy must weigh heavier in a given situation? Whether surveillance technology is applied, or whether someone is placed under such surveillance, is often not one made at an individual level. This runs counter to the present day tendency whereby the individual plays a central role. That is because the protection of privacy is not just an issue for individuals; it must also take collective needs into account. Paradoxically, it would seem that the 'protection' of constitutional rights justifies a certain selective infringement of those rights. This can be explained in terms of the relative utility of the application. To the extent that it affects

individuals, legislators must be careful not to make unwarranted generalizations, as this could result in the public rejecting the use of technology. This would be a pity as when people were asked whether they would support the registration of DNA and the use of extensive databanks holding sensitive information, those asked apparently attached more importance to safety than to privacy.

3.3. Suspects and non-suspects

When it is contended that surveillance technology infringes personal privacy, one aspect that is brought to the fore is that surveillance technology does not differentiate between people; the surveillance entails the monitoring of both suspects and non-suspects. Modern technology means that an innocent person's privacy can be infringed as a side effect of tracking a suspected person's movements. This breaches the legal principle that coercive measures should only be used against those for whom reasonable grounds have already been established to suspect them of criminal activity.

However, firstly, it is not the case that the authorities, including the police and the judiciary, may only do what has been specifically laid down. To a certain extent they may, just like ordinary citizens, ask people questions, telephone people and send sms messages. These activities cannot be categorized as coercive measures, for citizens are free in deciding whether to answer or not, nor are such activities limited to 'suspects'. That people do not like to be spoken to by the police, that they could feel intimidated, means that the police must be careful in the way they approach the public, but there is no reason, and indeed it would not be desirable, to fetter their capacity to ask questions. This applies even where a person refuses to answer the question, meaning he could become a suspect, and as such the subject of coercive measures. Nor does, for example, receiving an sms from the police mean that the recipient must be considered to be a suspect. During an investigation, the police need to contact people as potential witnesses.

Secondly, the rule of law does not prevent the authorities from using coercion against someone who is not a suspect. The law often lays down a general competence for a certain activity. For examples, surveillance cameras may be used to detect speeding. Checking that drivers do not exceed the maximum speed limit does not make all road users 'suspect'.

4. Conclusions

The use of surveillance technology need not, in general, be seen as irreconcilable with the right to the protection of personal privacy. Safety is not in opposition to privacy, but an aspect of it. Furthermore, it could be argued that the right to personal privacy is not an absolute right; other factors can be taken into account.

A general application of surveillance technology does not have to be contrary to the principle of criminal procedure that there should be reasonable grounds to see the subject as a suspect. That is because surveillance technology is not in itself a coercive measure. Surveillance technology is a means that is not confined to the purposes of criminal procedure. A person may cooperate, for example at a check-point, without having first to be identified as a suspect. There are also positive effects, such as the use of technology to increase the usefulness of services to the public and to respect the enforcement of basic rights. Although arguably more vigilance is required to guard against the threat posed by those who reject the established authorities rather than the authorities themselves, care must always be taken to prevent the abuse of power. Surveillance technology has already increased the power of the executive and the legislature. Other applications of IT, such as the Internet and decision support systems, have also served as an instrument of the executive. It seems that the judiciary, that is supposed to play such an important role in the protection of constitutional rights, is losing ground. [10]

Technology not only makes surveillance a more practical matter; in a more complex way it leads to a new organization of state power. This is possibly the most important point of discussion with respect to legal and social change as a response to technological progress. It can be argued that a new fourth power is inevitable[11]; just as the appearance of an executive power was inevitable once the law could not only be written but also printed. That development led to the large-scale bureaucracies we seen today. The technical possibilities offered by computers and the Internet will not be less far-reaching. The appearance of a new power, a monitoring power, would seem likely. We have already witnessed this development in the form of such institutions as the Ombudsman, the National Audit Office and the National Competition Authority.

