THE USE OF

PET

Privacy-Enhancing Technologies

AS A COMPLEMENTARY TOOL FOR PRIVACY
PROTECTION IN ONLINE ENVIRONMENTS

PER HAMMARSTEDT, LL.M.
JANUARY 2000

A Pre-Study Financed by KFB, the Swedish Transport
and Communications Research Board

Swedish Institute for Systems Development

Content

Summary

Personal data in itself is becoming an economic resource. Sometimes even forming the core of online business models such as in the case of *infomediary* companies. This development is increasingly establishing also in the European market.

However, the knowledge in Europe in general about individuals' online privacy preferences is limited, especially in the context of e-commerce and in other use of online services. The best way to protect these presumptive preferences is not necessarily through a body of strict online legislation and regulation framework only. It has come to our knowledge that data legislation suffers from non-compliance. Seeking complementary ways to protect privacy in online environment ought to be (or will soon become) an issue on every privacy researchers' or advocates' agenda.

One ingredient in a modern online privacy protection is the use of Privacy-Enhancing Technologies (PETs). Important advantages with a P3P concept are that traditional practices (and privacy policies) of Web sites will be challenged/threatened. Hopefully this challenge also makes service providers in general a) aware/reminded of privacy interests and b) to outline legally adequate privacy policies and comply with them.

Irrespectively the chosen system used to protect online privacy, i.e. by use of legislation and other regulation, self-regulatory measures, contracts, or by technology, they all are expected to work effectively. The criteria of effectiveness reflect the ability of every system to a) deliver a good level of compliance with the rules set, b) to support and help individual data subjects, and c) provide appropriate redress to individual that suffers from privacy infringement.

The overall mission statement is to *earn knowledge about possibilities and impediments of implementing European legal framework and self-regulatory measures, and with this knowledge use a co-regulatory approach to online privacy protection in accordance with common indications of online privacy preferences*.

Thus, the focus in this pre-study and the outline of a forthcoming project on online privacy protection is on the following key issues:

- Users' trust and privacy preferences in the online marketplace.
- The appearance, use, and meanings of privacy policies.
- The implementation of Privacy-Enhancing Technology (PET) in forms of a P3P agent as a tool for privacy negotiations strengthening user control of personal data.

This paper is a summary report on a PET pre-study project, financed by KFB, the Swedish Transport and Communications Research Board. For further information in connection to each section, please notice referred Web site constructed especially for this project: http://www.integritet.nu (Swedish version is due to international cooperation limited to certain sections available via the Project Web site).

1 Introduction

This study aims to take a closer look at and understanding of Privacy-Enhancing Technologies (PETs) and the context in which they are used, the area of online privacy.

The concept of privacy protection has become broader and deeper due to the relatively wide spread use of information technology. By tradition, the legal framework in Europe developed to protect privacy is mainly designed after the prerequisites arisen from the use of database technology in the public sector. Government has been given a prominent role in fostering social welfare and the development of markets and technology has played a limited role.

The wide concept of privacy protection is today rather limited when it comes to the use of Internet technology. In Europe, a relatively small amount of services demanding identifiable personal data is in use. The development of electronic commerce[1] and new electronic communication services overall has been rather slow. The question of *online privacy* has hence been of rare occurrence in the public debate. Instead, focusing on the implementation on the European data directive, the questions have been limited to the requirement of consent. To the legislative caveats to mention a friend or a politician by his or her name on a Web site. Online privacy and marketing on the Internet (for instance) has not until recently been addressed by a Swedish governmental study.[2]

However, the forthcoming development of e-commerce, expanding use of modern technology creates and leaves vast amounts of personal data behind each transaction in forms of electronic tracks or footprints.

In the US, many new online services and products are daily being introduced. They are slowly making their entrance into the European market, with ease since they are based on Internet technology. There are many examples showing how the existence of personal data has become a great market on its own (due to profiling and mining technologies), sometimes even a prerequisite for new corporations in the information market.[3] We will come to these cases later in this paper. The effect of this development is (among other things) that the online industry seeks to find ways to protect consumers' privacy by vary of self-regulating measures. A legislative solution is under consideration but will only become a reality if self-regulation seizes.

Focus in this study is the different means that forms the core of privacy protection in online environments. The understanding of the implementation of legislation and self-regulatory measures in this context is thus of most

---

[1] The definition of *e-commerce* is though open to debate, often used in a careless way without notice of distinction between *commerce* and *trade*. This study follows the definition by OECD in referring to "commercial transactions occurring over open networks, such as the Internet. Both business-to-business and business-to-consumer transactions are included." See OECD, Organization for Economic Cooperation and Development, *Measuring Electronic Commerce* 3 (1997), p.12, available at http://www.oecd.org/dsti/it/ec/prod/E_97-185.htm

[2] Consumers and Information Technology (*Konsumenter och IT – en utredning om datorer, handel och marknadsföring*, SOU 1999:106), for a summary in English, se for instance *A summary of the official report (SOU 1999:106)* available at http://www.kov.se/summary.htm

[3] For an introduction to profiling, see Roger Clarke, Profiling*: A Hidden Challenge to the Regulation of Data Surveillance*, http://www.anu.edu.au/people/Roger.Clarke/DV/PaperProfiling.html

importance. As well as the use of technology itself to improve protection of rights reflected by Internet users' privacy preferences.

Technologies, discussions, and regulation forms and practices development are hence discussed. Thus, it is of interest to combine the European legislative approach with the US attempts to use self-regulation as a privacy regime.[4,5]

In the following section we shall take a closer look at the concept of privacy and issues related to the definition, collection and use of personal data, and the need of control of such data in online environments. The next (third) section describes the essential elements of European legislation and the self-regulatory means adapted in the US. Implementation on the Internet of these rules is the most intriguing question here. An inventory of PETs with a commentary of strength and limits in a legal context forms section four. This shows how the technology itself may be used to protect the interests of privacy. The finishing section (five) holds recommendations to a few desirable steps in order to earn more knowledge of the needs of improvement for privacy protection in the online marketplace.

[4] However, the concept of US privacy must be treated with care in a European point of view since it is *inter alia* highly influenced by social, legal and cultural contexts.

[5] Later this spring, SISU holds a seminar to discuss the herein addressed questions. Hopefully, this paper and attached activities – such as the Project Web site: http://www.integritet.nu – will somehow elucidate the privacy questions that most certainly will be of importance in the nearest future due to the development of e-communication.

2 The Concept of Privacy

2.1 Introduction

The concept of privacy represents many interests of protection rights. These are reflected in laws of camera surveillance, Criminal Acts, Security Acts, Credit Information Acts and Data Acts (when other laws not are applicable) etc.

Thus, one should bear in mind when discussing privacy protection, that the legal framework is not limited to protect privacy in *online* environment. Albeit these questions have been increasingly addressed due to the development of Internet during the last few years. On the contrary, the protection of a privacy sphere in forms of personal data online is in this perspective rather limited, but nonetheless an important issue.

In creating a personal sphere or space free from interference from others, the dimensions may be summarised as the privacy of person, privacy of personal behaviour and privacy of personal data and communication.

It is well known today that the fast technology development has led to uncertainties about how to protect and remain respect for intellectual property and privacy rights regarding the privacy of personal data and communication. This is the case in not just one market. As an example, Zona research Inc. pegs the US business-to-consumer e-commerce market at $63 billion in 2001.[6] Leading market segments include securities transaction, travel and tourism, and durable consumer goods. A new study by the Boston Consulting Group predicts that as much as one-fourth of all US business-to-business purchasing will be done online by 2003.[7] The e-commerce market in Sweden is estimated at $0.3 billion in the beginning of this year[8].

Under this development where more and more of our every day services will be done via the Internet, it is of great interest how and when personal data are collected and processed into customer profiles for later use or just collected without idea what the future use will be.[9] Vast amounts of data are today collected and will soon be possible to sort through, i.e. by use of data mining tools. Data of an Internet user have become to represent an economic value in the online industry. It has been estimated that each customer name is worth 15 cents.[10] Together with other (millions of) online customers, it is not surprising that knowledge about the consumer also is power.[11]

---

[6] ZDnet, http://www.zdnet.com/anchordesk/story/story_4277.html

[7] ZDnet, inter@ctive investor, http://www.zdii.com/industry_list.asp?mode=news&doc_id=ZD2412831&pic=Y&ticker=

[8] Which would be approximately 0.7 percent of total market of business-to-consumer commerce, see, (in Swedish), *Konsumenter och IT – en utredning om datorer, handel och marknadsföring*, SOU 1999:106, p. 45.

[9] For instance, all literature for this study was bought via Internet (www.bokus.se and www.amazon.com etc.), almost all papers and articles, viewpoints, collected from online services, lists, newsletters etc. (The curiosity may make one wonders which of these services shared information with the ones who now and then keep sending unwanted mails etc.)

[10] http://www.callaw.com/stories/edt0614f.html

[11] A free interpretation made for the online market of the "Idola" of Francis Bacon (in his Novum Organum 1620).

The interest of privacy protection is most likely not a fiction of privacy advocates or specialists.[12] Other manor international surveys show that users care for control of use and secondary use of "their" personal data is of importance. In the 9th user survey by GVU in 1998, 72.9% answered that they strongly agree on the question if the consumer should have total control over which Web sites that have access to demographic data about the consumer.[13]

In 1997, the Federal Trade Commission (FTC) reported (in the sweep of 1400 commercial Web sites) that 85% of visited sites collect personal information from consumers. Only 14% of those disclosed a so-called *privacy policy* (or notice) declaring if and what personal data that was collected. No more than 2% of the Web sites had a more comprehensive privacy police.[14]

2.2 The lack of legal definitions

In European privacy protection law there is no definition of the context of privacy. The reasons hereto are, on the whole, its complexity.[15]

Historically, the term "privacy" was first mentioned in the Supreme Court in 1886, when applied to the interests of the US Fourth Amendment in protecting citizens' (property) from unreasonable searches and seizures.[16] Four years later, "The Right to Privacy" was articulated as the *right to be let alone*[17] by the Supreme Court Justice Louis Brandeis and his colleague Samuel Warren.

Later on, the concept of privacy has also become a right referred to as the respect of private and family life, being a fundamental human right.[18]

2.3 Physical and idealistic spheres

One may narrow the concept of privacy down in different areas in which the issues are discussed (public sector, private sector, camera surveillance, searches and seizures etc.). Distinguishing the rights of privacy is necessary. The concept of privacy could be diverged to what are privacy interests of the physical space or sphere (household, car, office, body etc), and to the interests in focus in this paper, the idealistic spheres, i.e. the privacy protection rights regarding *personal data*.

In defining the right of privacy – in a data protection context – David Flaherty offers a descriptive listing of information-related privacy interests reflected in the doctrine. These interests consist of the right to be left alone, to control

---

[12] If it against all odds would be, it will most likely not be so in the nearest future. See for instance, Reg Whitaker (Professor of political science at York University in Toronto), *The End of Privacy, How total surveillance is becoming a reality*. A most interesting analyze over the awaiting surveillance society (a la George Orwell in the 21th century), where there is no room for privacy. Instead, all information about everyone is free.

