Symbolic and Structuring Effects of the Internet on Privacy

Albin ZUCCATO, Simone FISCHER-HÜBNER
Department for Computer Science,
Karlstad University, Sweden
Albin.Zuccato@kau.se, Simone.Fischer-Huebner@kau.se

Abstract: Technology has influenced human lives since the beginning of mankind. Sociologists have described the effects that technology has on society as structuring or symbolic. We will use the same concepts to investigate the capability of the Internet to influence privacy. We analyse the structuring and symbolic effects of technology on privacy and thereby demonstrate some potentials of Internet technology and their effect on our life in society

Key words: Techno-sociology, structuring effect, symbolic effect, privacy, Internet, Privacy Enhancing Technologies

INTRODUCTION

Technology has influenced human life throughout our history. Today the progress of civilization is measured by means of technology. In this paper, we will discuss the structuring and symbolic effects of technology.

One of the most broadly discussed media in modern society is the Internet. The goal of this paper is to treat the effects of the Internet on life in society. We will focus our examination on privacy and look at how sociology describes the effects of technology on society. Our sociological approach will be a description of the effects as symbolic of structuring. Using comparisons with other techno-sociological approaches we will argue why we believe that this method is appropriate. In general, symbolic effects reflect how technology influences collective practice and the (sub)cultural meaning system, as well as the social behaviour of individuals. From a social viewpoint, structural effects describe the consequences of technology on the sensory perception and the practical actions of the subject.

Before examining effects on privacy, we will define privacy and Privacy Enhancing Technologies (PET). We must also look at social phenomena related to privacy and the Internet, in order to demonstrate that the Internet has comprehensive structuring and symbolic effects on the perception of privacy in modern society.

The first step is an investigation of structuring effects and a discussion of current legislative tendencies in the area of privacy and the extent of the Internet's influence on that legislation. We further discuss what we call extensive profiling - the automatic generation of extensive personal profiles describing different aspects of the individual's customs and behaviour - and describe the increasing demand for Privacy Enhancing Technology as another structuring effect.

Secondly, we deal with the question of how far symbolic effects can be observed. As an example, we analyse how greatly the Internet has influenced the perception of privacy as this relates to legislation in Europe and the US. We will also investigate the role of the Internet in the prevention of cyber-crime, cyber-war and cyber-terrorism in relation to privacy. We discuss tendencies concerning socially and politically motivated privacy organizations founded to act in response to the Internet's privacy threats.

This article, written by members of the IFIP Working Group 9.6/11.7 (IT Misuse and the Law), should contribute to the aim of their Working Group to develop an understanding of the impacts of IT systems on current IT law and potential problems and threats associated with IT systems and related legal concerns.

STRUCTURING AND SYMBOLIC EFFECTS OF TECHNOLOGY

This article describes effects of technology on society. To do so in a methodical way we must follow an approach that supports the investigation of the problem at hand. We have chosen to describe the effects we observe as structuring or symbolic as proposed by [Steinhardt, Ste99a].

We therefore start with the definition of symbolic and structuring effects and then will look at historic examples to clarify the application of the approach. Finally we investigate other techno-sociological theories and argue why we have chosen the approach in question.

Definition

In sociology the impacts of technology are described by its structuring and symbolic[1] effects. While all technologies that find a place in our daily life develop these effects, they are sometimes neglected and a particular technology disappears, only slightly influencing social life. There are also technologies - like the railway or the car - that have had such dramatic effects that they have been adopted into social life.

In the following section, we will use the railway as an example to explain what we mean by symbolic and structural effects. The railway is chosen for its familiarity, which makes it a good example of how drastic the effects of technology can be.

First we present a definition [Steinhardt, Ste99a] of symbolic effect: *"As a symbolic form technology has a double character: On one side it is an expression of collective practice and (sub)cultural meaning systems; on the other side it affects the subjects and their social behaviour"*[2]. This means that technology not only has a socio-cultural semantic effect (influence on social life) but also an effect on the subject's world experience (it influences the perception of the world and what the individual understands this to be). Consequently, the symbolic effect characterizes how the social individual sees his/her world on the basis of the existence or use of technology.

According to Steinhardt, technology not only influences our perception but also our activities. He says that *"(...)technology structures our sensory perception as well as our factual practical actions by suggesting specific ways of action and perception, preventing others, or presenting new ones (...)"*[3] [Steinhardt, Ste99a]. The structuring effect thus influences individual behaviour in proportion to technology. The difference is that the symbolic effect gives rise to a different worldview which generates a subsequent action whereas the structural effect causes a direct reaction.

