Criteria for Privacy Supporting System

Markku Laukka

Department of Computer Science
Helsinki University of Technology
P.O.Box 9700 02015 HUT Finland
Tel: +358-9-451-5786
E-mail: markku.laukka@tml.hut.fi

The concern about privacy issues has increased among web store customers. The merchants are trying to convince the public about the level of privacy on their sites by using privacy statements. This is not, however, an easy task, because the very nature of privacy is unclear. It is hard to define the requirements for a system that is capable of protecting the privacy of the users. The approach of this study is first to explore the research on the psychological processes of privacy regulation and then to analyse its fundamental elements. Thereafter, the acquired knowledge is used to define a set of criteria for a system that is able to fulfill the requirements of human privacy processing and is able to support that process in online situations.

Keywords: Privacy, trust, control, system requirements, personal information

Introduction

"**The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to.** "

George Orwell, 1984.

In his famous piece, George Orwell described a world of continuous and uncontrollable surveillance. Presumably, there is little controversy about the fact that the privacy of Winston was severely violated. However, when we come closer to the everyday life, the distinction between justified collection of information and an unjustifiable invasion of privacy seem to be harder to make.

The data collection in the Internet has been a topic of lively discussion lately (see e.g. the Wired magazine[1]). Many attributes of the electronic marketplace, the web pages, are quite easy and cheap to change even every time the page is downloaded. Therefore, it is possible to tailor the service every time a different customer enters, and

[1] www.wired.com

to aim the marketing more accurately to the potentially interested customers. This requires, however, that the relevant customer information is available.

Compared to the real world entrepreneurs, an Internet store is in a good position when it comes to gathering customer data. The identifying registration forms together with cookies make it easy to follow the actions of even a single, identified customer. The "normal" offline trade has also its own ways of collecting customer data. The company discount cards are used for just the same purpose as cookies and registration forms in the web. However, the new merchants seem to have much more problems with the customer reactions toward this data collection than their more traditional counterparts do (BW/Harris Poll, 1998).

To react to the rising concern among the customers, many merchants are attaching privacy statements to their sites. In these statements the will to protect the customers' privacy is expressed. For example, a lately bankrupted Internet toy retailer, Toysmart, assures that "we take great pride in our relationships with our customers and pledge to maintain your privacy while visiting our site". However, the compliance with these promises is sometimes far from perfect: it seems that the degree of actual privacy depends more on the wording of the privacy statement than the spirit of it. At least three companies, Boo.com, Toysmart[2] and CraftShop.com have either sold or are trying to sell customer data that can include personal information such as phone and credit card numbers (CNET news, June 29.[3]). This is surprising since two of these, Toysmart and Boo.com were granted the TRUSTe[4] seal as they "adhere to TRUSTe's established privacy principles of disclosure, choice, access and security".

As manifested in the behavior of these TRUSTed companies, it seems that the term 'privacy' can be used in so many meanings that the existence of a privacy statement is not enough to ensure the protection of this unclear condition in a satisfying way. Therefore, we present that it is highly important to establish well-defined criteria for a privacy protecting system to help the merchant to set focused goals for the system development and help the customer to get a clear picture of the features she is justified to demand.

To be able to address the necessary factors influencing the regulation of privacy in the internet and to notice the factors invalidating this process, we must first understand the determinants of the privacy regulation we conduct successfully every day. This study reviews the research on information privacy regulation and discusses its applicability, limitations and implications when applied in the Internet. On the basis of this analysis, a set of criteria for a privacy supporting system is established.

The rest of this paper is organised as follows: in the first half of the paper the fundamental elements of privacy are presented. First, the nature of control needed in the privacy regulation is discussed. Next, the different types of privacy, and the distinctive features of information privacy are studied. Then, the functions that privacy regulation serve are explored before the different mechanisms to enforce a certain level of privacy. Discussing the three central elements affecting the desired level of interaction in a given situation ends the review of the elements of privacy regulation. After collecting together the central building blocks of the concept of privacy, a brief conclusion of them is presented before proposing criteria for a privacy supporting system. After the criteria have been presented, some possible directions for

[2] www.toysmart.com

[3] news.cnet.com

[4] www.truste.com

future research are discussed, ending with a conclusion of the paper.

Defining Privacy

It is common to hear people talking about their privacy. However, in the everyday language the meaning of the word is quite unclear, and this meaning changes from one situation to another. It is possible, for example, to talk about a private place while referring to a quiet place. However, privacy can be invaded in a crowded place, indicating that before the invasion, some form of privacy was enjoyed.