[13] http://www.gvu.gatech.edu/user_surveys/survey-1998-04/

[14] See comments on the survey by Lorrie Faith Cranor, *Internet Privacy: A Public Concern*, available at http://www.research.att.com

[15] For the swedish approach on all theories in use to define the concept, see for instance the theories listed by Professor Peter Seipel in *Juridik och IT*, 6 uppl. 1997.

[16] See *Boyd* v. *United States*, 116 US 616, 625-26 (1886).

[17] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, vol. 4 (December 1890), p. 193.

[18] See European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8.

information about oneself, to limit accessibility, the right to secrecy and to enjoy anonymity etc.[19]

Focusing on normative – rather than descriptive – aspects of privacy, Arnold Simmel emphasizes the right to exclusive control of access to private realms:

> "Privacy is a concept related to solitude, secrecy, and autonomy, but it is not synonymous with these terms; for beyond the purely descriptive aspects of privacy as isolation from the company, the curiosity, and the influence of others, privacy implies a normative element: the right to exclusive control to access to private realms."[20]

The respect of individual privacy, private life, sphere or space, or whatever one would like to call it, is – in the practical use of information technology – thus strongly connected to the question of *control* of personal data. First, we shall take a brief look at what personal data are and how they appear.

2.4 What is regarded as Personal Data in online environments?

In the European legislature tradition, *personal data* is "any information relating to an identified or identifiable natural person ('data subject')".[21]

The first question that need to be asked is therefore if data collected is identifiable (i.e. referring to a certain individual), the other is how to keep unidentifiable separated from other data that can be used to identify data subject. Data referred to a certain computer is not necessarily the same as data referred to a certain physical individual. The most common computer data collection is the use of so-called cookies. These do not generate data about a user name or even the IP-number of computer used. Instead, the technology generates a unique identifier merely used by the service as a customer number. I.e. by giving each (anonymous) customer a unique number the service provider knows what a customer did last time she visited the service and when, for how long etc.[22]

---

[19] The total listing includes the right: a) to individual autonomy; b) to be left alone; c) to a private life; d) to control information about oneself; e) to limit accessibility; f) of exclusive control of access to private realms; g) to minimize intrusiveness; h) to expect confidentiality; i) to enjoy solitude; j) to enjoy intimacy; k) to enjoy anonymity; l) to enjoy reserve; and m) to secrecy. See David H. Flaherty, *Protecting Privacy in Surveillance Societies*, (University of North Carolina Press, 1989), p. 8, table 1, (Flaherty is the data protection commissioner for British Columbia).

[20] Arnold Simmel, "Privacy", *International Encyclopedia of the Social Sciences*, vol. 12, p. 480.

[21] "An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." I.e. any kind of information once linked with an individual. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art 2.

[22] The typical ingredients of a cookie are 1) a cookie name (chosen by Web server); 2) value of the cookie (the specific data that are being stored for future recognition and action by the Web server); 3) the expiration date 4) information about the path of the Web page a user was on when the cookie was sent; 5) the domain the cookie is valid for; 6) the need for a secure connection to exist to use the cookie (if marked "secure", the cookie will only be transmitted on a secure server), see easy steps of *What to do about Cookies*, Information and Privacy Commissioner/Ontario, http://www.ipc.on.ca/Web_site.ups/Matters/Know/cookies.htm

When unidentified data is collected, the major issue is thus that this data also is kept unidentified and separated from other information which may reveal the real identity of individual.

Thus, how can information about a user (personal data or not), be collected in online environments? We have for this project created a model which shows the appearance of what may be called *electronic footprints* and *electronic tracks*:[23]

Electronic tracks is normally generated in or by:

1. The user's computer. Normally, outgoing and incoming mail is stored in specific mail boxes. Internet traffic generates cookie files, history files or global files stored on the users own computer. Communication software such as ICQ, Microsoft Netmeeting, Winfax etc also creates log files of interactions made.
2. Work station for user's computer back up.
3. Third party in the organisations' network (i.e. log files including data of user activity in network as well as in each computer).
4. Incoming and outgoing e-mail (copying in for instance an SMTP-server used for e-mail traffic).
5. Internet servers (i.e. server log on employees' Internet traffic).
6. Web sites (log files including IP-number, referring URL/Web site, data submitted by user log in to the service in question).
7. Third party in forms of eavesdropping (surveillance) of e-mail or other Internet activities.[24]

2.5 Control and use of Personal Data in online environments

As earlier indicated, the balance of interests – to determine the sphere of privacy or the infringement hereof – is not just a simple balancing act of the purposes of the data controller and the data subject right to be let alone. There are various situations where the use of personal data is a mutual interest of the user/controller and the data subject. This could be the case in public as well as the private sector. For instance, the report on Info-Society 2000 in Denmark regarding handling personal data within the public administrative authorities, states as a principle that public institutions shall not request the same information twice from a citizen if the data can be transferred electronically.[25] Personal data must hence be disseminated widely between all public administrative authorities.[26]

---

[23] For further presentation of this model, see http://www.integritet.nu. About the distinction between personal (identifiable) data and *user* (non-identifiable) *data*, see the project Web site: http://www.integritet.nu/elektroniska_spar.htm and especially the report (in Swedish) by Lundblad, Nicklas, *Elektroniska spår* part financed by Teldok, p. 10-37.

[24] Such as the product so-called *NetBus*.

[25] Ibid. Cit.: "Information which has already been submitted by citizens and companies to a public institution, and which can be transferred electronically, shall not be requested by another institution again."

[26] For further information (in Swedish) about the dissemination and commercialization of personal data by public authorities, see for instance Hammarstedt, Per, in *Myndighetsinformation i informationssamhället, En studie om myndigheters rättsliga stöd för informationsspridning med hjälp av IT*, SITI-Publikation 1999:02.

In the private sector, online profiling technologies used to track and gather information about consumers' behaviour and preferences gives the online business possibilities to offer products or services in line with those preferences. Internet observers think that we have just scratched the surface of Web personalisation's potential.[27] Reading, watching or hearing ads and articles in offline environment does not leave any information about the user behind. In the online marketplace, however, many actors have the ability to watch a user as she brows across various Web sites, record what is read or not, make certain that the same ads not are shown twice, whether or not she clicks and ad or not etc.[28]

Of course, the use of demographic information in marketing often are of interest also for the user herself, offering the services, products (or just ads) in accordance with her demands. On the other hand, the customer may not want data containing personal preferences spread out on the online marketplace with limited choices (as opt-out models) to retrieve control over personal data.[29] Or at least, partly decide if, and in that case, which data that could be used. Thus, there is a need to address consumers' concerns by agreeing to provide consumers' control over data used in e.g. the creation of online profiles.[30]

A central outcome of this perspective, is that it supports a solution for online privacy protection where the user and controller gives an opportunity to *negotiate* on a case by case basis which data and how long, for what purpose etc they may be used. Below we will study this alternative more closely and the technology that supports it.[31]

2.6 Control and use of Personal Data from a user perspective[32]

Control is a basic human need. User control is a central usability design principle within the multidisciplinary research field of Human Computer Interaction (HCI). The aim of HCI is to develop IT systems and products that are safe, effective and enjoyable to use, largely done by using the concept of usability. Usability is a complex concept and not easily defined since it is dependent on the purpose of the system, the context of use and the users themselves. However, most researchers agree upon some aspects.

ISO 9241 Part 11 Guidance on Usability defines usability as:

> "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

Within traditional HCI, (where focus often have been on the human interaction with one single computer), researchers have identified several important design

---

[27] See for instance Discussion Paper prepared for the EC Workshop in Seville on 25-26 October '99 *Personal Data Protection in the Digital Economy: the Role of Standardisation*, available at http://www.law.kuleuven.ac.be/icri/papers/doctrine/standardization.pdf

[28] For further information on the technology in use for this, see http://www.integritet.nu.

[29] A 1998 *Business Week* Poll showed that 61 percent of non-Internet users cited privacy as a key reason for nonuse, *Business Week*, March 16, 1998, p. 102.

[30] Recently (the 8th of November), the Federal Trade Commission (FTC) were asked by government to launch an immediate investigation into the growing practice of data profiling.

[31] See under section 4.4.

[32] Co-writer in this section is Thomas Soltesz (B.Sc.), a behavioral science researcher at SISU.

principles and guidelines for the development of computer systems. One of them has to do with the users need for control and several others like system transparency, flexibility, and feedback closely related to it.

2.6.1 User control

To have control is a basic human need. Within HCI this need is especially important for expert users. Events initiated by the system, trouble getting the right information, lack of opportunity to perform an action are all examples on lack of control that creates frustration and stress for the user. Users need to be the initiators of events not the recipients of them.

2.6.2 System transparency, -visibility and –observability

This usability principle means that the objects in the digital environment must indicate, correspond with their functionality and the effect of using them. System transparency is also closely related to the concept of affordance, which means that the qualities of an information object must indicate how and for what they can be used. Observability has to do with the possibility to judge the systems internal status, which is important for the user to decide on what to do next.

2.6.3 Flexibility

Flexibility refers to the multiplicity of ways the user can interact with and exchange information with the system. Some principles for this are dialog initiative, which means that the user should initiate the communication between system-user. Multithreading refers to the ability of the system to allow several tasks to be performed simultaneously.

2.6.4 Feedback

Feedback is a fundamental and important design principle. Timely feedback is necessary for the users to keep them informed and feeling in control. Preece define feedback as the sending back information to the user on what action that has been done and the results that has been accomplished.[33]

Although these principles are still highly, perhaps even more relevant, Internet (as the system development context) have put them in a different light as it have made computer use to a social activity/phenomenon. The Internet is already a complex socio-technical Web that is forming our online relations and activities.

Thus, the individual need for control has expanded and now includes also the need for control over the user herself *visavi* other people, organizations and companies since a user is exposing her computer use (herself) to others. The basic need for control is no longer a question about which part initiates processes and activities in the system. The social dimension of Internet, hence forces the principle to also includes the need to be left alone, to control information about oneself, to limit accessibility etc, for instance by use of personal data, to the wills of other individuals, organizations and companies.[34]

---

[33] See Preece, J., Sharp, H., Benyon, D., Holland, S. and Carey, T., *Human Computer Interaction*, Addison-Wesley Pub. Co., 1994.

[34] Cf *supra* note 19.

3 Public and Private Regulation

3.1 Introduction

The definitions used herein are the same as in the European framework, most and foremost the EU Data Protection Directive.[35] Thus, for further explanation see the definitions in Art 3.[36]

3.2 OECD Guidelines

It is the basic principles [of national application] of data protection laws that constitute the knowledge on the concept of privacy, as we know it by the tradition.

These principles focus on all varieties of processing of personal data and can be summarized as follows:[37]

(i) *Collection Limitation Principle*
Personal data should, when collected, be collected by fair and lawful means.