Thus the focus of this method, and this article, is to describe effects of technology on society. As we are well aware, however, technology is also influenced by society and, as [Steinhardt, Ste99a] argues, there is reverse causality for every symbolic and structuring effect.

Historic examples

The steam engine and the railway are often considered a driving factor in the industrial revolution. The railway is used as an example to illustrate how effects can be classified as structuring or symbolic.

The following description is based on [Steinhardt, Ste99b]. Of course none of the descriptions present purely symbolic or structural effects, but one effect can be considered more distinct than the other.

Structuring – Unification of time

Before the introduction of the railway, every town had its own time based on the position of the sun that differed slightly from time in other places.

This was not important: the speed of travel was so slow that a few minutes earlier or later made no difference.

In the beginning of the railway history (in Britain), each station had a timetable written in local time. This affected people from other cities such that they became confused as they tried to fit their times to the local time. It is easy to imagine that this system proved very impractical. For this reason every railway company decided to create a timetable that gave the company's home city time as the reference time. This system was not successful either, as people had difficulty adjusting the different company times to the local time. Finally the pressing need for a harmonization of a country- wide time led to the creation of the Greenwich Mean Time system. Unified time stems from the railway - and today we see unified time as perfectly natural.

Symbolic – Change of perception behaviour

In his description of his Italian travels, Goethe writes about his departure from Frankfurt[4] with the post coach. He gives details about the different smells and portrays a farm close to his route. This is called direct perception.

In travel descriptions from the earliest history of the railway you find a very negative attitude: it is mentioned that the smell was awful and that the landscape passed at such speed that nothing was recognizable. People obviously still used direct perception. The same view is described some years later, but is portrayed then as a beautiful train trip through the passing landscape and a wonderful overall picture of the mountain area. A third author saw the same situation from another point of view: it was very refreshing to feel the pure rush of air, caused by the rapid speed of the train, on his face.

Here the perception has changed into what we call "panoramatic perception". The coming of the railway led to a different world perception mechanism, which represents a symbolic effect.

Theories of Techno-Sociology

In this section, Steinhardt's approach toward analysing technological effects on society by their symbolic or structural nature is briefly compared with other prominent techno-sociological approaches to explain why we have chosen Steinhardt's approach. We would like the reader to note however that this comparison should not be seen as a ranking or judgment of the theories described. Our only goal is to argue why the approach that we have chosen is the most suitable and appropriate one for our purposes.

We start with social constructivism as a prominent theory and will go on to investigate technological evolution, determinism and technological imperative as approaches to describing the interaction between technology and society.

Social constructivism

According to [Pinch and Bijker, PB87], social constructivism describes the "*development process of a technical artefact (...) as an alternation of variation and selection*" driven by social groups. This means that the development of a technology is driven by the selection of technological solutions to problems that social groups, interacting with the artefact, have.

This approach focuses apparently on the development of the technical artefact, whereas our goal in this article is to describe the effects of technology on society[5] .

Technological Evolution

The technical evolution theory sees the development of technology in a way similar to that of Darwin's theory of evolution. [Winner, Win77] argues that humans are merely a selection mechanism that decides which technology will survive and which will perish.

As this approach assumes that humans only determine the success of technology, it seems unsuitable to use it for a description of the effects of technology on mankind.

Technological Determinism

According to [Winner, Win77] technological determinism means *"(1) that the technical base of a society is the fundamental condition affecting all patterns of social existence and (2) that changes in technology are the single most important source of change in society"*.

From a general point of view, technological determinism would be applicable to our problem. However, we do not agree with the ultimate shaping role of technology. As Mesthene[6] puts it: "*patterns of technology are themselves largely influenced by conditions of the societies in which they exist*". We believe that technology is also influenced by social phenomena.

Technological Imperative

The concept could, according to [Winner, Win77], be put as *"technologies are structures whose conditions of operation demand the restructuring of their environment"*.

The focus on structures of operation seems too great a limitation for us, as it focuses more on physically existing technology than on a more abstract technology, which the Internet[7] is. We also assume that society itself is capable of choosing the way in which it can restructure. Thus the demanding character of technology does not fit our convictions.

After looking at different approaches, our conclusion is that the most promising way to describe the effects of the Internet on society is by symbolic and structuring means. The approach chosen is capable of structuring the effects of technology by including ideas of a backward coupling of effects on technology made by society to shape it[8] .