This new power, the result of social change, will have far-reaching consequences for the law, and for the functioning of the state of law and the legal profession. The growth of the executive power led to large-scale bureaucracies. Such organisations may be of use, but can easily lead to excesses. The systematic monitoring of those in charge of the use of surveillance technology in a democratic state is a necessity. In a globalizing and increasingly technological world, democracies will need monitoring powers to supervise the use of surveillance techniques. The old question ‘Quis custodiet ipsos custodes’ (who should monitor the monitors) has lost none of its relevance. [12]

[10] Mulder, R.V. De, ‘The Digital Revolution: From Trias to Tetras Politica’, in: Snellen, I.Th.M. , Donk, W.B.H.J. van de (Eds.), in: *Public Administration in an Information Age. A Handbook*, p 47-56, Amsterdam: IOS Press 1998, ISBN: 90 5199 395 1.
[11] Idem.
[12] More detail on this discussion may be found in the concluding remarks of this book.

Conclusion

P. Kleve, R.V. De Mulder & C. van Noortwijk
Erasmus University Rotterdam

1. Introduction

Technology for surveillance and monitoring has, in today's society, become commonplace. It appears in various forms, for example, in the form of a warning system. As a consequence of the disastrous tsunami in December 2004, a tsunami warning system was installed in the Indian Ocean. In the Netherlands, because of the risk to public health caused by air pollution, certain so-called 'sniffing poles' were installed in the Rotterdam area. They measure the level of air pollution and when a certain limit is reached a warning system is activated. Many processes are now monitored with the help of technology; hospitals use technology to monitor the state of the human body and financial obligations are monitored by computers that send reminders and final demands if the payment has not been made on time. Moreover, camera surveillance is on the increase both in the public domain and on private property. Visitors to a company could well find that instead of signing in using the traditional guest register, they are required to undergo a video registration by complying with the friendly request to look in the camera and give their name.

2. The increasing importance of monitoring

Monitoring and supervision, safety and security form an area of multi and interdisciplinary study in which a lot of dilemmas in society come to the fore. Technological developments can appear to be out of control. The climate is changing, the world is globalizing at a fast rate, states loose control over their territory because of the Internet and low transport costs for goods and people. Terrorist threats and the threat of the proliferation of arms of mass destruction are constantly discussed in the media. These seemingly unmanageable developments, with which citizens and governments are confronted, engender a feeling that more control is needed, a better grip on what is happening is required, and more transparency must be demanded.

These needs bring with them a multitude of dilemmas. Empirical and normative questions arise such as: How is more control to be obtained? What will it cost? Are monitoring and control always desirable? Or will the cure be worse than the illness? These questions concerning monitoring and control are also interesting from another perspective: Which "enforcement system" is applicable? Monitoring and control can be carried out by the criminal law system, but also by fiscal competences or with the power derived from administrative law. This means that questions are raised with respect to information interchange between

these systems, but also about the fundamental properties of the criminal law system, the administrative law system and other systems that are meant for monitoring, control and law enforcement. Responsibilities are changing. Non-criminal law organisations have also taken on the responsibility for prevention and/or repression of crime and other unlawful behaviour. Furthermore, an important element is that self-regulation and the privatisation of safety and security have become of increasing importance in society. This has, in turn, created new dilemmas.

Finally, these developments have had an impact on the role of large corporations and vice versa. National governments and intergovernmental organisations, like the OECD, ILO and the European Union, have shown an inability to regulate multinational corporations effectively. The increasing lack of trust has lead to more external monitoring and supervision of firms. However, both governments and their new monitoring organisations have had to agree that this external monitoring is hardly effective or efficient unless the corporations involved feel responsible for behaving appropriately and are prepared to comply with regulations.

3. The seminar

The papers presented at the seminar could be divided into three categories: concerns, tools, and theory. The articles in this book have been presented on the basis of these three categories. The resulting three sections also represent a different approach to the problems of monitoring and supervision.

In the concerns section, three areas of concern are addressed: concerns with respect to privacy as a consequence of the increasing levels of data retention, the safety of children who communicate via the Internet and the protection of personal data. The approach adopted in this section is a traditional legal one.