(ii) *Data Quality Principle*
The amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering.

(iii) *Purpose Specification Principle*
Personal data should be gathered for specifies and lawful purpose(s) and not processed in ways that are incompatible with those purposes.

(iv) *Use Limitation Principle*
Use of personal data for other purpose(s) than specified, should only be made with the consent of the data subject or with the legal authority.

(v) *Security Safeguards Principle*
Reasonable security measures should protect personal data from unintended access, modification or dissemination.

(vi) *Openness Principle*
Data subjects should be informed about the use of personal data about themselves.

(vii) *Individual Participation Principle*
Data subjects should be given access to data about themselves, and be able to rectify inaccurate or misleading data.

(viii) *Accountability Principle*
Data controllers should be accountable for complying with measures which give effect to the principles stated above.

The principles, albeit developed pre-Internet time, still form the core of privacy protection and are hence included in the online privacy protection rights. For instance, implementation of the *Openness Principle* in online environments

---

[35] The European Parliament and the Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data described below, available at http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

[36] Id.

[37] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, see http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM#3

requires that service providers inform users when data about them are being collected. One possible way to do that is by disclosure of practices in so-called privacy policies or statements.[38] The *Use Limitation Principle*, give users the right to prevent receipt of electronic junk mail or the creating of personal profiles. A user may also want to check the accuracy of possible consumer data collected, which is supported by the *Individual Participation Principle*. Furthermore, the *Collection Limitation Principle*, may be interpreted so that data should be erased or made anonymous as soon as the communication ends.[39] According to a recommendation by the *Working Party*,[40] information for billing purposes should not be kept by Internet Service providers for a period of time longer than necessary for billing. Periods of no longer than three months have been successfully applied in several Member States.[41]

The challenge regarding these principles is to find proper practical means for implementation whether or not based on formal law or self-regulation. Last year OECD considered these means by placing them on the agenda of the Group of Experts on Information Security and Privacy.[42]

3.3 The European data directive[43]

3.3.1 The rules governing data processing

In the end of the 1980's (i.e. long before the common use of global networks as the Internet), the Member States of the European Union started to discuss the creation of a European framework as regarding the protection of personal data and the protection of free movement of such data within the union. In October 24th 1995 a directive was released, a directive with a set of rules that give substance and specifies the principles laid down in the European Convention No 108 of 1981.[44] These establish the minimum level of protection and Member States shall therefore determine more precisely the conditions under which the processing of personal data is lawful.[45]

---

[38] See section 3.5.2 below.

[39] Cf. Article 6, *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.* Available at http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html (The general rule of erasure and anonymity of data has however exemptions for billing and interconnection payments and marketing purposes.)

[40] See further under section 3.3.10 below.

[41] Working Party, *Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes*, available at http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp25en.pdf

[42] See *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*, available at http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm

[43] See *supra* note 35.

[44] Idem. The directives' preamble p. 11 says: "Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;"

[45] Art. 5.

3.3.2 Data quality principles

A basic rule regarding processing of personal data is that the data must be collected for specified, explicit and legitimate purpose(s). Processing must also be compatible with those purposes. One major reason – why a purpose must be established – is that the data subject must know why or why not the processing is done, in order to give an informed consent or not.

Furthermore, the data should be adequate, accurate, relevant and in relation (by kind and time) to the purposes for which they are collected.

3.3.3 Legitimate processing criteria

Since there is no legal definition of what is or could be considered as a privacy infringement, the legal framework by tradition holds certain criteria of what should be seen as lawful processing in order to diminish, or if possible, eliminate the risk of violating someone's privacy.

By establishing six criteria, at least one of which must be satisfied if processing is to take place lawfully, Art 7 does not absolve the controller from the need to respect the data protection principles. The criteria, which stating that processing is lawful, are the following:

(a) The (unambiguously given) consent.
The main rule is that processing should be deemed legitimate if the data subject does not opposes the processing by giving a consent *unambiguously*. Of course, there are many situations not requiring consent of the data subject.

(b) Performance of a contract,
may include data processing, which is deemed lawful due to the interests of both (contracting) parties.

(c) Legal obligations,
allows processing where there is a legal obligation upon the controller, (should be self-explanatory).

(d) Vital interests.
Processing may be done if necessary to protect the vital interests of the data subject. *Vital interests* should be read as "an interest which is essential for the data subject's life".[46]

(e) Public interest,
or "in the exercise of official authority". The expression seems hard to define precisely. It will most certainly vary from case to case due to the individual circumstances therein.[47]

(f) Other overriding interests.
This is *the balance of interest*s test, which makes it possible to balance the interests of the controller towards the interests of the data subject. This is probably the most important provision in the whole legal framework since it establishes the comparison that has to be made between the legitimate interests of processing and the "fundamental rights and freedoms" which might be put at risk by the processing.

---

[46] Recital 31.

[47] Examples given in the proposition may be the registration of a Nobel Price Award winner or Championship participants, processing for research or statistic and similar use.

3.3.4 Special processing categories and sensitive data

Processing personal data of certain sensitive character is forbidden according to the directive.[48] However, this is not the case when the data subject gives her explicit consent to this processing or the data is manifestly made public by the data subject. There are also other exceptions from the prohibition if the purpose(s) of the processing represents an interest that takes the upper hand. Those interests may be the (data controllers) obligations according to employment law, vital interests of the data subject, legitimate activities by association or any other non-profit-seeking body solely related to the members. Other interest may be preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, or processing relating to offences, criminal convictions or security measures. The latter may only be carried out if under the control of an official authority.

Furthermore, national law or a supervisory authority may provide other exemptions or derogations from the provision regarding sensitive personal data.[49] Some attempts hereto are discussed below.

3.3.5 Information to the data subject

Another important feature in the data protection framework is the openness between the data controller and the data subject. To create, or uphold, this form of trust between involving parties of the processing, the information rules require certain information to be provided to the data subject either where the data are collected directly from the data subject or where they are collected from some other source.[50] The information should contain the identity of the controller (and any representative), and the purposes of the processing.[51]

3.3.6 The right of access

According to Art 12, the data subject has the right to – "without constraint"[52] – obtain certain information from the controller about the data which are being processed. The information should contain the purposes of the processing, the categories and source of data concerned, and the recipients or categories of recipients to whom the data are disclosed.[53]

The data subject also has the right of rectification, erasure or blocking of data when processing is against any rule in the directive. The data controller should in these cases notify a third party – which has received data – to the same unless this proves impossible or involves a disproportionate effort.

---

[48] With sensitive data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life (Art 8 p 1).

[49] Art 8 (4).

[50] Art 10 and 11.

[51] These principles are non-the less new, instead it follows the international holdings in as well European Convention No 108 and the OECD guidelines.

[52] The expression is not very clear. The German text is "frei und ungehindert", which is the sense of *without impediment*, (in Swedish "utan hinder" and Danish "uhindret").

[53] Furthermore, the data project should receive information about the knowledge of the logic involved in any automatic processing, regulated in Art 15(1).

3.3.7 The right to object

When it comes to processing for certain purposes, e.g. processing for the purpose of direct marketing, the data subject has in addition to all other protective provisions – a right to object that processing. The right to object should be free of charge and offered to the data subject before the data is disclosed to or used by a third party for direct marketing purposes.

3.3.8 The confidentiality and security of processing

For all processing of data, and in particular where the processing involves the transmission of data over a network, the controller must implement appropriate technical and organizational measures to protect personal data. The protection should prevent data from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

With "appropriate" measures, means that costs and technical solutions should be in correspondence to the nature of data processed and the risks of the processing.

These obligations embraces of course both the processor and the controller, which means that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security and organizational measures.

3.3.9 Exemptions and restrictions

There are certain interests and circumstances that can motivate exemptions from several of the principles laid down in this directive.[54] National legislation may restrict the rights according to the data quality principles, Art 6(1), the information duty, Art 10 and 11.1, the right of access, Art 12, and measures regarding registration and publicizing of processing operations, Art 21. Many interests may motivate such exemptions or restrictions, however, the directive shows that they must be of certain dignity and part of the interests of the social community. Examples are national or public security, defense, economic or financial interest and more.[55]

3.3.10 Transfer to third countries

Transfer of personal data to third countries (i.e. outside the EU and the EES) is lawful only if the receiving country provide an "adequate" level of data protection. However, the exemptions in Article 26 are extensive and the first step for the controller is usually to pay regard to if any of these are applicable to the transfer in question. Since the use of personal data via the Internet should be seen as transfer to any country, including third countries, the question of *adequacy* is of special interest, (and we shall look deeper into this question soon).

In accordance to the criteria for legitimate processing, transfer of personal data should be deemed lawful under certain circumstances (albeit the receiving country ensures an adequate level of protection or not). The typical circumstances are that

(a) the data subject has given his consent ("unambiguously"),

or if the transfer is necessary:

---

[54] Art 13.

[55] Idem.

(b) for (the conclusion or) the performance of a contract between the data controller and the data subject, or between the data controller and a third party,

(c) for important public interest grounds, or for the establishment, exercise or defense of legal claims, or

(d) in order to protect the vital interests of the data subject.

Transfer is also deemed lawful if made from a register that is providing information to the public and the interests of the data subject are regulated in this context.[56]

Finally, the data controller has a possibility to provide appropriate contractual "adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals".[57] These contractual possibilities are addressed by the so-called *Working Party*, including three criteria by which the effectiveness of a data protection system (contractual or not) should be judged.[58] The criteria reflect the ability of the system to a) deliver a good level of compliance with the (contract) rules, b) support and help to individual data subjects, and c) provide appropriate redress to individual that suffers from privacy infringement.[59]

The *adequacy* of a third country protection should be assessed by "all the circumstances surrounding a data transfer operation or set of data transfer operations".[60] This means that privacy protection in third countries not necessarily has to be established through formal laws. Other (non-legislative) measures may constitute the adequacy of the level of protection afforded. Since the US approach is to use self-regulatory means, it is essential that self-regulation is considered to fulfill the requirement of adequacy. Otherwise, transfer of data between Europe and US that do not fit within the above mentioned exemptions becomes illegal.[61] The negotiations about so-called *Safe Harbor principles* are the attempt to solve this conflict between Europe strictly regulatory framework and the US self-regulatory regime. US organizations declaring that they comply with the principles herein are to be regarded as *Safe Harbors*. I.e. transfer to these organizations is also in accordance with the European framework.

---

[56] A register "which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case."

[57] Art 26(2)

[58] See Article 29 for the establishment, concept and composition etc. of the *Working Party*, or for leverables at http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/

[59] See for instance: Working Party, *Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries*, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp9en.htm

[60] S*upra* note 57. Particular consideration shall be given to e.g. the nature of the data, purpose, country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

[61] For further information on the US approach to the directive, see for instance Swire, P., Peter, Litan, E., Robert, *None of your business, World Data Flows, Electronic Commerce, and the European Privacy Directive*, 1998, p. 31.