PRIVACY AND PRIVACY ENHANCING TECHNOLOGIES

Privacy is recognized as a fundamental human right. In general the concept of privacy has three aspects [Rosenberg, Ros92], [Holvast, Hol93]:

- Personal privacy - protection of a person against undue interference, such as physical searches or information violating his/her moral sense;
- Territorial privacy - protection of a person's close physical area;
- Informational privacy - control of whether and how personal data can be gathered, stored, processed and selectively disseminated.

The first definition of privacy was given by the American lawyers Samuel D. Warren and Louis D. Brandeis, who in their article "The Right to Privacy" published in 1890, defined privacy as "the right to be let alone" [Warren and Brandeis, WB90]. The most common definition of informational privacy in current use is given by Alan Westin: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [Westin, Wes67].

With increasing personal data traffic over the Internet and expanding Internet applications (such as eHealth-, eGovernment, and e-/m-Commerce), it is mainly the informational privacy of individuals that is at risk which, according to Westin's and other common definitions can be defined as the right of informational self-determination. Nonetheless, in the mobile and traditional Internet, the problem of unsolicited commercial emails (spam) is increasingly affecting privacy in the sense of the right to be let alone. It can also be seen as an intrusion of territorial privacy and of privacy of the person (if indecent or offensive information is distributed). Hence, with the expanding mobile and traditional Internet, all three aspects of privacy are at risk.

To protect the right of informational self-determination, data protection laws of primarily Western states, as well as international privacy guidelines or directives (such as EU Directive 95/46/EC on Data Protection [European Union, Eur95]) and the OECD privacy guidelines [OECD, OEC80], require basic privacy principles to be guaranteed when personal data are collected or processed. These include:

- Legitimacy: personal data collection and processing are admissible only if permitted by legal provisions or if the data subject has consented (Art. 7 EU Directive);
- Purpose specification and purpose binding: personal data must be obtained for specified and legitimate purposes and should not be used for other purposes (see Art. 6 EU Directive);
- Necessity of data collection and processing: the collection and processing of personal data shall only be allowed if it is necessary for the tasks falling within the responsibility of the data processing agency (see Art. 7 EU Directive);
- Transparency and basic rights: the data subject's right to information, notification and objection and the right to correction, erasure or blocking of incorrect or illegally stored data (see Art. 10 - 14 EU Directive);
- Requirement of adequate technical and organizational security mechanisms to guarantee the confidentiality, integrity, and availability of personal data (see Art. 6, 17 EU Directive).

An international harmonization of data protection legislation, besides the EU Directive on data protection is needed, but hardly achievable due to cultural, historical and political differences (see also [Fischer-Hübner, FH00]). The recent transatlantic debate about the adequacy of the Safe Harbour privacy principles in comparison with the EU data protection directive has demonstrated the difficulty of harmonizing data protection legislation. For this reason and because law is not an ultimate protection, it is required that privacy should also be protected and enforced by technology and should be a design criterion for information and communication systems.

There are two major ways of enhancing privacy in the Internet by means of technology. Privacy can be protected most effectively by technologies that avoid or at least minimize personal data and that thus provide anonymity, pseudonymity, unlinkability or freedom from observation for the users. The requirement of personal data avoidance or minimization can be derived from the legal privacy principle of the necessity of data collection and processing, which requires that personal data should not be collected or used for identification purposes when not truly necessary. However, such technologies cannot be applied in applications where personal data must be processed. Other privacy technologies can technically allow a control that personal data are used only according to legal provisions. For instance, the Platform for Privacy Preferences Protocol (P3P) by W3C [W3C, W3C02] can be used to enhance transparency and control for users over the use of personal information on Web sites they visit.. Further examples are privacy access control models that can technically enforce legal privacy requirements, such as the necessity of data processing and purpose binding (see [Fischer-Hübner, FH01], [Karjoth and Schunter, KS02]).

STRUCTURING EFFECTS ON PRIVACY

Today we face a communication era in which the Internet is structuring our privacy related behaviour and perception. An influence on our ordinary behaviour can be recognized already, and this tendency will influence us even more in the future when phenomena like eCommerce and global information society become daily realities.