Unfortunately, in the field of research this confusion further continues. The concept of privacy has aroused much interest in many different disciplines, including at least psychology, legal science, sociology, computer science and philosophy. The wide use of the term has resulted in numerous definitions and different ways to look at this phenomenon. In the literature, the term privacy seems to be connected to a group of different settings. For example Pedersen (1997) has separated six different types of privacy, four of them originating from Westin (1967). These types are solitude, isolation, anonymity, reserve, intimacy with friends, and intimacy with family. *Solitude* refers to being in a position, where other people can't see or hear what a person is doing. *Isolation* involves using physical distance to separate oneself from others. *Reserve* means controlling the verbal disclosure of personal information to others. *Intimacy with friends* and *intimacy with family* are conditions of being alone with a group excluding other people. Finally, *anonymity* is seeking privacy by going in a crowd of strangers without being identified.

Even though these different types of privacy have clearly many separating features, they can still be treated as different manifests of a single process. If these types of privacy are examined in more detail, it is evident that all of these are conditions in which the individual can somehow control the level of interaction with other people.

The Central Role of Control

If we go through the different definitions of privacy, the absence of unwanted input from others seems to be present in most of them. However, when it comes to voluntary, desired, inputs from others, the definitions deviate. For example Fisher (in Newell, 1995) describes the condition of privacy in the following manner: "(privacy occurs)... when the watching self and the world fall away, along with geometric space, clock time, and other contingencies, leaving an intensified relationship with the intentional object". The essential nature of privacy is here to be free from any external input. However, we can see that this kind of privacy definition leaves no room for intimacy kind of privacy presented by Westin and Pedersen, where privacy can be experienced in a close group of people being together voluntarily. So, if we want to accept the idea that intimacy is one type of privacy, we must find a different focus for our definition.

In fact, instead of concentrating on the limited level of interaction, the most definitions of privacy do stress the central importance of *control*. Westin (1967) has presented that privacy has a property of having "freedom to choose what, when and to whom one communicates", including "personal control over personal information". Jourard (1966) saw privacy as a result of a person's wish to control the perceptions and beliefs that others might hold of her. Folly and Finighan (in Newell, 1995) shared this belief: "Privacy is the possession by an individual of control over information that would interfere with the acceptance of his claims for an identity within a specified role relationship". To conclude, all these definitions stress the ability to control the level of inputs and outputs from the other people.

Now, if we focus our definition of privacy to the ability to control the level of

interaction, we must further discuss the nature of that control. In fact, *control* contains not only the ability to choose, but also the ability to *enforce* the selected output. Johnson (1974) separated four elements of such regulatory control. They were the control over choosing the desired outcome (level of privacy); the control over selecting the behaviours to pursue the selected outcome; the factual effectiveness of the selected behaviours; and the ability to monitor and evaluate effectiveness of the selected behaviours in reaching the desired outcome. This analysis was adopted also by Altman (1975) to his model of privacy regulation discussed later.

In addition to the theoretical work concerning privacy, the central role of control has been confirmed also by empirical studies. Fusilier and Hoyer (in Tolchinsky et. al., 1981) found that those individuals who perceived that they had some control over the uses of information after its disclosure, experienced less of an invasion of privacy than did those individuals who believed that they had no control over the uses of information. In fact, the violation of the right of a given individual to control her private area, be it physical space or personal information, seems to be the major factor making the individual feel that her privacy has been invaded. The information in itself may not be the issue. It is easy to find examples by only exploring the websites of individual people. These sites may contain loads of personal information that the site owners voluntarily publish for everyone to study. However, if another person were to download the page and set it in another public forum, the original site owner could still experience this as an invasion of privacy.

Dimensions of privacy

Now, being in control seems to be an essential element of the feeling of privacy. In this section we discuss the areas people want to control, dimensions of privacy. Burgoon (1989) has, on the basis of a literature review, delineated four dimensions of privacy, each with distinguishing set of properties. These partly overlapping dimensions are physical, interactional (social), psychological and information privacy. We discuss these areas briefly to make clear the distinguishing features between them.

Physical privacy as defined by Burgoon, is freedom from surveillance and unwanted intrusion upon personal space by the physical presence, touch, sights, sounds, or odours of others. The clear examples from this need are the personal areas surrounding people and territorial behavior, like fencing in the forecourt. The basis of this need is seen to be biological, as the same behaviour occurs also on animals. Typically, in the circumstances producing physical privacy there is spatial, physical or temporal buffer reducing the amount of sensory stimulation.

Interactional privacy is experienced by an individual or a group, when they can control who, what, when and where of encounters with others, and are therefore able to achieve a manageable number of social relationships (Burgoon, 1989). An effort to reach interactional privacy is aimed to satisfy the needs for security and intimacy, while avoiding unwanted conversations or involvements.