In the tools section, more concerns are expressed, but the emphasis on the ways in which these concerns can be dealt with is different from the legal approach that characterises the first section. The concerns raised in the tools section are: plagiarism and fraud in education, how to create an international digital working environment for legal professionals in which freedom of speech, the right to access to information, copyright, privacy and safety and security are protected in a balanced and coherent way, and finally, the dangers of ambient intelligence. In all these papers, the appropriate tools are analysed or suggestions are made in order to deal with the concerns identified.

In the third section, again more concerns are expressed and tools (other than legal tools) are proposed. However, the approach in the third section differs from that of the previous two sections: the concerns and tools are considered in a theoretical way that combines the legal, technical and economic approach. An

important foundation for this form of analysis is the use of a model of man. In both papers, the REMP model is applied. The REMP model is relatively new, certainly compared to the traditional legal approach. It can be argued, that it is the new theory, possible even a new paradigm as meant by T.S Kuhn[1]. The REMP model is an important theoretical tool for understanding individual motivation, the relationship between authorities and individuals and the relationship between individuals. It is therefore very relevant for an understanding of the balance between monitoring and surveillance on the one hand and constitutional rights on the other hand.

4. The REMP

Many social scientists base their research on a sociological model of man. This model states that people will behave in a way consistent with the norms of the group to which they belong. However, modern economists usually use a different model of man, the REMP. REMP stands for the Resourceful, Evaluative, Maximising Person[2]. The basis of this model is the homo economicus. The homo economicus originates from economic theory and has a history starting around the year 1900. The REMP is a more sophisticated version of the homo economicus, who was mainly interested in money. Like the homo economicus, he REMP was developed to try to explain the human decision-making process. According to this model, man is a rational being who considers alternatives and then chooses the one which will be of most value to him. He uses information in this decision-making process where available and if the cost of the information is less than the value of the information.

This assumes that people have a utility function that indicates their preferences where there is more than one alternative and that they will try to maximise their level of utility. In choosing the alternative that has the highest value, an individual makes his own estimate of value. What is considered to be the highest value is subjective and will vary from person to person. The value does not have to be financial; it could be measured in terms of usefulness or happiness to that particular individual.

The further development of the homo economicus model into the REMP model owes much to two economists, William Meckling and Michael Jensen. It is not contended by its makers that the REMP model provides anything more than the basic building blocks to explain human behaviour, or that it will elucidate every single individual's behavioural pattern. The essence of the REMP is that people exhibit four basic characteristics which will determine their behaviour: every individual is an evaluator, his wants are unlimited, he is a maximiser and he is resourceful. Processes are studied from the perspective of methodological

[1] Thoma Samul Kuhn, *The structure of scientific revolutions*, Chicago: University of Chicago Press 1962.
[2] Michael C. Jansen and William H. Meckling, "The Nature of Man", *Journal of Applies Corporate Finance*, Summer 1994, V. 7, No.2, pp. 4-19.

individualism, in other words described, explained and predicted on the basis of the behaviour of individuals. The REMP is an individual who tries to maximise his own utility in all his decision-making. Ideologically, that may sound undesirable. However, in practice it is often the case that individuals see their own interests are served by taking others into account and by interacting with the outside world in a creative and anticipatory way.

5. Factors that influence the growing importance of surveillance technology

Consistent with the REMP model, individuals, organisations and states have developed and used surveillance technology and have made use of various techniques. Information in a digital form makes it possible to use techniques that were unknown only a short time ago. Equipment can be used not only for (passive) registration, but also for analysis and interpretation. One example of the combination of techniques can already be found in American airports: video cameras utilising image recognition software used in combination with pre-existing information. This method is also used to deal with hooligans at football matches, rather than checking their individual club cards. Surveillance technology also includes fingerprint and DNA techniques. These methods are not only used for active control, for example to gain access to restricted areas, but also retroactively to reconstruct a given situation. Digital technology is also responsible for the increasing use of biometric techniques.