Legal aspects

Provisions of the OECD Privacy Guidelines, EU Directive 95/46/EC on Data Protection and national data protection laws also apply to the collection and processing of personal data in mobile and traditional Internet environments. Nevertheless, more specific privacy requirements for the Internet were recently formulated in Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communication sector [European Union, Eur02]. This new directive, 2002/58/EC, has replaced the directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector [European Union, Eur97] and, in contrast to directive 97/66/EC, has an extended scope to apply to both the classic telecommunication sector as well as the Internet sector. Whereas in Directive 97/66/EC traffic data refer only to "calls" in so-called circuit switched connections (traditional voice telephony), the new directive, COM (2000) 385, covers all traffic data in a technology neutral way, including Internet traffic data.

In addition to the protection of traffic data, directive 2002/58/EC also addresses location data giving the geographic location of mobile users or, more precisely, of their devices. It thereby acknowledges that, particularly in the mobile Internet, mobile location based services that allow the tracking of a user's location require appropriate privacy safeguards for ensuring location privacy. According to its Art.9 I, location data may only be processed when they are anonymous or, with the consent of the users or subscribers, to the extent and for the duration necessary for the provision of a value added service. Exceptions are formulated for emergency services (Art.10) and for necessary measures to safeguard security, defence and criminal investigations (Art. 15).

Further Internet-related privacy problems that are regulated are unsolicited communication (spam) and cookies. Art. 13 introduces an opt-in system for unsolicited electronic mail and thus restricts spam. According to Art.5 III, Member States must ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed if the subscriber or user concerned is provided with clear and comprehensive information and is offered the right to refuse such processing by the data controller. This provision should protect users and subscribers against cookies, spyware, web-bugs and other hidden privacy-intrusive data collection techniques.

We have discussed above two different kinds of structuring effects for privacy legislation. The first kind of effect is that existing legal rules are enhanced in order to cope with Internet-related privacy risks. The second type, a generating effect, is that new legislation is introduced to cope especially with problems such as spamming, cookies or location privacy which have especially emerged with the use of mobile Internet technology.

To protect privacy rights on the Internet, a more Internet-specific privacy legislation must be enacted, in addition to general data protection legislation.

Extensive profiling

Introduced in 1930, "Gläserner Mensch" - "Visible Man" [Deutsches Hygiene Museum, Deu02] made the physiology of a human visible. The term has taken on a second meaning since then, away from the natural sciences to a more sociologically oriented meaning where it is seen as a representation of a person about whom various pieces of information (private as well as public) are gathered and compiled into profiles. Profiling sufficiently extensive to generate a "Visible Man" was unfeasible without the funds of a governmental organization in the pre-Internet world, for reasons of processing and storage restrictions. However, with emerging Internet technology, where users leave traces of their communication and consumer behaviour and in which there are cheap processing and storage capabilities, profiling also becomes possible for less powerful organizations.

With the help of two examples, we will try to demonstrate the special role of data networks (especially the Internet) in their relation to extensive profiling.

Customer Profiles

A classic goal in marketing is to determine and exactly analyse the preferences of a potential customer in order to be capable of determining his/her special needs. With this knowledge, it is possible to create a demand by the customer and to then fulfil it at the present as well as in the future. In regular business, it is almost impossible to collect all data about a person's behaviour due to the limited processing capabilities of conventional tracking methods. It is of no doubt that an exact recording of every step of the customer's actions would violate privacy. The result would probably be that he or she would immediately stop the business relation.

The situation is different in the case of electronic purchases (eCommerce). Here all data about a customer's choices and purchases are available via an electronic data processing system, which makes it easy to create a profile of the demands and wishes of a customer. This information can accordingly be used as part of targeted marketing.

At the moment, Amazon.com[9] is one of the most popular eCommerce sites. The business concept of Amazon is to create a platform for the purchase of books for the customer. The customer has no contact with the delivering book dealer. Amazon plays the middleman, who passes the order to the local partner in the customer's neighbourhood. The local partner conducts the effective commerce activity and Amazon receives a part of the commission. This kind of activity is often defined as virtual business.

A model of this kind is dependent on the volume of books that is sold via the company. To reach sales goals it has been necessary to choose an active marketing policy by means of exact user profiles and, with help of this information, to offer potentially interesting books to the customer. These user profiles are based on a very precise recording of every book chosen and purchased. Such a structure of course has a very great effect on the privacy of a customer.