Psychological privacy protects an individual from intrusions upon person's thoughts, feelings, attitudes and values. In other words it is a condition where you can introspect, assimilate, plan and analyse without interference from others. It also contains freedom from persuasive pressures, intentional or unintentional, insults, and other forms of cognitive or affective interference. A crude example of violation of psychological privacy could be harassment in the workplace. To reach some level of psychological privacy, an individual can conceal her faults by controlling the depth of her self-disclosures. Thus, the means people use to achieve psychological privacy overlap

significantly with the means used to achieve the last dimension of privacy by Burgoon, information privacy.

Information privacy is the ability to control, who gathers information about oneself or one's group and under what circumstances. Burgoon used the term 'information privacy' to refer to the information collected into formal databases, which were, therefore, governed partly by law. However, in our analysis the term information privacy is used to refer to any personal information regardless of the receiver of the information. It is easy to see that this form of privacy is very close to psychological privacy, especially when controlling the spread of the kind of information that could be used to cause emotional discomfort. Furthermore, Burgoon (1989) found out in his study that people were really handling the invasions of psychological and information privacy as similar offences. Therefore, we see that the broad use of the term information privacy is justified in this paper.

Now when we have briefly discussed these four areas of privacy by Burgoon, a very significant difference between the first two and the last two dimensions must be pointed out. If we think of the regulation of privacy in temporal dimension, the individual has a different control over her physical and interactional privacy than over her psychological and informational privacy. The difference is the possibility to both open and close the personal area from other people. After reducing the area of her personal space i.e. letting someone enter very close to her, the regulating individual can decide to back away as she pleases. The same thing can be done with interactional privacy: talking to someone does not make it impossible to never talk to that person again. When related to the issue of control discussed before, we see that the individual maintains the control over personal physical and social areas.

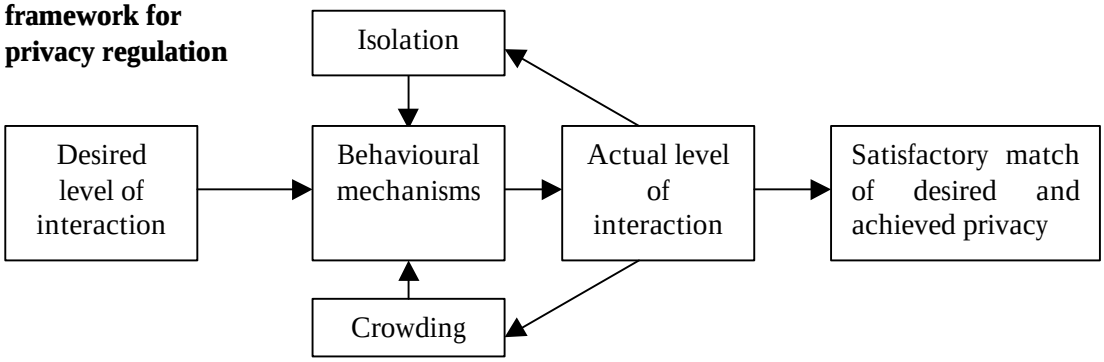
However, in the case of psychological or informational privacy this is not the case. Once leaked, a piece of information can not be retained under the control of its originator any more. This means that an individual regulating her information privacy has only the options to give or not to give some piece of information. She has no way of taking back the piece of information once disclosed. This makes the regulation of information privacy different from other forms of privacy and creates the possibility to make irreversible mistakes. This feature is of relevance when we later discuss the privacy mechanisms used to reach a desired level of information privacy.

The Functions of Privacy

The essential element of privacy, control over personal boundaries, and the different dimensions of that boundary have been discussed so far. It is, however, unclear what do we need this kind of boundary regulation for.

Sidney Jourard (1966) refers to the experiences of psychotherapists when he states that the ability to have privacy promotes "physical health and psychological and spiritual well-being". This is the result of being free to "utter, express and act" in different ways and not being obligated to fear external sanctions because of them. Newell (1994) expresses this same idea in her systems model of privacy. In the model, an individual is conceptualised as a stationary open system. The function of privacy is to provide protection for the system maintenance and development i.e. providing e.g. the cognitive and emotional relief for the individual by protecting her from potential external threats. Also Kelvin (in Altman, 1975) argued that privacy regulation is a mean of regulating our vulnerability and that privacy is a condition of independence from the influence and powers of others. In his reasoning, our ability to control the interaction and to achieve the desired states of privacy decreases the powers others have on us and therefore leave us less vulnerable.