The questions of providing explicit (opt in) choice with respect to sensitive data, journalistic exceptions, the role of Data Protection authorities and notification procedures etc are listed in Frequently Asked Questions (FAQ's) issued by the US Department of Commerce.[62] Recently (December 1999), the working party stated that the proposed Safe Harbor arrangements remain unsatisfactory. They find that the principles lack reliable arrangements allowing *Safe Harbor* participants to be identified with certainty, that enforcement by an appropriately empowered body must be made clear etc.[63]

3.3.11 Codes of conduct

"Codes of Conduct" usually refer to industry association or sectorwide provisions. These are to be distinguished from "principles" or "policies" usually referred to individual company arrangements.[64]

According to the directive Art 27, codes of conduct shall be encouraged. Member States shall also make provisions for trade associations and other bodies that have drawn or intends to draw up draft national codes.

The *Working Party*, which were established through the directive, is among other things giving opinions on codes of conduct drawn up at Community level.

This fall, codes of conduct were established for the marketing sector by SWEDMA (Swedish Direct Marketing Association).[65] The codes consists of two fundamental rulings regarding the collection of personal data, stating that data should only be collected from the user directly, or from a register hosted by third party if the user is aware of that register (and not has *opt-out*).[66] Hence, these provisions do not seem to prohibit the collection of personal data through users behavior of Web browsing or similar cases. It should be mentioned that the codes of conduct have been supervised by the supervisory authority, the Data Inspection Board.

3.4 National implementations

3.4.1 Status of the Directive implementations

Sweden is one of the few countries that has managed to implement the directive within the time stipulated in the directive, i.e. 3 years from the directive release (28 of October 1995).[67]

The implementation made through the Swedish Personal Data Protection Act of 1998 is, in whole, more of a translation of principles and provisions into the Swedish legislation language and context, rather than restricting or in any other

---

[62] List of the FAQs relating to the US Safe Harbor Principles, http://www.ita.doc.gov/ecom/menu.htm

[63] Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp27en.htm

[64] See section 3.5.2 below.

[65] The codes are available at http://www.swedma.se/dokument/allmanna/info.pdf

[66] Id., Article 4.

[67] At the moment there are only 7 of 15 Member States that have implemented the directive as a whole (Austria, Belgium, Finland, Greece, Italy, Portugal and Sweden). Other states are close in the proceedings of adoption, (Denmark, Ireland, Germany, Luxembourg, Spain and The Netherlands). See http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm

way by legislative measures elucidate the rights provided for in Art 9, 12 and 14. There is therefore of minor interest to list all the provisions of the Act here. Instead, a few notes should be made on possible openings in the directive and correlative holdings in the Personal Data Act.

For instance, Article 9 in the Directive holds that "Member States shall provide for exemptions or derogations"..."for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[68] The Personal Data Protection Act regulates in the same wording that some provisions (9-29, 33-44 and 45.1 and 47-49 §§) are not applicable *for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression.*[69]

However, the Swedish delegation made clear during the discussions that the "purposes" mentioned rather more takes into consideration the means of expression than the content or quality of the communication.[70]

3.4.2 "Adjustments" in Swedish law

Recent adjustments in the Swedish Personal Data Act, focus on an attempt to establish a concept for what is regarded as *harmless* personal data. A critique on this change is that it does not change the practical balancing between dissemination data and protecting data appreciably. The main reasons hereto are that personal data *per se* not is sufficient when judging the lawfulness of processing data. Other circumstances, as the purpose and the controller processing are playing a major role in the act of balancing of interests.[71]

The other adjustment proposed is an overall easing-off the liability for violations of the Personal Data Act.[72] In short, sanctions will not come into force for *insignificant* non-compliance with provisions regarding:

a) the duty to inform data subject of processing data, (directive Art 10 and 11),
b) the demands on processing of sensible data, (Art 8),
c) the transfer of data to third countries, or (Art 25 and 26),
d) the duty to report processing to supervisory authority, (Art 18 and 19).

Finally, an interesting interpretation and elucidation on the *requirement of informed consent*[73] for online disclosure was given last year in case law. According to the County Administrative Court in Stockholm, a telephone company has the right to make the telephone directory's White Pages (i.e. that part of the directory

---

[68] Idem.

[69] See 7 § idem. It is also stated in the proposition that the provision should have the identical meaning as the (above cited) directive Art.

[70] Öman, S., Lindblom, H-O., *Personuppgiftslagen – en kommentar*, p 49.

[71] Introducing a concept of *harmless data* or *harmless information* may be at the first sight regarded as a step in the right direction. However, it only seems to bring in another thing to get confused about. Personal data such as a name, address or even a picture, are probably mostly seen as harmless data. However, used in wrong situation, e.g. at a Web site for Nazism, Terrorism or Pornography may though question if the same data still are seen as *harmless*.

[72] See the proposition 1999/2000:11 p. 23.

[73] See section 3.3.3 and 3.3.10 above.

that lists private persons) available on the Internet.[74] The court rules that a requirement of informed consent not is motivated due to the (limited) risks of privacy infringements.[75]

3.5 Self-regulation

3.5.1 What is self-regulation?

Self-regulatory measures are often defined in a negative way, distinguished from measures of public authorities, i.e. legislation and attached regulations.

Organizations and industry sectors have an incentive to exercise restraint on their own behavior and on that of their competitors. There are major constraints on the capacity of industry associations to impose standards on their members. However, arguments against self-regulation based on the aphorism "Wolves self-regulate for the good of themselves and the pack, not the deer", are used to describe the proclaimed limited use of self-regulatory measures as a complement to legislation.[76]

Thus, self-regulation must do more than just articulate broad policies or guidelines to be meaningful. Effectiveness involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.[77]

Principles of fair information practices include consumer awareness, choice, appropriate levels of security, and consumer access to their personally identifiable data.

Recent OECD work in this area has focused on the various approaches adopted by Member countries to implement and enforce good privacy practices in the context of global network technologies. The OECD's Committee for Information, Computer and Communications Policy reaffirmed the relevance of the Privacy Guidelines to global networks and the need for co-operation between governments, industry, individual users and data protection authorities in the development of policies and technological solutions to protect online privacy.[78]

A Draft Declaration by the OECD Group of Experts on Information Security and Privacy includes a factual inventory of privacy instruments and mechanisms for implementing and enforcing the OECD Privacy Guidelines on Global Networks.[79]

---

[74] Case number Ö 5456-98, between Telia InfoMedia Respons AB and the Data Inspection Board (the Swedish Privacy Commissioner) in the County Administrative Court in Stockholm, verdict January 14, 1999.

[75] Op. Cit. See for comments in Hammarstedt, Per, *Deviation from the requirement of Consent for Distributing Personal Information on the Internet*, available at Project Web site: http://www.integritet.nu/white_pages_verdict.htm

[76] See Roger Clarke, (1998c) Submission, Senate Legal and Constitutional References Committee, Inquiry Into Privacy and the Private Sector, available at http://online.anu.edu.au/people/Roger.Clarke/DV/SLCCPte.html#Need

[77] See for instance Staff Discussion Paper, *A Framework for Global Electronic Commerce*, available at http://www.doc.gov/ecommerce/staff.htm

[78] See *Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet* (October 1997), available at http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm

[79] Draft for Ministerial Declaration on the Protection of Privacy on Global Networks, available at http://www.oecd.org/dsti/sti/it/ec/prod/reg_11e.pdf

3.5.2 Privacy Policies

The development in the US towards a privacy self-regulatory regime has beside industry codes of practice mainly focused on the formation and use of so-called *privacy policies* or *privacy statements*. These policies disclose the rules according to which a service provider collects and use personal data about an Internet user.[80] The Federal Trade Commission (FTC)[81] recently testified to the House Telecom Subcommittee that "legislation to address online privacy is not appropriate at this time".[82] The use of privacy policies has increased significantly. As an example, sixty-six percent of the sites visited in the Georgetown Internet Privacy Policy Survey ("GIPPS") post at least one disclosure about their information practices.[83] Only 13.6% however, mentioned all the minimum five elements that concern information privacy: notice, choice, access, security and contact information.[84]

Several privacy policy generators are today available helping online actors to create adequate statements. The OECD Privacy Policy Statement Generator is an 'html' experimental tool based on the OECD Privacy Guidelines.[85]

It should hence be mentioned that the mere providing of a privacy policy is not demanded by any law. It is also most certainly so that the obligation to inform a data subject about processing data not is met by such disclosure.[86] However, informing visitors of a Web site of an organization's privacy policy is (as shown in several US surveys) a positive step towards helping the customer to make informed choices regarding the use of referring personal data and hereby gaining increased trust in the online marketplace.

In order for this to be true, the policy must naturally be accurate for the practice in question. Forming accurate and legally adequate privacy policies that in the same time are easily obtained and understood (human-readable), obviously includes certain impediments.[87] This is a most intriguing question that unfortunately has not been discussed any further in the online privacy literature.

Neglecting the behavioral science approach here mentioned, there are also essential legal questions to be addressed besides the issue of duty to inform. For instance:

- Conceptual meaning: Could a policy be seen as a "warrant" for the service, are they just an instrument to earn goodwill, or do they stipulates as provisions in

---

[80] For examples of privacy policies, see the Project Web site at http://www.integritet.nu/policies.htm or just make a simple search on "Privacy Policy" with Altavista or Yahoo search engines.

[81] FTC's, mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices.

[82] See *House Telecom Subcommittee Holds Hearing on Online Privacy*, available at http://www.techlawjournal.com/privacy/19990713b.htm, and the FTC report to Congress, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS, available at http://www.ftc.gov/os/1999/9907/privacy99.pdf

[83] Georgetown Internet Privacy Policy Survey ("GIPPS") report, available at http://www.msb.edu/faculty/culnanm/gippshome.html

[84] Id.

[85] http://www.oecd.org/scripts/PW/PWHome.ASP

[86] About the duty to inform, see section 3.3.5 above.

[87] Cf. section 4.4.4 below

the agreement concluded by the consumer automatically accepting them in moment of visiting a Web site?

- Meeting privacy legislative demands: May the acceptance of a privacy policy in forms of user interaction be regarded as meeting the prerequisite of "unambiguosly consent" for data processing?[88]
- Enforcement caveats: Furthermore, when non-compliance to a policy is the case, in what way can the consumer proclaim any rights of infringements or even breach of contract?

3.5.3 Marking on the Internet

Since a couple of years ago, the online industry in US developed a concept using marking as a mean to assure customers that service providers have tested their privacy practices and disclosed them on their Web site in a privacy policy. The mark or seal-logo used on a Web site gives the customers indications that the privacy policy is in line with legal and social demands, and that the service provider complies with them.