In some Internet sites the customer is required to register and supply a great deal of personal information about his/her preferences to be entitled to reductions or allowed to use the service. This means that the customer is asked to sell his or her privacy in exchange for certain advantages. Sites such as GMX*TM*[10] and other free-mail providers are good examples of this. Here the customer is offered a free email account if he/she provides a multi-page preferences set. This information is then used for direct marketing. GMX*TM* explains that it is financed by advertising and therefore needs a detailed profile. A look at their service supply page shows that they do direct marketing, based on the user profiles collected previously, to everyone.

It can be argued that privacy is deliberately given up in exchange for certain benefits. However, customers are often unaware of such privacy intrusions. We believe that if they knew they would probably not use the service or would reconsider their actions.

Thus, the structural effect of the Internet is that it enables the creation and use of extensive customer profiles, and several organizations will use these options. As such, the Internet enables privacy intrusions and related behaviour that has not possible to that extent before this time. Another structuring effect on privacy that arises from profiling is the orientation toward financial profit that often threatens privacy.

Aggregated Profiles

We described in the section above how companies can use customer profiles to their benefit. If we imagine that someone collects profiles from different sources and combines them, even more information can be gained about individuals.

In Austria and other countries, legal authorities are entitled by law ("Sicherheitspolizeigesetz" - security police law) to collect data on individuals without their knowledge. This legislation was introduced in Austria to enable law enforcement to prevent criminal activities.

In the "Briefbomber" (mail bomber) case some years ago, Austrian police used the permission granted by the "Sicherheitspolizeigesetz" to generate a profile about a potential suspect and then processed large amounts of data to look for people fitting the profile. To the police's disappointment, they did not succeed in finding any true suspects but instead severely affected the privacy of a large number of innocent citizens who had been identified as suspects. That the terrorist was found in the end was pure luck and not due to the profiling investigations. For us it is more interesting however that the whole investigation was only possible by means of interconnected computers, where a single controlled machine collected and aggregated data from different sources.

The structuring effect of the Internet here was not the release of a law - as this already existed. Internet technology in fact made it possible for the police to use the legal basis in a new way. Thus the structuring effect was that the Internet produced a new method of investigation that strongly affected privacy. It could be argued that it is acceptable to restrict the privacy of criminals. However, a large number of unrelated innocent people also had to face an intrusion into their privacy.

Looking at the potential of aggregated profiles we can imagine that, in the future, non-governmental organizations will also increasingly become engaged in generating aggregated profiles - especially if we consider large multi-national organizations or groups of direct marketing oriented companies. Here again, the Internet's structuring effect is a constructing one.

Examples of companies that engage in extensive user profiling are service providers such as DoubleClick. These companies use advertisement banners or web bugs to collect information on websites visited by a user by means of cookies and then accumulate the information on visits to all the different sites on which they put advertisements or web bugs. Hence, an aggregated profile of the Internet users' preferences can be compiled (and later be used for customizing web pages) with the data on these users, who are usually uninformed and thus unaware of this kind of profiling.

Increasing demand for privacy-enhancing technologies

Privacy enhancing technologies (PET) are important security technologies for protecting the privacy of users and data subjects. Basic technologies for protecting the user's privacy, such as Mix nets, DC nets, Anonymous Re-mailers and blind signatures, were introduced in the 1980s by David Chaum and other researchers. On the way to a networked society, where all user communication and actions on the Internet can be easily traced and compiled into extensive user profiles, privacy technologies are becoming increasingly relevant.

Thus another structuring effect of the Internet has been an increasing awareness of the need of PET and the expansion of PET research and of a commercial market for privacy technologies. PETs have also become an issue for standardization activities.

In 1995, the Dutch Data Protection Authority (the Registratiekamer), in cooperation with the Information and Privacy Commissioner for the province of Ontario, Canada [van Rossumn et al, vRGB+95], created the term PET in their reports on "Privacy-Enhancing Technologies - The path to anonymity". Since then, further PET studies and research by data protection commissioners and research labs have been initiated, and PET research is becoming an important part of security conferences and publicly funded research programs.

The IT market has also responded to the user's privacy needs. Some companies, such as Anonymizer.com and ZeroKnowledge Inc., have started to offer privacy-enhancing security products, although so far with only limited economic success. In November 2001, IBM established its Privacy Institute, which is an organization in IBM Research to promote and advance research in privacy and data protection technology. The Institute's goal is "*to develop the necessary technologies for enterprises that enable the transition from today's privacy-unaware or even privacy-intrusive ways of* *doing eBusiness to privacy-enabling ways*". It has created a global research program to develop new privacy-enhancing services and technologies, among others for eBusiness solutions and pervasive and mobile computing and knowledge management [IBM, IBM02].