Figure 1: Altman's framework for privacy regulation



Pedersen (1995) investigated further the functions of privacy regulation and found several functions fitting to the groups of system maintenance and system development proposed by Newell (1994). However, he also studied what functions the different types of privacy (e.g. solitude and reserve) serve. Without going any deeper into his findings it can be pointed out that the functions of reserve, the most interesting area from the information privacy's point of view, were recovery, autonomy and concealment. Also an item "protecting oneself from what others might say" appeared as a separate factor in the analysis. Pedersen bundled it together with the recovery factor, but from our perspective it is interesting as a separate factor and fits well together with Jourard's notion about the protection from external sanctions by privacy as well as Newell's notions of system protection. Furthermore, Kelvin's definition of privacy regulation as a control over the powers that others have on us, i.e. our vulnerability, is supported by the autonomy enhancing function of reserve. Thus we can conclude that the main function of privacy is the *protection* of individuals psychological well being and stability.

Privacy Behaviours

From the discussion so far, the fundamental elements of information privacy regulation are beginning to emerge, as we have discussed the central role of control to the sense of privacy, the differences between the different dimensions of privacy, and the protective function of privacy. However, an important part defining the efficiency of the privacy regulation, the means to exercise the regulatory control, has not been studied yet.

Irwin Altman has presented an influential overall framework of privacy regulation (1975) connecting the separate fields of crowding, personal space and privacy research (figure 1). He presented that an individual or a group develops momentary desires for certain levels of input and output to and from others, and that this level of *desired interaction* is subject to change as the situations and interpersonal relationships change. Furthermore, he presented that the regulation of interpersonal privacy is an optimisation process between desired and *achieved privacy*. Too much privacy is called isolation and too little privacy crowding. In our analysis we will use the term invasion of privacy instead of crowding. Also, Altman's isolation should not be confused with the privacy type called isolation by Pedersen. Pedersen's isolation is a voluntarily selected condition, but Altman's isolation is an involuntary, aversive state as much as the invasion of privacy.

From our point of view, the most interesting part of Altman's model is the conceptualisation of behavioural mechanisms to achieve the desired level of privacy. In his analysis, Altman separates four different groups of privacy

mechanisms: verbal, nonverbal, environmental and cultural mechanisms. Harris (1996) adds two mechanisms: cognitive and temporal privacy regulation mechanisms. It is important to note that these mechanisms are used not only to decrease but also to increase the level of interaction and are used in combinations to reach the desired level of interaction.

Verbal privacy mechanisms include the verbal content, structural aspects of verbal communication, amount and intimacy of verbal output, and immediacy in verbal communications. Content refers to 'what' is said, for example "keep out", "come on in" or "I'd like to be alone". Structural aspects involve for example pronunciation, dialect, voice quality, and vocabulary selection. Amount and intimacy of one's verbalisations influence also the communicating partner's level of intimacy in communication and is called reciprocity or dyadic effect (e.g. Jourard, 1966). Finally, immediacy, i.e. intense and direct personal references, communicates closeness or desire for some level of closeness with another person.

Nonverbal privacy behavior involves the use of various parts of the body for communication. Especially, the facial expressions are very important in communicating our attitudes and feelings to others.

Environmental privacy mechanisms are different uses of physical environment to regulate privacy. For example, the accepted size of the personal area in a communication setting communicates the level of intimacy in the situation, and the adjustment of the distance from the other person is a signal of either willingness to increase or decrease the level or depth of the interaction.

Cognitive mechanisms mean different ways of regulating the level of interaction by moving the focus of attention. Ignoring a person is a form of cognitive privacy regulation.

Temporal mechanisms refer to actions the purpose of which is to arrange privacy at a given moment. An example would be a plan to go walk the dog when an undesired person is about to come for a visit.

Finally, the group of culturally based privacy mechanisms overlaps with all the five groups presented above. It is easy to find several cultural norms and customs of the western culture that have the function of facilitating the regulation of personal boundaries. For example, the function of a closed door is not only to keep noise out, but also to signal the willingness to limit the level of interaction with others. Other people also notice the message, rarely bursting in without knocking.

Determinants of the Desired Level of Privacy

There is a major limitation in Altman's framework presented in the previous section. Altman states that the desired level of interactions is a result of balancing between forces to be open and forces to avoid interaction. The strengths of these forces change over time and result in a change in the desired level of interaction. However, the questions of what these forces are, and why they are changing, are not really covered in Altman's analysis. In this section, the three major factors affecting the choice over a desired level of privacy are discussed. They are interpersonal trust, potential harm caused by the disclosure, and the reward gained by disclosing.

Trust

Sidney Jourard (1966), again drawing from his experience as a therapist, states that the most powerful determinator of the variance in self-disclosure is the identity of the person to whom one discloses herself. More specifically, when the other person is perceived trustworthy, the disclosure is most likely. This same observation has been repeated in numerous empirical

studies (e.g. Wheeless, 1977; Boon, 1999; Charbonneay, 1999; Pistole, 1993; Steel, 1991; Corcoran, 1989). However, as Adams & Sasse point out (1999), the effect of trust to the disclosure of personal information has not been studied in the context of electronic communication.