TRUSTe is today a well-known organization for licensing their seal-logo for use on online companies' Web sites if they comply with the standards for privacy protection contained in the TRUSTe seal program.[89]

BBBonline is an organization using a similar business model as TRUSTe, offering three closely related types of seal programs in order to promote trust and confidence on the Internet. Awarding companies that meet the standards of Reliability Seal, Privacy Seal and Kid's Privacy Seal, helps the customer to identify responsible online businesses.[90]

Recently BBBonline also started the formulation of the *Code of Online Business Practices*. The code is intended to contain practical e-commerce guidelines designed to allow online businesses to "take advantage of technology and to foster innovation while adhering to fair business practices that provide truthful and accurate information to online consumers." The performance-based principles focus on accurate *disclosure*, truthfulness, *information practices*, "aim to please [the customer]" and the protection of children. [91, 92]

3.5.4 The value of marking

Recently, organizations as TRUSTe has had their credibility damaged, since several of the licensees have not been punished for breaking their privacy policies. This has furthermore underlined the question whether privacy policies or other non-traditional measures may substitute/complement legislation for online privacy.

There are three different types of actions that can come into reality when breaking privacy policies within a seal-program:

---

[88] See section 3.3.3 above

[89] See http://www.truste.org/

[90] See http://www.bbbonline.org/

[91] The code may be downloaded at http://www.bbbonline.org/download/draft.doc

[92] SISU is also working on a concept similar to bbbonline (called QMI, Quality Marking on the Internet), focusing on legal, usability and technical aspects.

1 Revocation of the logo (and the licensor suffers bad publicity).

2 File for breach of contract (between the *licensee* and *licensor*).

3 Case forwarding to responsible authority (i.e. FTC in this case).

As of yet, there is no case when an organization as TRUSTe has revoked a logo. The risk of potential public relations backlash may not stop companies and other organizations from violating privacy. Most certainly, the reason hereto is that the calculated risk for liability and possible tort claims widely falls short of the profit in collecting personal data for business purposes.

The remedies in question are also regulatory means only on an organizational level, i.e. the matter of a tort claim against a data collector due to a privacy infringement will come real only after a reaction of the responsible authority (p.3).

In other words, even if different self-regulatory actions may be applicable and relevant in different online environments, there will still be a need for a legal framework that gives the individual a platform to file charges against any actor collecting/using personal data in a non-acceptable way.

Self-regulatory measures as marking seem therefore, due to lack of remedies, not be an alternative as "oppose law and regulations".[93] Instead, these means could be a good complement in upholding fair information practices.

3.6 "Co-regulation"

Online privacy protection may be handled in several different ways. By (traditional) *legislation* and other regulation, by *self-regulatory measures* just mentioned, by *contracts*, and by *technology* (see section below).[94] All these approaches have enforcement and redress as mutual fundamental issues. Measures needed in order to meet these demands may be summarized as follows:[95]

(i) Establishing general privacy protection principles.

(ii) Legal application of the principles to all organizations.

(iii) Creating effective sanctions against non-compliance.

(iv) Development of operational codes of practice consistent with the principles.

(v) Establishing dispute-resolution procedures at the levels of individual organizations and within industry associations.

(vi) Making principles, codes and sanctions enforceable through quasi-judicial (tribunal) and court procedures.

(vii) Supervising the process and framework and investigate complaints by watchdog agencies, such as privacy commissioners.

---

[93] The spokesman of TRUSTe, Mr. David Steer, also holds that "[O]ur program is only a part of a solution", see http://www.zdnet.com/zdnn/stories/news/0,4586,2387000,00.html?chkpt=zdhpnews01

[94] See for instance OECD, *Draft Background Report For The Ministerial Declaration On The Protection of Privacy on Global Networks*, available at http://www.oecd.org/dsti/sti/it/ec/prod/reg_11e.pdf

[95] See for instance Clarke, Id. http://online.anu.edu.au/people/Roger.Clarke/DV/Florham.html#Reg

In addition, certification mechanisms can provide assurance for compliance of privacy principles. Market forces such as the threat of bad publicity may encourage online businesses to comply with privacy principles and provide redress voluntarily.[96]

The Swedish approach in short, is that legislation is the primary tool to protect consumers' rights in the online marketplace. Legislation forms the regulative frame and is hence supportive for the construction of codes of conduct and other self-regulatory measures, preferably outlined with the guidance of consumer organizations.[97]

[96] See section 3.5.3 and 3.5.4 above.

[97] This is one of the key issues stated in the hearing with the IT-commissions legal observatory, documented in the Observatory report 2/97 (*Konsumenträttigheter i informationssamhället*).

4 Privacy-Enhancing Technologies

4.1 Introduction

The characteristics of technology are paradoxical in threatening and enhancing online privacy at the same time. The first question that needs to be asked is: when is it truly necessary for information systems that individuals' real identities are revealed? There are many situations where the service provider needs the exact identification in order to perform his obligations towards the data subject, e.g. for billing procedure. On the other hand, in several cases the individual's identity can be replaced by a pseudo-identity. Then main challenge of PET is located in the situations where identifying data can be minimized, restoring privacy considerably but still permitting the collection of needed information.

Distinguishing Privacy-Enhancing Technologies (PETs) from other technologies is not all that simple, but still necessary. For instance, PET should not be mixed up with security-enhancing technologies. These two categories work in similar but still not the same perspective on information protection, and privacy and confidentiality should be separated.[98] Confidentiality is just one component of privacy in keeping information secure and inaccessible to unauthorized parties, i.e. strong encryption is extremely useful for security but may be less useful for protecting privacy.[99] The area covered by privacy protection is much broader than this, extending from limitations on the initial collection of personal data, to restrictions to the specified purpose and prohibitions on secondary uses (outside this purpose and without the informed consent of the data subject).

PET could also be distinguished from technologies that are sympathetic to the interest of users' privacy, privacy-sympathetic technology (PSTs).[100]

In order to getting closer a definition of PETs, the first classification of information technologies may be made by diverging them into three categories:

(i) Privacy-Intrusive Technologies (PITs),

(ii) Privacy-Sympathetic Technologies (PSTs), and

(iii) Privacy-Enhancing Technologies (PETs).

A few short comments and examples should be made on (i) and (ii) groups.

4.1.1 Privacy-Intrusive Technologies (PITs)

Many technologies may be more or less used in a privacy-intrusive way, but technologies that deny anonymity and include data-trial intensification, data-mining (warehousing) etc have been expressly defined as Privacy-Intrusive Technologies, (PITs).[101] On the other hand, there are technologies designed to

---

[98] This also follows from the prerequisites in the Data Directive, Art. 17, which states that the controller must implement appropriate technical and organizational measures to protect personal data.

[99] For further discussion on the distinction between Privacy and Security, see Peter P. Swire, *The Uses and Limits of Financial Cryptography; A Law Professor's Perspective,* http://www.osu.edu/units/law/swire.htm

[100] Roger Clarke, The Legal Context of Privacy-Enhancing Technologies and Privacy-Sympathetic Technologies http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html

[101] Id.

directly track down personal data about a certain individual, being a helping device of no risk for privacy when used properly. Example hereof is the Net Detective.[102] However, the risks for privacy infringement due to the possibilities to create personal profiles are increasing significantly, and must be observed.

4.1.2 Privacy-Sympathetic Technologies (PSTs)

The concept of Privacy-Sympathetic Technologies has been suggested by Clarke[103], to define the technologies delivering genuine anonymity that improves the balance of interest to be made between privacy interests and the use of personal data. The distinction between PETs and PSTs are thus not clear, since the function of the two represents the same interests. The PSTs however, is perhaps more strongly connected to pseudonymous technologies by working more in the open and even in an identifiable context (e.g. cryptographic tools).

4.2 Definitions and Characteristics

Privacy-Enhancing Technologies, are in a broad perspective a scope of different technologies which all have one thing in common, namely to function in a user friendly way by supporting the protection of online privacy.[104]

Herbert Burkert finds that:[105]

> "PETs are technical devices organizationally embedded in order to protect personal identity by minimizing or eliminating the collection of data that would identify an individual…"

The balance of interest made between privacy and other interests is thus approved by technologies capable of delivering genuine anonymity. Together, PET and PST may be placed in a framework in which the characteristic of the technologies are classified by ways of minimizing identifiable data in information systems. Minimizing data is possible by using *anonymity services*, *pseudonymity services* and through enforced principles of Personal Data Protection.[106]

As we shall see, several of the services providers offering PETs today have a business model built upon the submission of personal data from Internet users. To have *control* of customers' personal information creates the position of an infomediary, with the object and power to negotiate and sell personal information to other Internet service providers. Thus, when user data is representing an economic value, the question arises whether the infomediary (or information

---

[102] Net Detective locates e-mails, phone numbers, addresses, purchase orders and any other information available via the Internet, http://find-person.com/nd/ (or http://www.collector-club.com)

[103] Idem. p. 6.

[104] For a quick summary of tools and products, see EPIC, Electronic Privacy Information Center, list: Online Guide to Practical Privacy Tools, http://www.epic.org/privacy/tools.html. PETs have been discussed at several international occasions, see for instance CFP99, Conference on Computers, Freedom + Privacy, http://www.cfp99.org and abstracts at the project Web site http://www.integritet.nu, or the Telematics Engineering Workshop on Data Privacy (Concord), *http://194.7.241.108/meetings/tewsoct99/agenda/agenda.htm*

[105] see Burkert, *Privacy Enhancing Technologies and Trust in the Information Society*, http://www.gmd.de/People/Herbert.Burkert/Stresa.html (Burkert is the president of the Legal Advisory Board, http://www2.echo.lu/legal/en/lab/lablab.html

[106] See for instance Clarke, R., op. cit.

broker) should be a third party or the customer/user herself.[107] To what extent do individuals have an interest of themselves controlling the use of data?

In the following, we shall make an inventory of the most common and the newest products and services deemed to be privacy enhancing.

4.3 Anonymizing technologies[108]

4.3.1 Remailers

Anonymizing technologies may focus either on anonymizing the object or on anonymizing the subject. A typical anonymity service is the Anonymous Remailers, such as the "Mixmaster". A remailer privatizes e-mails so that the true name or true e-mail address of the sender not can be revealed. As Bacard[109] explains it, the remailer is "in sharp contrast to the average Internet Service Providers [ISP]"... which, in fact, "could equally stand for *Internet Surveillance Point*."[110]

When e-mail is sent via a remailer, sender name and address are replaced with a pseudo-identity. For instance, e-mail from perh@sisu.se would be replaced by "abc@remailer name.se".

However, anonymous remailers could be distinguished from *pseudonymous* remailers. The example just shown is one of the pseudonymous ones, since the operator must keep a log to know the real name and address in order to send and receive the e-mail in question. *Anonymous* remailers, as the "Mixmaster" or "Cypherpunk remailers" are not actually anonymous until they (two or more remailers) are used at the same time excluding the possibilities for the operator to know the senders' real name and address.

4.3.2 Anonymizer and similar products

Anonymizer[111] is one of the oldest services offering anonymous access to the Internet. By connecting to Anonymizers' proxyserver, the user gets access to the Internet but does not reveal his or hers real identity, since the user to a third party seems to be the anonymizer-server itself. Anonymizer also offers anonymous e-mail and Internet browsing.