Standardization bodies have recently given attention to privacy-enhancing technologies. An important standardization document acknowledging privacy as a significant technical security aspect is the harmonized Common Criteria [ISO, ISO99] for security evaluation, which became an International Standard (IS) 15408 in December 1999. The Common Criteria define a Privacy Class that can be used to describe and evaluate the security functionality of PET, mainly for protecting the privacy of users while communicating over the networks. One of the main privacy initiatives of the World Wide Web Consortium (W3C), which promotes interoperability for the World Wide Web, has been the Platform for Privacy Preferences P3P, which became an official W3C recommendation in April 2002. Microsoft has already incorporated P3P functionality in its Internet Explorer to allow users to be well informed about and to better be able to control the use of cookies.

In contrast to the other PET effects presented, where technology influences society, we see the phenomenon that expectations driven by society form the technology. This means that the existence and shape of technology are determined by its social application. [Steinhardt, Ste99a] argues that these influences of technology and society in both directions are true for all effects. We agree with this but would like to argue that, as concerns privacy, this effect is most notable for PET and is therefore mentioned only here.

SYMBOLIC EFFECTS ON PRIVACY

For the most part, the symbolic effects have a much deeper impact on society than the structuring effects. It is easy to see from a historic viewpoint what kinds of symbolic effects a technology has had. It is difficult to predict how present and future tendencies will develop, and it is a vague field to move in, as it is impossible to predict the potential changes that will occur in society. It is also important to keep in mind that we use our own cultural meaning system, even though we have tried to minimize its influence.

We therefore wish to clarify that our perspective is based on the central European culture and may be seen quite differently by others. Nevertheless, we hope to show some of the symbolic effects in ongoing developments and to point out the tremendous potential of the Internet in relation to the influence on our culture and subcultures.

Tendency – Privacy Regulations – Difference between the USA and Europe

Owing to different cultural backgrounds, the development of the concept of privacy has taken different directions in the USA and Europe.

Negative historic experiences, where dictator regimes violated the privacy of individuals, have led European development to foster strong data protection that covers both the public and the private sector. These regulations have raised awareness about privacy (among individuals as well as organizations).

The situation is different in the USA, however. The public sector is covered by the US Privacy Act on the federal level and, on a local level, the states have their own data protection legislation. In the private sector, statutory privacy regulations cover only a few specific areas (e.g. video rental) while most areas are unregulated by law and a self-regulation approach is supported in order to protect privacy. Furthermore, in contrast to Europe, the US has no data protection authorities to regularly monitor data processing and act upon complaints made by data subjects that believe that their privacy rights have been violated.

As demonstrated above, the Internet has developed structuring effects concerning privacy behaviour via adjusted legislation. Here we would like to present two symbolic effects related to that area.

The first symbolic effect is that a cultural awareness related to privacy has developed in both cultures, although to different extents. People are caring more about their privacy in the Internet society. The effect is that the industry has been motivated to introduce privacy extensions and privacy-enhancing technology into their products, as discussed above. An example is that more and more privacy statements can be found on companies' web pages. This has led to the interpretation that privacy is becoming a sub-cultural (here meaning the Internet subculture) topic and is receiving greater and greater attention. A further result is that the subculture starts to span over multiple cultures as a subset of them.

Another symbolic effect is expressed with the "Safe Harbour initiative" - an initiative for harmonizing privacy protection in the global world of the Internet. A cultural need can be discerned (driven only partly by legislation) to harmonize the two cultural approaches to privacy. European cultures were forced to accept the US' method for (self-)regulated privacy protection by means other than legislative ones. The US, on the other hand, must consider a more formal and stricter regulation to satisfy European needs. And even after the formal enactment of safe harbour, both parties criticized[11] and even questioned[12] the agreement and its enforcement. All the problems with its introduction underline even further the symbolic effect. If we recall the first description of the railway - which was not at all positive - we can conclude that a cultural change rarely meets with any resistance[13].

Tendency - Cyber-War, Cyber-Crime and Cyber-Terrorism

The September 11th catastrophe started very broad discussions about terrorism. Suddenly this has again become a major issue of public interest. Information scientists and the military had long spoken of the potential of using the Internet for cyber-war, cyber-crime and cyber-terrorist activities. From a crime perspective, fraud, copyright infringement and illegal pornography have become problems impossible to ignore. The economic and social damage caused has taken dramatic dimensions.