Potential Harm

As we have presented that the function of privacy is to control our vulnerability, it seems reasonable to assume that the potential harm associated with the information is a major factor affecting individuals willingness to reveal a piece of information. That's because the control of external risk can be considered equal to the control of person's vulnerability and potential harm is one factor affecting people's perceptions of risks (see e.g. Gartner, 1989 or Holtgrave, 1993). However, there seems to be very little research on the effects of the potential harm of the disclosure to the willingness to disclose. Kline proposed that the potential harm can be an undesirable effect of the disclosure to the discloser, the recepient of the disclosure, or both (Kline, 1987). In general, the personal information valued positively by the revealer is associated with smaller risk (Nelson, 1976).

The perceived risk associated with a disclosure is a function of potential harm and the relationship with the recipient (Kline, 1987). The nature of the relationship between these two concepts, potential harms and trust, is clear when we study the definition of trust by Rousseau et. al. (1998): "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another". In other words, trust is a belief that the other party would not harm us even if it could.

Now, the level of trust can be used to estimate the probability of the misuse of the given information, and, together with the potential harm they can be used to estimate the expected harm caused by the disclosure.

Reward

Till this point we have only discussed the reasons not to give personal information to anyone. However, people are constantly sharing also very intimate information about themselves. It seems obvious that some kind of rewards can counter-balance the increase in vulnerability associated with a disclosure.

The forms of these rewards can be diverse from getting help from a therapist (Jourard, 1966) to getting financial benefits using a company discount card. Foddy (1984) proposed that at least the needs to get feedback about one's opinions, to compare one's views with others, to set up an exchange relationships for mutual benefit and to meet a physical and/or psychological minimum level of stimulation could make individuals seek interaction. A common reason to reveal personal information is to increase the intimacy and the sense of trust in a relationship (Prager, 1995). The reward can influence the acceptability of some actual level or privacy even after it has been established. In a study by Fusilier and Hoyer (in Tolschinsky et. al., 1981) a positive outcome of the disclosure (a job offer) prevented the sense of privacy invasion.

However, as the reward is rewarding only after it has been interpreted as such, almost anything can function as a facilitating factor for disclosure. Also, we have no evidence for defining the types of rewards that can be used to balance a condition of vulnerability. Therefore, we must just note that there is a wide variety of different relevant rewards that should be studied.

Conclusions of the Regulation of Information Privacy

We have now discussed all the central elements of privacy regulation in general. We pointed out the essential significance of the control to the sense of privacy and discussed the protective function of privacy. The different areas of privacy were presented, and the unique nature of information privacy regulation was discussed. Then, the different types of mechanisms used to reach the desired level of privacy were presented and finally the research of the factors affecting the desired level of privacy was explored.

The theoretical work presented in the previous sections is concluded here by applying the gathered knowledge to the information privacy regulation. The elements of information privacy regulation are presented in figure 2.

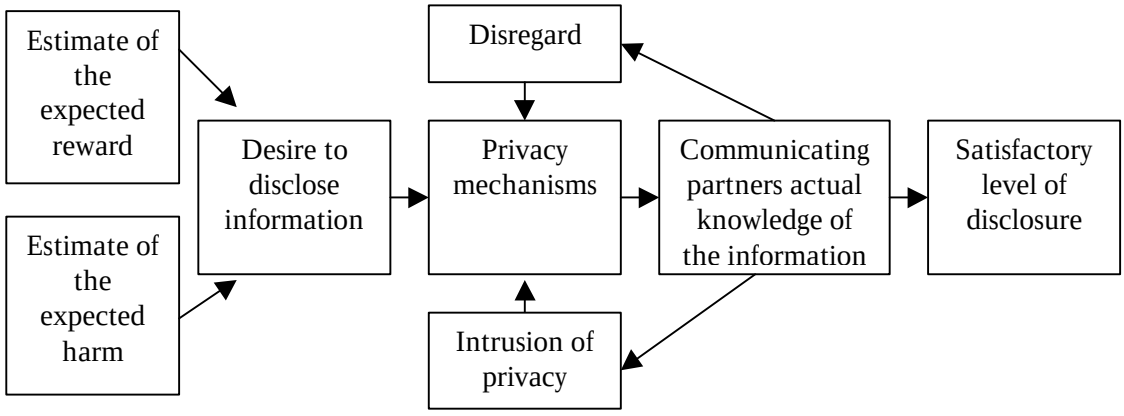
The starting point is a situation where a person or a group has a desired level of privacy (Altman, 1975). In the figure 2 that is the desire to disclose given information, maybe consisting of several different pieces of information. The factors affecting the conception of the adequate disclosure are the estimated rewards and expected harms caused by the disclosure. At least the trustworthiness of the recipient and the potential harms associated to the misuse of the disclosed information have an effect on the decision making process. The adequate rewards vary from one person and situation to another.