---

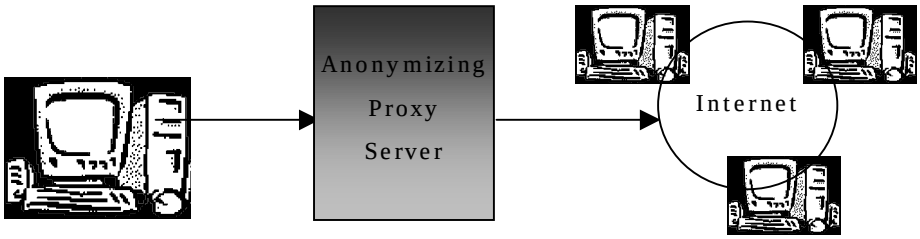
[107] It is a parallel question to the commercialization of personal information also within the public sector. Who should gain profit of personal/customer/citizens data? This political question is also addressed in Hammarstedt, *supra* note 26.

[108] A description in Swedish over many of these technologies are also available at the Project Web site at http://www.integritet.nu/att_kapitalisera_integritet.pdf

[109] see Bacard, Andre, in *Computer Privacy Handbook*, http://www.andrebacard.com/index.html or draft at http://www.andrebacard.com/remail.html

[110] For further information about remailers and Mixmaster, see http://www.andrebacard.com/remail.html

[111] See http://www.anonymizer.com



Other examples of anonymity services is the LPWA, a multi protocol service based on a proxyserver which remains the true identity unknown to Web sites. The LPWA product *proxymate* gives the user possibilities to use aliases (as "spam-filtering") when submitting information for a special service.[112]

- *Freedom*

Freedom is a product that allows anonymous profiles and provides up to five different online aliases. Since Zero Knowledge Systems (the developer), is a Canadian company, the technology is based on stronger encryption than similar American products. There is thus not possible to trace e.g. browsing, e-mail or chat activities.

- *Crowds*

The Bell Labs and AT&T Labs have developed Crowds system, which uses a virtual "crowd" of people to hide the users identity while browsing the Internet. Users are placed in random groups and each time the user gives instruction to a browser the command is randomly routed. Hereby it is impossible to track a group member individually.[113]

- *Onion routing*

The Onion routing system, under development by the Naval Research Laboratory, keeps third parties from tracking surfing activities by randomly routing messages through a series of routers before the message reaches its destination.

4.4 Negotiating supportive technologies

4.4.1 Functioning

Having an exclusive right to users personal data creates economical possibilities in administrating and selling data to companies and others in need of customer preferences. The market for privacy protection products is growing heavily and companies are responding with a variety of technological tools and services.[114] There are today several types of technologies that can be used as support for a

---

[112] See http://www.lpwa.com/ There are several similar projects that use the same technology and business model and therefore not are described any further, e.g. Idzap.com, http://www.idzap.com/, or Private Power Project (PPP), a new Swedish service built on a technology called winSqueeze, see http://www.ppp.nu and http://www.winsqueeze.com/

[113] See at http://www.research.att.com/projects/crowds. AT&T also have a service called *Chat 'N Talk*, which is an innovative application that provides Internet chat room users with a way to connect by phone without revealing their phone number or identity, hereby maintaining a level of anonymity and privacy, see at http://zing.ncsl.nist.gov/hfweb/proceedings/fairbrother/index.html

[114] The Californian start up company *Lumeria* describes the new marketplace as *Identity and Knowledge Publishing* and *Identity and Knowledge Commerce*, see under 4.4.3.

negotiation on how an Internet users' personal data may be processed and used by a service provider. In some cases the infomediary is a third party, and in some cases the individual herself.

4.4.2 PrivaSeek and Persona

Different kinds of relatively untested so-called infomediaries are more and more gaining ground on the US information market. PrivaSeek is a company that offers a product (Persona) which let the user set her preferences on how her personal data may be sold. These infomediaries thus requires that the user creates a detailed personal profile to enable the technology to negotiate the release of personal data on her behalf. PrivaSeek gets a commission when the user according to the profile is willing to sell her personal data in exchange for a discount at a certain site.

4.4.3 Other infomediaries

Since this paper presents technologies in a tentative manner, and thus not aims to be a complete account, we shall also mention some similar newly developed technologies.

Enonymous advisor, a free Web browser gives the user a 4 star rating system evaluating over 15,000 sites' privacy policies. The *advisor* also fills online forms automatically and allows the user to get information about how different sites store and use personal data.[115]

A similar product *DigitalMe*, developed by Novell, also stores the users personal data for automatic form filling and keeps track of passwords and user names.[116]

The California based company Lumeria, is developing products that provide users with a system for *Personal Asset Management*.[117] One type of product helps the users to securely organize their information and knowledge in a way that these may be selectively shared and published. A similar product allows users to selectively and anonymously share and publish their individually created identities/profiles.[118] This latter system disintermediates traditional sales and management as well as Web based marketing and e-commerce.

The profiling system Lumeria uses is based on the principles of the so-called P3P. From a privacy (or a right to control information) perspective, this technique is of certain interest since it transfers the role of the infomediary function, from the product or service provider to the individual/user herself.

---

[115] http://www.enonymous.com/

[116] http://www.digitalme.com, see also the jotter at http://www.jotter.com.

[117] See http://www.lumeria.com/What1.html

[118] Lumeria also allows the user to browse the Internet anonymously by providing inaccurate information to the "cookie" files set by Web sites. For more information about the cockie-technology, see http://www.cookiecentral.com/, and legal context, see Viktor-Mayer-Schönberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, available at http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm

See also the W3C proposal for labeling cookies with privacy disclosures at http://www.w3.org/PICS/extensions/cookieinfo-1_0.html

For similar technology see e.g. Cookie Crusher at http://www.supershareware.com/Apps/2620.asp or Webroot at http://www.webroot.com/

4.4.4 Platform for Privacy Preferences, P3P

As we have seen, many of the products and services presented above can offer a good privacy protection for users in an online market. However, to be able to use certain services, the service provider often is in need of more information than may be collected due to the use of anonymity or "cookie-busting" functions etc. Hence, there is a need for an extended function of negotiation between the user and the service provider. Therefore, technologies like the P3P come easy at hand.

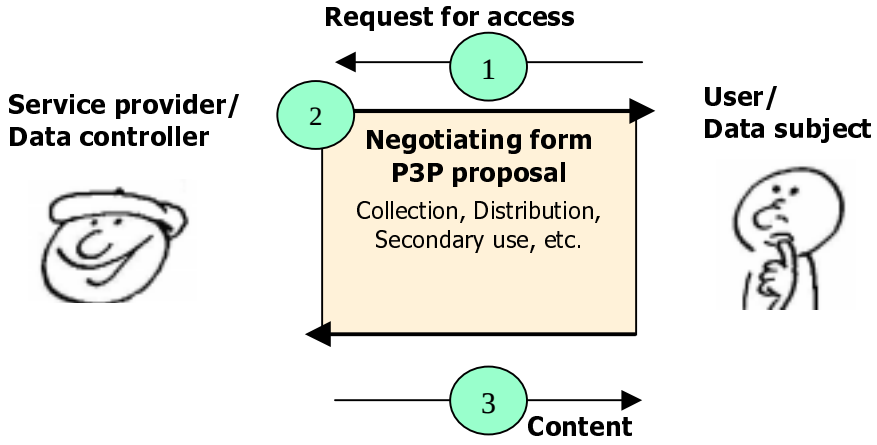
P3P has been developed by a conglomerate of different organizations, called the W3C (the World Wide Web consortium).[119] P3P stands for *Platform for Privacy Preferences* and aims to be a standard making it possible for the Internet user herself to decide any (secondary) use of personal data by a Web site she visits.

The purpose of the P3P specification is to enable Web sites to specify their personal data use and disclosure practices; Web users to specify their expectations concerning personal data disclosure practices; and software agents to undertake negotiation, on behalf of the parties, in order to reach an agreement concerning the exchange of data between them.[120]

By creating a personal profile, the Internet user may set the options for which, when and how personal data may be processed and used by the Web site. When the browser requests a connection, the Web site server declares which data is to be needed for that particular connection.[121] If the desired data (or use of data) is not coherent with the options set, the user gets the possibility (through agent technology) to decide whether to submit these data or not.

Thus, the negotiation application allows users to be informed about privacy practices, delegate decisions to their computer agent, and tailor relationships with specific Web sites.

A simple model will show how the system works:



The P3P proposal is encoded in Extensible Markup Language (XML)[122] and is a declaration of server identity and the organizations privacy practices. The P3P

---

[119] See http://www.w3.org/p3p

[120] See Roger Clarke, *Platform for Privacy Preferences: An Overview*, available at http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html

[121] See Appendix B: Sample P3P Proposal, *supra* note 119.

[122] For more information on XML and RDF used, see W3C overview at http://www.w3.org/XML/ and rearding RDF, Resource Description Framework, at http://www.w3.org/RDF/

policies identify the legal entity making the representation of privacy practices in a policy, enumerate the types of data or data elements collected and explain how the data will be used.[123] The data recipients, possible identifiable use of data or data retention, address of human readable privacy policy etc. are also identified by the policies.[124] However, the P3P policy does not address if there are any law enforcement demands for the information in use (i.e. requirement of reporting or redistributing data to public or private authorities).

The user agent – built into Web browsers, browser plug-in, proxyservers etc – compares the P3P proposal to the users' privacy settings generating the agreement on privacy practices.[125] As aforementioned, the agent may present alternatives in the case the user has no settings appropriate to the proposal given, or if the requested data is not consistent with the site policy. This negotiation is necessary only the first time (i.e. provided that none of the agreement provisions have been changed), and the follow-up visit to the same service therefore only includes a presentation of this agreement together with the request for access and content.

The Statements are (part of the agreement) describing the data practices applied and group together data that consist of five different elements:

- The *Identifiable* element specifies if (or if not) data is used in a personally identifiable way *per se* or in connection with data from other sources.
- The *Consequence* element describing and providing further explanation about why suggested practice may be valuable, especially if not direct evidential.
- The *Purpose* element contains one or more purposes for the data collection.[126]
- The *Recipient* element contains one or more recipients of the collected data.[127]
- The *Data* element describes the types of data collected.[128]

A most interesting P3P user agent implementations made is the *Privacy Minder* developed by AT&T Labs Technology.[129] The implementation is designed for demonstration and tests, but since the development (as to this date) of other P3P

---

[123] See Specification (P3P 1.0) Draft 2 November 1999 (latest version expected to last until next call in April 30, 2000), available at http://www.w3org/TR/P3P

[124] See Id.

[125] The user agents look for P3P headers and link tags (embedded in HTML content) that indicate the location of a relevant P3P privacy policy.