Extrapolating a crime scenario to a terrorism scenario doubtless generates fear. There is namely a critical difference between these two forms of attacks: the crime scenario has (personal) financial profit as its motive, whiles the terrorism scenario, on the other hand, has fanaticism at its roots. It is consequently very unpleasant to imagine the potential of the Internet. Used in an organized way it could easily lead to a cyber-war.

Speculative media reports about September 11th state that the terrorists used steganography to hide their communication over the Internet. As a consequence, control measures such as crypto controls that had already been ruled out as being more privacy-intrusive than effective for fighting cyber attacks, were suddenly again proposed. In addition, new privacy-intrusive controls, such as "antiterror biometrics", are being discussed. The USA Patriot Act, signed by President Bush in October 2001, is expanding surveillance of Internet users, e.g. through wiretapping or spying on web browsing, with reduced checks and balances. In other Western countries, similar acts have been passed or are under discussion. The effects of these control measures on privacy have been broadly accepted out of fear.

Given the threat of terrorism via the Internet, the effects on privacy are that people are forced to accept restrictions to their privacy. The cultural need for privacy has been overruled by the technical possibilities of cyber attacks. Thus, a symbolic effect on society can be seen - not directly implied by the technology itself, but by means of its effects. Furthermore, the technology is the vehicle and therefore also the symbolic reason.

Looking at cyber-crime threats we can see that the (structuring) effect of the Internet is that more crime preventing legislation is starting to address this kind of crime - such as the cyber crime treaty of the Council of Europe [Council of Europe, Cou01]. This legislation entitles authorities to restrict the privacy rights of people during investigations. The symbolic effect is that, with the emerging threats of child pornography and other forms of cyber-crime, people are shocked and call for preventive actions by authorities, while at the same time accepting drastic privacy restrictions.

Tendency – Private persons organizations

With the widespread use of the Internet, several privacy organizations have received public attention (such as the Electronic Privacy Information Center (EPIC), Privacy International,...) or have been founded (Internet Privacy Coalition ...). These organizations - here called private person organizations (PPO), as their major goal is to protect private persons - try to exert symbolic and practical opposition to the existing tendency to undermine privacy through the use of insufficiently regulated technology, technology that lacks any regulation at all or out of total ignorance.

PPOs such as EPIC try for example to create court cases in the United States to make privacy violations obvious. They are active mainly against the US government but have also generated some court cases against private corporations. Here the Internet plays a double role. The symbolic effect of the Internet here is that it has caused/initiated privacy activities or campaigns organized by PPOs.

Another symbolic effect of the Internet seems to be that it enables the generation and prosperity of organizations. The "Internet Privacy Coalition (IPC)" uses the technology as a part of its name. Their motto is: "*The Mission of the Internet Privacy Coalition is to promote privacy and security on the Internet through widespread public availability of strong encryption and the relaxation of export controls on cryptography.*" [IPC Homepage, 1999].

CONCLUSION

We have described a wide spectrum of privacy-related effects of the Internet. Even if we think that none of these should be seen in isolation, or as being caused solely by the Internet, they show an influence on privacy that is caused mainly by this technology.

From a structuring perspective we have seen effects that grant us more specific privacy rights. Unfortunately, there are also major structuring effects caused by the Internet that are threatening our privacy. As a secondary cause of privacy threats we have found a group of structuring effects that seems to neutralize negative effects. Recalling parts of the definition of structuring effects – *(...) suggesting specific ways of action and perception, preventing others, or presenting new ones (...)* – we see that the Internet gives rise to all three possible action modifications.

In the introduction to the symbolic effect section we wrote that symbolic effects are more difficult to analyse because of the problem of being part of the system under observation. We have nevertheless attempted to point out some symbolic effects. All the effects indicate that the Internet influences both our social behaviour with respect to privacy as well as the perception of privacy and privacy needs. Recalling again the definition – *(...) an expression of collective practice (...) affects the subjects and their social behaviour (...)* – (...), we see the exactness of this fit. The symbolic effects provide evidence of the importance of the Internet – only a technology of this kind could have produced these effects in such a short time.

While we hesitate to predict future effects based on current trends we believe that the Internet will exert even greater influence on our daily life and on our privacy-related behaviour. We would like to go further and say that we believe that the Internet - not only with respect to privacy - will shape our society as much as the railway or the car has done earlier.

REFERENCES

[Cas56] Ernst Cassirer. *Wesen und Wirken des Symbolbegriffes.* Wissenschaftliche Buchgesellschaft Darmstad, 1956.