After deciding about the pursued level of disclosure, the different privacy regulation mechanisms are used to reach that goal. In fact, most of the mechanisms presented earlier (verbal, nonverbal, environmental, cognitive, cultural, and temporal) could be used here. However, how to use them depends on the specific features of the communication situation. When communicating by phone or on the Internet, the selection of effective privacy behaviors is limited, because of the absence of visual input and output.

The third part of the process is to monitor and evaluate the cap between the desired and achieved privacy. If satisfactory balance is not reached the person can try using a different set of privacy behaviors. If the behaviors available turn out to be ineffective, the condition of disregard (less than desired amount of information revealed) or invasion of privacy (more than desired amount of information revealed) takes place.

As discussed above, there seems to be three important points to consider, when the ability to control one's informational

Figure 2: Regulation of Information Privacy



privacy is considered. They are the choice of the desired level of interaction, the availability of effective privacy mechanisms, and the ability to monitor and evaluate the relationship between the desired and achieved level of information reveal in a given situation. It should be stressed that to be able to regulate one's privacy, one must have control over all these three elements. A failure to exercise control in any of these phases makes real control of one's privacy impossible.

Criteria for a Privacy Supporting System

In the previous section, the three central elements of information privacy regulatory control were established: 1) choice of desired level of disclosure, 2) availability of effective regulatory mechanisms, and 3) ability to monitor and evaluate the difference between the desired and achieved levels of privacy.

In this section a set of criteria is proposed on the basis of this analysis. The theoretical foundations of each criterion are presented, along with the discussion of the current state and possibilities of Internet services in relation with the criterion.

Choice of the desired level of disclosure

A starting point to the regulation of privacy is establishing a desired level of privacy. To support this decision-making, the system should provide all relevant information that is used in determining the desired privacy level.

In the previous sections, we formulated two major factors affecting the decision of the information reveal. They were the expected harms and expected rewards from the disclosure. The expected harm was further divided into the elements of potential harm and probability of the harm realization estimated by trust. The decision is made by balancing these two factors. Therefore, the benefits of the information disclosure should be clearly presented *together* with the potential harm that the misuse of the information could cause. Of course, this information should also be *reliable*. Providing the information needed to balance the pros and cons of disclosure form the criteria 1 and 2:

Criterion 1: The potential harms caused by the misuse of the disclosed information should be reliably communicated

Criterion 2: The benefits of the disclosure should be reliably communicated

If we consider the kind of information submitted to the web stores today, it is neither reasonable nor possible to map the potential misuses of all that personal data. However, the most obvious dangers (e.g. the misuse of credit card number) should be explained in detail and a more general description of the possible uses of demographic data should also be provided in straight connection with the information about the offered rewards. The information provider could be an independent third party making the information a bit more reliable.

The desired level of interaction changes as a function of situational and personal factors. Therefore, to provide the user the same level of control as when regulating her physical privacy, it should be possible to regulate the level of intimacy in the communication in both directions at any time. Especially, as the experiences of the communicating partner affect the level of trust, the once desired level of communication may very easily become totally undesirable.

Criterion 3: The customer should be able to change the level of interaction whenever she wants to.

As discussed in the next subsection, the fulfillment of the criterion 3 is quite problematic, especially if the level of disclosure should be decreased.

Availability and selection of effective privacy mechanisms

After the user has established a level of desired disclosure, she uses various opening or closing mechanisms to reach the desired level of interaction. In other words, she communicates, what level of intimacy she is ready to accept in further communication. In an effective privacy supporting system, the user should be able to communicate her desire for some level of disclosure. If this choice affects the reward offered, the process should continue from there on as a cyclic negotiation.

Criterion 4: The system should provide the user an opportunity to negotiate the depth of the disclosure

However, as stated before, information privacy differs from physical and interactional privacy in a fundamental way, because the regulation of privacy can be done in one direction only: to make the public area larger. Of course, we can conceal the information again to prevent future leaks, but we have no effective privacy behaviours to get the information back, to undisclose it. In fact, the implementation of the criteria 3 and 4 would very likely require the use of trusted third parties that could enable the user to grant the right to use the information without revealing the information itself.

When this criterion is reflected against the current situation of the Internet, we see that the negotiation opportunities provided by the service providers are quite limited. The user has very often three options: to leave, to lie, or to give all required information. Leaving from the situation, a really effective mechanism, provides a rough way to regulate the level of interaction. However, this binary choice regulation can hardly be called a real negotiation. Therefore, it is very likely that the user is forced to accept an undesirable level of disclosure or to lie, instead of leaving. Lying enables the user to make more fine-tuned choices. It can be argued, however, that if using a system effectively requires lying, the system is not really supporting human privacy regulation mechanisms i.e. giving the user enough control over the level of disclosure. False information is also a severe problem to the service provider.