Surveillance technology has, without doubt, made an impact on society. *Technological advances*, in general, have been considerable over the last 150 years. It is a period that has seen the Industrial Revolution superseded by the Information Revolution. Technological applications are numerous and various, and have become integral to the society we know today. That technology should be used for surveillance is, in this context, not extraordinary. Indeed, its application is rather obvious given that the techniques are easily applied to surveillance and that society as a whole has acquired a more technically orientated character.

What perhaps is less obvious is that technology offers diverse possibilities with respect to complex relations. *Management* is of vital importance in carrying out tasks, whether those tasks are related to business or public sector organisations. Technology can assist in planning, control and communication.

It has also affected people at an individual level. That there are more and more options open to people, and more and more information, makes it necessary for people to approach decision-making *rationally*. Increasing wealth and economic independence have prompted a process of individualisation. Traditional social structures have become less a matter of course, indeed they are sometimes

experienced as obstacles in the way of reaching individual goals. The rational model of man is arguably now the best predictor of human behaviour.[3]

These aspects are partly responsible for, or augment, the tendencies listed below:

Globalisation
Technology has increased mobility and thereby accelerated the process of globalisation. Not only can people travel more quickly from place to place, but communication has also become much easier and faster with the advent of Internet and the mobile phone. The world order, as we have known it, is changing and that makes directing, controlling, enforcing traditional norms or obtaining an overview of society in general more difficult. Change brings uncertainties with it.

Resistance
The use of technology has become commonplace. It is, therefore, not surprising that technology has been used for various forms of surveillance and for the enforcement of established legal aims. Nonetheless, the implementation of new technology invariably leads to public resistance. In the time of the Industrial Revolution, it was argued that the working man would see his livelihood taken away from him by a machine and that poverty would be his lot. An updated version of this fear was voiced with respect to the Information Revolution: there would be massive unemployment because office workers would become superfluous. In both cases, although some forms of traditional work did die out, new work replaced them. The Industrial Revolution took people out of the fields and put them in factories. The Information Revolution took people from filing cabinets and put them at the computer. In both cases, women became an increasingly important part of the salaried workforce. The general level of welfare in the technically progressive West has never been so high. Yet despite a certain level of public familiarity with technological applications, surveillance technology has met with some public resistance. It is, however, very likely that that resistance will be overcome. Surveys already indicate that members of the public feel safer where there are cameras, for example in shopping centres.

Ease of use for all
There are many useful applications for technology and technology is becoming increasingly accessible to the public. Simplicity of use, smaller sizes and lower prices have meant that the kind of equipment once only found in a professional setting has now become a consumer product. There is, however, a darker side to this development. It has become much easier for individuals, even those without much technical knowledge, to use modern technology for the purposes of terrorism or other criminal activities. The potential harm they can cause is huge.

[3] See note 2.

Businesses can be seriously undermined by computer viruses. Members of the public can be the victims of terrorist attacks on public transport. Public facilities in general form other potential targets, such as the energy supply or drinking water. The use of surveillance technology must be seen against this background; technology is used to combat the harmful use of other forms of technology.

Changing norms
The most important factor in the implementation of new technology is the expected level of efficiency and effectiveness. The use of technology depends on what it can achieve and how much it costs. Less obvious perhaps is that it is also responsible for a shift in norms. Technology has made things possible that were once not possible; this ranges from copying films from the Internet at home and interactive television to in vitro fertilisation. New technology has made existing norms less self-evident; indeed some norms seem to change with the times. A person who would not dream of going to a cinema without paying for a ticket, could easily be prepared to download a new film at home.