Agent technology finds its roots in the study of Artificial Intelligence (AI), human computer user interface design, and software engineering. Currently available agents (which are typically 'smart' Internet search engines developed to support commercial Web sites) are beginning to display the characteristics envisioned by the visionaries, see Intelligent Software Agents, ISA, Turning a Privacy Threat into a Privacy Protector or the overview of agent technology at http://www.w3c.org

[126] A Web site must classify purposes according to P3P model: *Current* (activity), *Administration*, *Custom* (for individualization of Web site), *Research* (and development), *Contact* (for e.g. marketing) or *Other* (Human readable explanation should be provided).

[127] Recipients must be classified as *Ourselves* (Web site agents) or *Same* (Web sites with similar practices) or *Other* (organization sharing information for other purposes) or *Publish* (by unrelated parties or public fora).

[128] Data should be classified as *name* (the name of a data element/set), *dataschema* (the default is the P3P data schema), *optional* (indicating reguirements of visitors submitting data) or *category* (e.g. Physical or Online contact information, Unique identifiers, Computer information, navigation and click-stream etc.)

[129] The demonstration are available at http://www.research.att.com/projects/p3p/

tools and P3P supportive Web sites is limited, no interoperability tests of any dignity has been performed.[130] Describing the application in short terms, the Privacy Minder provides a tool bar on the user's computer desktop letting the user *View proposal* of the XML encoding, select *Repository* to view and modify the personal data settings, or *View/Edit agreements* made with Web sites under the current privacy setting.

Future features to be developed by AT&T is a privacy settings editor, encryption of the user data repository, adding support for data set extensions and checking privacy proposals against a P3P DTD.[131]

Another P3P implementation has also been made by NEC in "P3P for the Pearl" (P3P4P).[132]

For the P3P concept to be efficacious, it should be used in conjunction with complementary technical and social mechanisms. There are several areas and situations in which other technologies may be a better alternative (see for instance the above introduced technologies). Since P3P focuses on privacy practice disclosure with respect to data collected through Web interactions, there are naturally still needs of technology to secure data in transactions. The P3P does not inhibit the use of these technologies.

4.5 Encryption introduction

Encryption is a wide spread technology protecting from unauthorized collection of data in communication. Since this area is highly developed with a rich amount of literature and products, this section will only briefly comment some of the well-known technologies in connection to PETs.[133] These are also what one would like to define as Security-Enhancing Technologies.[134]

4.5.1 Pretty Good Privacy

Pretty Good Privacy (PGP) is nowadays a well known encryption technique, which is often used in digital correspondence, e-mail. By using PGP, one may create digital signatures and to encrypt a messages content, so that there is no doubt about whom sent the message and that the message has not been changed on its way to the receiver.[135]

4.5.2 Secure servers and browsers

Secure Socket Layer (SSL) creates a secure connection for transmitting documents and information over the Internet, e.g. credit card numbers. SSL may

---

[130] Necessary specifications for the implementation of interoperability P3P applications are found in Specification (P3P 1.0). Idem, s*upra* note 123.

[131] Document Type Definition (DTD). For further information about DTD and other future features, see http://www.research.att.com/projects/p3p/pm/readme.html

[132] See at http://www.nmda.or.jp/enc/privacy/p3p-press-en.html (Privacy Information Management System), or http://www.w3.org/P3P/contributed/nec.co.jp/

[133] For further information about encryption, see for instance European Cryptography Resources at http://www.apparatus.org/~avs/eu-crypto.html

[134] See section 4.1 above

[135] PGP is available for free use at http://www.pgpi.org/

become the accepted standard for Web based transactions that require a high degree of security.[136]

A similar safeguard for credit card numbers is the Secure Electronic Transfer Transaction (SET) which works by using encryption to protect information exchanging over the Web. It also uses digital signatures to ensure the identity of both the user and the service provider.[137]

4.6 Strengths and limits of PETs

Strengthening privacy arguments on the level of systems design is emphasized in Burkert's introduction to PETs:[138]

> The essential change PETs bring about is a change in the burden of argumentation: While system designers – whether designing systems from a technical, political or economic level, would point to the need of identification within information systems, it can now be argued – on the that same level – that secure identification and secure personal identification are not the same and that additional arguments are needed to put forward reasons for personal identification within given systems; these arguments would then reveal themselves as economic, social and political rather than technical arguments. PETs would thus serve as strengthening privacy arguments on the level of systems design. PETSs would force the need to argue why personal information is needed in a system at all, and if so, why its use is not minimized or filtered through identity protectors.

Privacy threats are strongly connected to the question of personal identification in system design. However, the identification does not necessarily have to be made through personal identifiers in a given system. Other data, object identification, action or systems identification may connect certain data to a certain individual and hence make these be referred to as *personal* data.[139] PETs are not designed to protect against this kind of identification, the combination of *per se* non-identifiable data.

In addition, PETs are of course closely linked to a particular technological development. The aforementioned paradox of technology effects on privacy is worth to be mentioned once more.[140] Any merely technical solution will stand and fall with the technology involved.[141]

Characteristic for the environment, in which PETs shall operate, is complexity. The more or less obvious strengths of P3P are that it is designed with flexibility in mind. P3P is hereby also distinguished from many other meta-data activities by the W3C. Platform for Internet Content Selection (PICS)[142], for instance, statically defines privacy practices. Options available in this case are thus a complete

---

[136] SSL is already in use in several services, such as in banking services (e.g. http://www.nordbanken.se)

[137] When not doing business at Web sites, and using SSL or SET, the individual messages such as email may be protected with a secure HTTP (SHTTP) see for instance http://www.sedeco.com.ar/secu1.html

[138] Burkert, *supra* note 105.

[139] See section 1.1.3 above.

[140] See section 4.1 above.

[141] Burkert, Id.

[142] See at http://www.w3.org/PICS/

accept or a complete reject when mismatch between users profile and providers' needs.

It is of certain interest that the flexibility makes it easy to implement P3P on Web site servers. Human-readable privacy policies may be automatically translated into the P3P syntax and most servers can be configured to support P3P implementations without installing additional software or extensions.[143]

Another important advantage with the P3P concept is that Web sites' traditional practices (and privacy policies) will be challenged/threatened. Hopefully this challenge also in reality makes service providers in general to a) be aware/reminded of privacy interests and b) to outline legally adequate privacy policies.

However, P3P has a number of limits as well. For instance, the complexity of the design (such as the communication syntax) may be of burden for developers of software for P3P transactions. Another critical point, is the lack of enforcement of the P3P negotiated agreement. A user that reaches an acceptable P3P agreement with a service, must have the necessary qualification to assume that the service abide that agreement, i.e. have the possibilities to call attention to liability for breach of contract. Sanctions available are in many cases quite trivial. In addition, there is a sufficient linkage between the privacy policies and the legal framework within which they are made. Self-regulatory codes like these may therefore be in need of *legislative stiffening*.[144]

Some external limits of PETs are their strong connection to market forces and demands. If there is a need for PET, the industry will build them.[145] On the other hand, to negotiate with every Web site visited may be somewhat tiring out for users in a longer perspective. There is a risk that a user will be more or less forced to give up her desires to the control of personal data in favor of access to Web sites in a "normal" fashion (in accordance with a cost-benefit argumentation). User tests of implemented prototypes are hence important in evaluating the practical effectiveness of P3P agents.

---

[143] The possibility to implement P3P extension header in forms of link tags also gives the alternatives to user one privacy policy for the entire site, or use several different policies for different parts of the site.

[144] See Roger Clarke, *Platform for Privacy Preferences: A Critique*, available at http://www.anu.edu.au/people/Roger.Clarke/DV/P3Pcrit.html, in which he describes the well aimed negatives on the coverage of privacy needs and of legal and cultural diversity, drivers for implementation and the mechanisms for ensuring compliance.

[145] Clarke, *supra* note 100.

5 The Next Step

5.1 Sum up

Hopefully, this paper has shown that privacy protection has an important role that is somewhat hidden in the overall hype over the Internet and its possibilities (in new economical prerequisites, business models, services, interactions etc). In United States there are new companies established built on the processing and dissemination of personal data. There are naturally certain risks for privacy in the forthcoming development of this personal information marked.[146] In Europe, small efforts have been addressed to the commercialization of personal information and the role (including impediment) privacy protection may have in the development of e-commerce.[147] This issue is however often raised in books, papers, and online articles etc of privacy commissioners and advocates around the world.[148] The reason for underlining this issue here, is that the use (and development) of technology in the US is frequently imported to European and other countries. It is thus of interest to learn how other measures than purely legislative ones may be of help to improve online privacy protection.

5.2 Recommendation for the outlines of a PET-project

5.2.1 Three work packages for improvement of online privacy

The outcome of this pre-study is, as aforementioned, that legislation is a primary tool to establish privacy protection rights. However, to improve the enforcement of these rights in online environments, there are mechanisms of non-legislative nature that can be of help. These mechanisms or measures can consist of:

a) To earn empirical knowledge through an Internet user survey. This gains better prerequisites to handle users privacy preferences in the next step.

b) The concept of Privacy Policies. These should be designed and used reflecting users' preferences, and backed up with means in cases of violation. The deeper understanding of policies is also of importance in a possible establishment of a national seal program.[149]

c) Implementation of a P3P agent application in Swedish based on users' privacy preferences and the design and use of privacy policies.

A few comments of the work packages are made in the following.

---

[146] Professor Peter Seipel at the Institute for Law and Informatics, introduces a new well-aimed concept regarding the e-commerce approach on personal data: TRAPs – Trade Related Aspects of Personal Protection Rights (in writing moment not yet published, see the Annual Book of Law and Informatics, 1999). Cf. the Gatt agreement – TRIPs, Trade Related Aspects of Intellectual Property Rights.

[147] Cf. WTO at http://www.nectar.org/update/stories/1998051202.htm

[148] For instance, see Lorrie Faith Cranor, *Internet Privacy: A Public Concern* by, available at http://www.research.att.com/~lorrie/pubs/networker-privacy.html, or Information and Privacy Commissioner/Ontario, *Privacy: The key to Electronic Commerce*, available at http://www.privacyexchange.org/iss/reports/ipcecommerce.html, *Vendors Balance Power Personalization With Privacy*, at http://www.techweb.com/wire/story/TWB19980206S0012

[149] Section 3.5 above.

5.2.2 Empirical knowledge through an Internet user survey[150]

Within the project presented herein, SISU has introduced cooperation with the Swedish Statistical Bureau (SCB) in order to perform a national survey of Internet users behavior when shopping online. Privacy preferences, policies, risks, trust or lack of trust and security aspects are the main issues included in an Online Privacy Questionnaire that hopefully will be launched later this spring.