The registration forms containing some voluntary items are the first minor steps towards a system that could fulfill the criterion 4. However, most sites do not offer any additional benefits as a reward from the disclosure.

Ability to monitor and evaluate the state of informational privacy in comparison to the desired state

After selecting the desired level of privacy and using some set of behaviours to reach that level, the user should be able to estimate the match between the desired and actual levels of privacy. After the evaluation is done, she is able to define the further use of privacy mechanisms. In the field of information privacy, this means that the user should be able to know for sure what kind of information the service provider knows about her.

Criterion 5: The user should have the ability to monitor the level of knowledge the other parties have about her

It is easy to see the magnitude of this requirement. How well we really know, how much and what kind of information even our friends have about us. How could we possibly ever find out? In our daily life we have to get along with estimates, so how could this condition be any better in the information networks?

However, when dealing with a single business unit or institution, the collected data is, or at least should be, possible to be explored. It should be totally possible to tell the user what kind of information there is about her in the database. It is also the legal responsibility of the parties maintaining a customer record in many countries. However, we must still believe

in promises to get all the information concerning ourselves. If the service provider acquires the information without our knowledge for example through fusion or use of cookies, we do not notice if this information is not reported to us.

Future research

The theories presented in this paper were developed earlier in the field of privacy regulation and self-disclosure. Here they were used to form a set of criteria to be used to evaluate different privacy critical systems. However, it should be noted that these theories have been developed from the research body concerning verbal disclosure as a part of synchronous communication cycle. There is surprisingly little empirical research of the elements of the privacy regulation on the field of computer mediated communication. Therefore, most of the observations lack empirical validation in the field of asynchronous computer mediated communication. Postal order business, the antecedent for the current Internet retail, could be a good place to start. We know far too little about the effects that for example trust and offered rewards have on privacy related decision by the users of Internet.

Issues of trust in the electronic environment have been a topic for research lately (see e.g. Karvonen, 1999). However, the role of trust as a mediating factor of privacy regulation has not been studied. Therefore, it would be valuable to validate the results of how trust affects the desired level of privacy in this new environment. It is also known that in the person to person relationships the intimacy of mutual disclosures increases as the trust in the relationship grows. Therefore, the development of privacy regulation as a function of time would be an interesting topic of study, as well as the development of the accepted level of disclosure in long partner relationships between customers and merchants.

In the analysis of the current research, the nature of the rewards affecting the desired level of privacy was left open. It is true that many kind of consequences of information disclosure can be perceived to be rewarding. However, in the current style of marketing, the financial benefits are the main rewards offered by data collectors. Therefore, it would be interesting to explore the potential of money as a reward. Is there some limit of its power as a facilitator of information disclosure? It is also unclear, if the subjective rewarding power of money follows a linear function. Also, if we widen the discussion beyond the risks concerning only privacy regulation, it should be explored what kind of risks can be balanced with money and how the amount of risk is translated into some monetary value. And, finally, there is a question of how much money can be offered for a piece of information without the information revealer becoming suspicious about the aims of the inquirer.

In our study a set of criteria for privacy supporting system was established. Now, this set of criteria should be tested by presenting different systems e.g. different web stores to a group of customers, and to study if these factors are of any relevance to the everyday experience of a shop user. The relevant questions include, what parts of the criteria are the most important ones, and, if there emerges any new relevant features enhancing the sense of control over one's privacy.

Finally, is it possible to build a system that would fulfil all requirements of this set of criteria? What kind of sacrifices of e.g. efficiency of the system or easiness of use should be made? Right now it seems that the construction of such systems would not be possible without extensive use of trusted third or even fourth parties. Here we come to the central question: what price the users are willing to pay for an increased control over their privacy? Would you buy a cheap and useful telescreen?

Conclusions

In this paper, the most central elements of privacy regulation were discussed to find out the central points to stress when evaluating the achieved privacy in a given system. From the review of literature four central themes were drawn: the nature of control, the protective function of privacy, the determinants of a desired level of privacy and the means used to reach that level.

The control over the level of interaction was defined as the most fundamental feature of privacy. Control consisted of three separate abilities including the ability to choose a desired level of interaction in a given situation, but also the availability of effective means to enforce that level and to monitor the achieved level of privacy.

The function of privacy was defined to be the protection of system maintenance and development. This means the protection of external threat to the psychological as well as physical well-being of a person.

To be able to control one's privacy, the first step is to define a desired level of privacy. We discussed three factors affecting the decision-making over that level. They were interpersonal trust, the potential harm caused by the disclosure and the estimated reward for a given level of disclosure.