If the technology is available, it is not difficult to predict that it will be used for surveillance and detection, geared up to the needs of the day. This shifting in norms outlined above will also affect the use of technology for surveillance, detection and law enforcement. It affects those who introduce the technology as well as those who are against it. Those working in the public sector not infrequently show a rather creative approach, which does not always conform to the demand for legitimate administration. Although the 'creativity' of public officials must be monitored, it would not be efficient to require a change in the law before new applications of existing technology can be implemented. The police and the judiciary would then be constantly one step behind. It is, however, necessary to evaluate the law in order to determine whether the creative use of technology falls within existing legal parameters or whether new laws are necessary to legitimise its use or forbid its use.

6. Technology and social control

The use of surveillance technology does not always entail an extension of an existing competence. It is more often a means by which that existing competence becomes more effective and efficient. The simple fact that something is useful, or more useful than it used to be, leads in itself to a certain shift in norms. It is, however, important that it is borne in mind that technology is itself primarily a 'means'; it is a means to make possible those things people find useful. Surveillance technology is, in this sense, a tool to enforce norms, in the same way as the law itself is a tool to enforce norms.

When people go on holiday, they often ask their neighbours to keep an eye on the house. If someone hangs around the deserted house, the neighbours might ask whether they can 'be of help'. That a police car would drive past the house

more often while they were gone would also be welcome. In former times, it was far more common for people to keep an eye on the behaviour of others. There are various reasons why that is less the case today. One reason is the tendency noted above for increased mobility and individualization. People are also aware that an intervention may not be without risk.

The social control and cohesion typical of society several decades ago no longer exists, at least not in that form. It is generally recognized that social control and social cohesion have a useful function. The gap left by the lack of social control can be filled by the use of technology; it can give social control and social cohesion form once again. In any evaluation of surveillance technology, factors to be taken into account are not only the costs and disadvantages, but also what it contributes and its social advantages.

7. Technology and solidarity

Whether a decision is made to use surveillance technology seems to be largely a matter of efficiency. Efficiency is a norm more often associated with the private sector, yet this consideration is relevant with respect to the public sector as well. Although it would seem that efficiency as a norm has achieved greater acceptance in the private sector than the public sector, it is not the case that the aim of efficiency is without criticism in the private sector, for example with respect to commercial profit at the cost of service. When this criticism is analysed, it would appear that the services sacrificed are those that were not sufficiently profitable or provided at a loss. What the private and public sectors share is that those individuals who are affected want a result that suits them, even if it is disadvantageous for others, although they are not personally willing to contribute more. This leads to a conservative approach. Efficiency as a criterion is nevertheless an important guarantee of solidarity. The use of technology can promote efficiency.

An important question is to what extent people will be prepared to contribute financially to an expensive system of redistribution, in which not all those who are intended to benefit from the redistribution do so, and some of those who do benefit were not intended to do so. Many of the organisations charged with the task of redistribution are founded on the principle of solidarity. This solidarity could be in the form of unemployment benefits, insurance, housing or social security benefits, contribution to church funds, or charitable organisations. An important factor here is the tendency pointed out above; the increasing complexity of society, increased mobility and individualization. As a consequence, it has become more difficult to reach those who have the right to such assistance, and more difficult to prevent fraud by those who do not have the right to this assistance. This puts solidarity under pressure and makes it crumble away. Surveillance and control could be made more efficient by using

technology, for example to prevent the fraudulent use of social security systems, and indeed its use could be demanded.

In practice, it is no longer possible to implement complex legal projects without the use of technology. Technology has, in turn, influenced the content of these legal rules, as the automation process itself may impose certain requirements and restrictions. Creating and keeping consensus depends on correct implementation, certainly in the long term. Using technology as a means of control or as a means to support the enforcement of control, could give those involved a greater feeling of certainty. It is because we have computers that we can refine general rules, so that relevant individual circumstances can be taken into account. It is this very ability to distinguish between cases that makes it possible to uphold the principle of equality. In this way, technology could contribute to a feeling of solidarity.

8. From Trias to Tetras Politica

Information technology and in particular surveillance technology will produce fundamental changes in the way in which the state operates. This can have a positive effect on legal administration. Modern legislators in liberal, democratic states should take it upon themselves to enter all legislation that is in force into an information system that would be accessible to everyone. In this way, everybody could monitor the state's legislative activities.