Examples of questions raised here are:

- How often do you use the Internet for each of the following purposes (examples given)? Have you ever and in that case how often purchased anything online?
- How concerned are you about privacy of information?
- How willing are you to provide personal information to Web sites?
- Would you be more willing to provide personal information for online advertising purposes if the Web site compensated you for your information?
- How important is your consent when sites sell/share your personal information with others, track your movement around their site, sites track your movement around the Internet or track your online purchases etc.?
- How would your usage of the Internet change if Web sites disclosed their information, or disclosed their information and were reviewed by a third party assurance agent? [151]

5.2.3 The concept and consequences of Privacy Policies[152]

In addition, an internal survey should be made on privacy policies used by service providers on the online market of Sweden. Focus is on how often policies are used, whether or not they are in accordance with the legal demands of the Personal Data Act and the principles of OECD guidelines etc.[153]

Knowledge generated out of the empirical study will mainly be used for research on the questions connected to the appearance, use, and shape of privacy policies.

The aim is here to create a privacy policy for the Swedish online industry, built on the legal framework and with a user-friendly approach focusing on the following questions:

- What is the legal status of privacy policies?
- How should a policy meet the demands in legislation and at the same time be easily human-readable to Internet users?
- To what extent is it necessary to use several privacy policies for different areas of a Web site etc?

---

[150] See also project Web site: http://www.integritet.nu/survey.htm

[151] The outlining of these questions can be followed at the project Web site, Id.

[152] See 3.5.2 above and the Project Web site at http://www.integritet.nu/policies.htm

[153] An overview of the most common Swedish services and their policies is available (in Swedish) in Lundblad, Id., Project Web site at http://www.integritet.nu/elektroniska_spar.htm

5.2.4 A P3P agent application in Swedish[154]

Finally, the privacy policy generated out of a user study and with reference to the legal context, could be used as a default statement in the prototype of a P3P agent in Swedish.[155]

Issues to take into consideration in the implementation are for instance:

- Developing in compliance with new versions of Web browsers.
- The expression of practices and preferences.
- To locate and describe incentives and disincentives in the adoption process of the P3P model.

In addition, marking procedures associated with assurance programs, e.g. TRUSTe or BBBonline, and legal sanctions for non-compliance are naturally connected hereto.

P3P supports users to bring pressure on Web site providers to express acceptable practices. Whether they will actually do it or not, depends heavily on the credibility of the complete architecture and process of the P3P model.[156] The effectiveness of an implementation of a P3P agent application is also the task in a user study that evaluates the needs and caveats from a behavioral science approach.

---

[154] See also the Project Web site at http://www.integritet.nu/implementation.htm

[155] See section 4.4.4.

[156] See for instance Clarke, *supra* note 144.

List of abbreviations

ACL	Agent Communication Language
AI	Artificial Intelligence
CFP	Conference on Computers, Freedom + Privacy
DTD	Document Type Definition
EU	European Union
FTC	Federal Trade Commission
ISA	Intelligent Software Agents
IP	Identity Protector
MAS	Multiple Agent Systems
OECD	Organization for Economic Co-operation and Development
OPS	Open Platform System
P3P	The Platform for Privacy Preferences
PAI	Parallel Artificial Intelligence
PDA	Personal Digital Assistant
PETs	Privacy-Enhancing Technologies
PGP	Pretty Good Privacy
PITs	Privacy-Invasive Technologies
PICS	Platform for Internet Content Selection
RDF	Resource Description Framework
SET	Secure Electronic Transfer Transaction
SSL	Secure Socket Layer
TTP	Trusted Third Party
W3C	World Wide Web Consortium
WWW	World Wide Web
XML	eXtensible Markup Language

References

A Better Business Bureau, http://www.bbbonline.org/

Amazon, http://wwww.amazon.com

Anonymizer, http://www.anonymizer.com

AT&T Labs, *Anonymity Loves Company*, http://www.research.att.com/projects/crowds,
Privacy Minder 1.0.1 BETA, http://www.research.att.com/projects/p3p/pm/readme.html,
AT&T Chat 'N Talk: Getting to Know You without Getting to Know All About You (Helen A. Fairbrother, Elizabeth A. Hohne, Steven Todd)
http://zing.ncsl.nist.gov/hfweb/proceedings/fairbrother/index.html

Bacard, Andre, *Computer Privacy Handbook*, http://www.andrebacard.com/index.html,
http://www.andrebacard.com/remail.html

Bokus, http://www.bokus.se

Burkert, Herbert, *Privacy Enhancing Technologies and Trust in the Information Society*,
http://www.gmd.de/People/Herbert.Burkert/Stresa.html

Callaw, (Deger, Renee), *Putting a Price on Our Internet Identities*,
http://www.callaw.com/stories/edt0614f.html

Clarke, Roger, *Platform for Privacy Preferences: A Critique*,
http://www.anu.edu.au/people/Roger.Clarke/DV/P3Pcrit.html

Clarke, Roger, *Platform for Privacy Preferences: An Overview*,
http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html

Clarke, Roger, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*,
http://www.anu.edu.au/people/Roger.Clarke/DV/PaperProfiling.html

Clarke, Roger, (1998c) Submission, *Senate Legal and Constitutional References Committee, Inquiry Into Privacy and the Private Sector*,
http://online.anu.edu.au/people/Roger.Clarke/DV/SLCCPte.html#Need

Concord, *A Telematics Engineering Workshop on data privacy Working with the EU Data Protection Directive: Project experience and open practical issues*,
http://194.7.241.108/meetings/tewsoct99/agenda/agenda.htm

Cookiecentral, http://www.cookiecentral.com/

Cookie Crusher, http://www.supershareware.com/Apps/2620.asp

Cranor, Lorrie Faith, *Internet Privacy: A Public Concern* by,
http://www.research.att.com/~lorrie/pubs/networker-privacy.html,
P3P Privacy Tools, http://www.research.att.com/projects/p3p/,

Det IT-rättsliga Observatoriet, *Konsumenträttigheter i informationssamhället*, rapport 2/97.

DigitalMe, http://www.digitalme.com

Discussion Paper prepared for the EC Workshop in Seville on 25-26 October '99, *Personal Data Protection in the Digital Economy: the Role of Standardisation*,
http://www.law.kuleuven.ac.be/icri/papers/doctrine/standardization.pdf

Enonymous, http://www.enonymous.com

EPIC, Electronic Privacy Information Center, http://www.epic.org, *List: Online Guide to Practical Privacy Tools*, http://www.epic.org/privacy/tools.html

European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8,
http://europa.eu.int/comm/dg15/en/media/dataprot/law/fechr.htm

Flaherty, David H., *Protecting Privacy in Surveillance Societies*, (University of North Carolina Press, 1989), p. 8, table 1.

Graphics, Visualization & Usability (GVU) Center,
http://www.gvu.gatech.edu/user_surveys/survey-1998-04/

Hammarstedt, Per, *Deviation from the requirement of Consent for Distributing Personal Information on the Internet*, http://www.integritet.nu/white_pages_verdict.htm

Hammarstedt, Per, Myndighetsinformation i informationssamhället, En studie om myndigheters rättsliga stöd för informationsspridning med hjälp av IT, SITI-Publikation 1999:02.

Idzap, http://www.idzap.com/

Information and Privacy Commissioner/Ontario, *Privacy: The key to Electronic Commerce*, available at http://www.privacyexchange.org/iss/reports/ipcecommerce.html,

Jotter @ your service, http://www.jotter.com.

Legal Advisory Board, http://www2.echo.lu/legal/en/lab/lablab.html

Lumeria, http://www.lumeria.com/what1.html

Mayer-Schönberger, Viktor, *The Internet and Privacy Legislation: Cookies for a Treat?*, http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm

Net Detective, http://find-person.com/nd/, http://www.collector-club.com)

OECD, Organization for Economic Cooperation and Development, *Draft Background Report For The Ministerial Declaration On The Protection of Privacy on Global Networks*, http://www.oecd.org/dsti/sti/it/ec/prod/reg_11e.pdf,
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM#3,
Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet (October 1997),http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm,
Measuring Electronic Commerce 3 (1997), http://www.oecd.org/dsti/it/ec/prod/E_97-185.htm

Private Power Project (PPP), http://www.ppp.nu

Privacy Information Management System, http://www.nmda.or.jp/enc/privacy/p3p-press-en.html, http://www.w3.org/P3P/contributed/nec.co.jp/

Proxymate, http://www.lpwa.com/

Sedeco, http://www.sedeco.com.ar/secu1.html

Seipel, Peter, *Juridik och IT*, 6 uppl., 1997

Seipel, Peter, TRAPs – Trade Related Aspects of Personal Protection Rights (not published, see the Annual Book of Law and Informatics, 1999).

Simmel, Arnold, "Privacy", *International Encyclopedia of the Social Sciences*, vol. 12, p. 480.

Swire, P., Peter, Litan, E., Robert, *None of your business, World Data Flows, Electronic Commerce, and the European Privacy Directive*, 1998

The Uses and Limits of Financial Cryptography; A Law Professor's Perspective, http://www.osu.edu/units/law/swire.htm

Techweb, *Vendors Balance Power Personalization With Privacy*, http://www.techweb.com/wire/story/TWB19980206S0012

The European Commission, Directorate General XV, *Status of implementation of Directive 95/46*, http://europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm, *European Convention No 108*, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, http://europa.eu.int/comm/dg15/en/media/dataprot/law/fechr.htm

The European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

The European Parliament and Council Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Available at:
http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html

TRUSTe, http://www.truste.org/

US Department of Commerce, Secretariat for Electronic Commerce, *Staff Discussion Paper, A Framework for Global Electronic Commerce*, http://www.doc.gov/ecommerce/staff.htm

W3C, http://www.w3c.org, *Extensible markup language (XML)*, http://www.w3.org/XML/, *Resource Description Framework*, http://www.w3.org/RDF/, Specification (P3P 1.0) Draft 2 November http://www.w3org/TR/P3P, *PICS Extension for HTTP Cookies* http://www.w3.org/PICS/extensions/cookieinfo-1_0.html

Warren, Samuel D., Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, vol. 4 (December 1890), p. 193.

Webroot, http://www.webroot.com/

Whitaker Reg, *The End of Privacy, How total surveillance is becoming a reality*, 1999.

WinSqueeze, http://www.winsqueeze.com/

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes*, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp25en.pdf Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp27en.htm

WTO, http://www.nectar.org/update/stories/1998051202.htm

ZDnet, *B2B booming*, http://www.zdnet.com/anchordesk/story/story_4277.html, *Can you trust TRUSTe?* (Robert Lemos), http://www.zdnet.com/zdnn/stories/news/0,4586,2387000,00.html?chkpt=zdhpnews01

ZDnet, inter@ctive investor, *B2B E-Commerce To Skyrocket* (Mel Duvall), http://www.zdii.com/industry_list.asp?mode=news&doc_id=ZD2412831&pic=Y&ticker=

Öman, Sören, Lindblom, Hans-Olof, *Personuppgiftslagen*, Nordsteds juridik, 1998.

Court Cases

Stockholm County Administrative Court, Case number Ö 5456-98, verdict January 14, 1999.

US Supreme Court: *Boyd* v. *United States*, 116 US 616, 625-26 (1886).