[Cou01] Council of Europe. Convention on Cybercrime - European Treaty Series - No. 185. Technical report, Council of Europe, 11 2001.

[Deu02] Deutsches Hygiene Museum. *Kurze Geschichte der Gläsernen Figuren,* June 2002.

[Eur95] European Union. 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, 1995.

[Eur97] European Union. 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, 1997.

[Eur02] European Union. Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC, 2002.

[FH00] Simone Fischer-Hübner. Privacy and Security at Risk in the Global Information Society. In D. Thomas and B. Loader, editors, *Cybercrime.* Routledge. London and New York, 2000.

[FH01] Simone Fischer-Hübner. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanims.* Lecture Notes in Computer Science. Springer, 2001.

[Hol93] J. Holvast. Vulnerability and Privacy: Are we on the way to a risk-free society? In *Facing the Challenge of Risk and Vulnerability in an Information Society,* J. Berleur, C. Beardon & R. Laufer editors, Proceedings of the IFIP-WG9.2 Conference, Namur May 20-22, 1993, IFIP Transactions A-33, Elsevier Science Publishers B.V. (North-Holland), 1993.

[IBM02] IBM Privacy Institute, http: //www.research.ibm.com/privacy/, 2002.

[ISO99] The Common Criteria for Information Technology Security Evaluation (CC) version 2.1 (aligned with IS 15408), 1999.

[KS02] Günther Karjoth and Matthias Schunter. A Privacy Policy Model for Enterprises. *15th IEEE Computer Security Foundations Workshop*, June 24 - 26 2002.

[OEC80] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 1980.

[PB87] Trevor Pinch and Wiebe Bijker. *The Social Construction of Technological Systems*, chapter 1 - The social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other, pages 17 – 50. MIT Press, 1987.

[Ros92] R. Rosenberg. *The Social Impact of Computers*. Academic Press, 1992.

[Ste99a] Gerald Steinhardt. Auf dem Weg zur kaleidoskopischen Wahrnehmung. Überlegungen zur Subjekt-Konstitution und Welt-Erfahrung im Zeitalter der neuen Informations- und Kommunikationstechnologien. *Psychosozial*, 22(1): 81–98, 1999.

[Ste99b] Gerald Steinhardt. Technische Universität Wien: *Techniksoziologie und -psychologie*. Lectures notes, 1999.

[vRGB+95] Hanke van Rossumn, Huib Gardeniers, John Borking, Ann Cavoukian, John Brans, Noel Muttupulle, and Nick Magistrale. Privacy-enhancing technologies. Technical report, Registratiekamer/The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995.

[W3C02] W3C, www.w3c.org/P3P/. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, April 2002.

[WB90] D. Warren and D. Brandeis. The Right to Privacy. *Harvard Law Review*, (5): 193–220, 1890.

[Wes67] Alan Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

[Win77] Langdon Winner. *Autonomous Technology*. Lighthouse Press, 1977.

[1] For a discussion of the term symbolic see [Cas56].

[2] Als symbolische Form kommt Technik ein Doppelcharakter zu: Zum einen ist sie Ausdruck kollektiver Praxis und (sub)kultureller Bedeutungssysteme; zum anderen wirkt sie auf die Subjekte und ihr soziales Handeln ein."

[3] (...) strukturiert Technik sowohl die sinnliche Wahrnehmung als auch das praktische Handeln der Subjekte , indem sie bestimme Handlungs- und Wahrnehmungsweisen nahelegt, andere verunmöglicht, neue eröffnet (...)

[4] His home town at this time

[5] We are well aware that this is bidirectional and, as is later argued, the approach chosen also supports this understanding.

[6] Technological Change: Its Impact on Man and society, p. 20, 1970, cited in [Win77]

[7] We consider the Internet as all information which is interlinked and not as the physical routers, gateways and computers.

[8] See arguments given in section

[9] Amazon.com, Inc. – www.amazon.com

[10] GMX Aktiengesellschaft – www.gmx.net

[11] A report of the European Commission in February 2002 on practical operation of the safe harbor agreement was criticized insufficient transparency among the organizations that have signed up to safe harbor.

[12] The Bush administration has pressed the EU Commission in March 2002 to weaken the proposed privacy standards for consumers, claiming that they would make it difficult for US financial institutions to conduct business abroad.

[13] Tom DeMarco and Timothy Lister discuss in their book "Peopleware" that changes almost always face resistance.