Table 1: Criteria for Privacy Supporting System

1. *The potential harms caused by the misuse of the disclosed information should be clearly communicated*
2. *The benefits of the disclosure should be clearly communicated*
3. *The customer should be able to change the level of interaction whenever she wants to.*
4. *The system should provide the user an opportunity to negotiate the depth of the disclosure*
5. *The user should have the ability to monitor the level of knowledge the other parties have about her*

When an individual has selected a desired level of privacy she must possess the means to enforce that level. We discussed the roles of verbal, nonverbal, environmental and cultural control in this process.

Finally, the established model was used to point the musts of effective information privacy control. A set of criteria for a privacy supporting system was presented (table 1) and its applicability and implications for current web commerce were discussed.

References

Adams, A. & Sasse, A. (1999). Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, of Let Them Lie? *Proceedings of Human-Computer Interaction INTERACT '99*, IOS Press.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding.* Monterey, CA: Brooks/Cole.

Boon, S.D. (1999). Exploring the Links between Interpersonal Trust and the Reasons Underlying Gay and Bisexual Males' Disclosure of Their Sexual Orientation to Their Mothers. *Journal of Homosexuality*, 37, 45-68.

Burgoon, J.K., Parrot, R., Le Poire, B.A., Kelley, D.L., Walther, J.B. & Perry, D. (1989). Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, 6, 31-158.

Brewer, M.B. & Mittelman, J. (1980). Effects of Normative Control of Self-

disclosure on Reciprocity. *Journal of Personality*, 48, 89-102.

BW/Harris Poll: Online Insecurity by Businesweek. (1998, March 16) Retrieved July 26, 2000 from http://www.businessweek.com/1998/11/b356107.htm

Charbonneau, A., Maheux, B. (1999). Do People with AIDS disclose their HIV Positivity to Dentists. *AIDS-Care*, 11, 61-70.

Corcoran, K.J. (1988). The Relationship of Interpersonal Trust to Self-Disclosure when Confidentiality Is Assured. *Journal of Psychology*, 122, 193-195.

Foddy, W.H. (1984). A Critical Evaluation of Altman's Definition of Privacy as a Dialectic Process. *Journal for the Theory of Social Behavior*, 4, 297-307.

Gartner, G.T., Gould, L.C. (1989). Public Perception of the Risks and Benefits of Technology. *Risk Analysis*, 9(2), 225-242.

Harris, P.B., Brown, B.B. & Werner, C.M. (1996). Privacy Regulation and Place Attachment: Predicting Attachments to a Student Family Housing Facility. *Journal of Environmental Psychology*, 16, 287-301.

Holtgrave, D.R., Weber, E.U.(1993). Dimensions of Risk Perception for Financial and Health Risks. *Risk Analysis*, 13(5), 553-558.

Jourard, S.M. (1966). Some Psychological Aspects of Privacy. *Law and Contemporary Problems*, 31, 307-318.

Karvonen, K. (1999). Creating Trust, *Proceedings of the fourth Nordic Workshop on Secure IT systems (Nordsec'99), November 1-2, 1999, Kista, Sweden.*

Kline, W.B. (1986). The Risks of Client Disclosure. *American Mental Health Counselors Association Journal*, 8, 94-99.

Nelson, J. R., Strong, S.R. (1976). Rules, Risk and Self-Disclosure. *British Journal of Guidance and Councelling*. 4, 202-211.

Newell, P.B. (1994). A Systems Model of Privacy. *Journal of Environmental Psychology*, 14, 65-78.

Newell, P.B. (1995). Perspectives on Privacy. *Journal of Environmental Psychology*, 15, 87-104.

Pistole, M.C. (1993). Attachment Relationships: Self-Disclosure and Trust. *Journal of Mental Health Councelling*, 15, 94-106.

Pedersen, D.M. (1979). Dimensions of Privacy. *Perceptual and Motor Skills*, 48, 1291-1297.

Pedersen, D.M. (1997). Psychological Functions of Privacy. *Journal of Environmental Psychology*, 17, 147-156.

Prager, K.J. (1995). *The Psychology of Intimacy*. New York, NY: The Guilford Press.

Rousseau, D.M., Sitkin, S.B, Burt, R.S. & Camerer, C. (1998). Not So Different After All. A Cross-discipline View of Trust. *Academy of Management Review*, 23, 393-404.

Steel, J.L. (1991). Interpersonal Correlates of Trust and Self-Disclosure. *Psychological Reports*, 68, 1319-1320.

Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W. & Fromkin, H.L. (1981). Employee Perception of Invasion of Privacy: A Field Simulation Experiment. *Journal of Applied Psychology*, 66, 308-313.

Wheeles, L.R., Grotz, J. (1977). The Measurement of trust and its Relationship to Self-Disclosure. *Human Communication Research*, 3, 250-257.

Westin, A. (1970). *Privacy and Freedom*. New York: Atheneum.