However, the use of technology could alter the current balance of power with respect to the administrative and judicial powers. Furthermore, it will provide the administration with new means to increase its control of society. Is it possible to avoid or reduce the risks that may arise for citizens?

A critical assessment of the trias politica is required[4]. It traditionally consists of the following powers:

- Judicial power
- Legislative power
- Administrative power

Legislation and administration are both concerned with initiating and acting, whereas the judicial power is mainly concerned with supervising and correcting. The administrative power is associated with the large-scale exertion of state power. This is illustrated by the following 'double dichotomy':

[4] Mulder, R.V. De, 'The Digital Revolution: From Trias to Tetras Politica', in: Snellen, I.Th.M. , Donk, W.B.H.J. van de (Eds.), in: *Public Administration in an Information Age. A Handbook*, p 47-56, Amsterdam: IOS Press 1998, ISBN: 90 5199 395 1.

	supervising and correcting	**initiating and acting**
not suitable for large-scale exertion of power	judicial power	legislative power
suitable for large-scale exertion of power	?	executive power

In the cell, marked with "?", there is space for a fourth power that is supervising and correcting as well as associated with the large-scale exertion of power. Such a power could be called the 'monitoring power'. Institutions like the government audit office and the ombudsman are probably the first signs of the new power.

The monitoring power would not be concerned with individual cases - those would stay within the realm of the judiciary - but with systematic, empirical investigation into the functioning of the other powers, including the judiciary. All the formal powers needed would be the competence to access all the information that the other powers have access to as well as the competence to interrogate the members of the other powers.

The **Tetras** politica

Judicial power	Legislative power
Monitoring power	Executive power

The work of the new power is not limited to monitor the other powers solely on the basis of conformity to the existing legal rules. The monitoring power will evaluate and criticise the other powers in a more general and comprehensive way. Not only legitimacy, but also effectiveness and efficiency would be investigated. Citizens are better off with the ombudsman than with a court for certain complaints. The ombudsman could carry out empirical research into the way civil servants have acted in general and suggestions for improvement could be made. On the basis of these investigations, the citizen could put his case to a judge if that would still be required. Furthermore, for the evidence to be produced with respect to certain complaints, for example in discrimination cases, statistical data are necessary. The victims in such cases would usually not

have the means to produce these data themselves. Finally, for all citizens it would seem to be an attractive prospect if the judiciary would be systematically monitored by an organisation that has the relevant powers and the skills for such monitoring.

9. Monitoring the monitors

In conclusion, surveillance technology gives rise to serious concerns in the modern world. Undoubtedly, there are many advantages to be gained from this new form of technology, but there are certain pitfalls which could compromise safety or other basic rights. On the one hand, citizens and organisations are threatened with a multitude of dangers from others, which could include even their own governments. On the other hand, there is the danger that governments, in their eagerness to protect citizens, will overreact and their damage control operations will engender more damage than the actual risk of harm itself.

Nonetheless, organisations and governments should not be prevented from using surveillance techniques, particularly if these techniques are used to reduce risks to safety and security. This does not, however, imply totally unrestricted monitoring, particularly when such monitoring could unnecessarily infringe fundamental rights such as privacy and information rights. In this book, a useful analysis has been produced[5] of the costs and benefits involved in monitoring and supervision. Based on this analysis, the conclusion would seem that more monitoring is required. A new monitoring power is needed that, like the judiciary, monitors, although not necessarily rectifies, the actions of governmental organisations and others that are regularly involved in surveillance. This monitoring could be carried out systematically and on a much larger scale. The competence of this new monitoring power would simply be the right to access information that is relevant to fulfil its task. This change to the checks and balances within the modern state organisation would see the expansion of the Trias Politica to a Tetras Politica.

[5] L.T. Visscher,."Monitoring and Supervision in the Economic Analysis of Safety and Security" , p. 97 of this book.