Informed Consent to Address Trust, Control, and Privacy Concerns in User Profiling

Thea van der Geest, Willem Pieterson, and Peter de Vries

University of Twente, Faculty of Behavioural Sciences, Department of Communication Studies. P.O. Box, 217, 7500 AE Enschede, The Netherlands
t.m.vandergeest@utwente.nl

Abstract. More and more, services and products are being personalised or tailored, based on user-related data stored in so called user profiles or user models. Although user profiling offers great benefits for both organisations and users, there are several psychological factors hindering the potential success of user profiling. The most important factors are trust, control and privacy concerns. This paper presents informed consent as a means to address the hurdles trust, control, and privacy concerns pose to user profiling

1 Introduction

On May 24 2005, personalisation was the prime topic in the newspaper headlines and the radio and TV news in The Netherlands. On that day, the Dutch Minister responsible for government reform informed the Parliament about a study of the administrative hurdles that local and national administrations create for the average citizen. The study showed that the collective Dutch citizens spend 112 million hours to meet administrative and bureaucratic demands, filling out forms and making regulations work for them. The number one annoyance of citizens is that they have to fill out forms with personal data that they have provided over and again. The Minister announced his objective of reducing the administrative burden by 25 %, particularly by investing in electronic, personalised communication, services and transactions. In the next few years, the Dutch citizens will increasingly be presented with forms that are pre-filled with all personal data available, to be accessed through a citizen's personal portal. Various government departments, such as the Tax and Welfare agencies, are already working on the realisation of personalised forms, transactions and portals. Their experience shows that there is more at stake than just technical and organisational issues. How can organisations like government agencies re-use personal data in a way that is acceptable for the average citizen? This paper relates acceptance of the use of personal data in electronic communication and services to the underlying personal psychological factors of trust, control and privacy concerns.

The rise of ICT and the Internet since the 90's of the past century has led to new possibilities for the purchase or acquisition of services or products. People no longer have to visit shops or counters to get information, communicate or perform

transactions. But the new technologies have more possible benefits. Personalisation (also indicated as customisation, or tailoring) is one of those benefits. Organisations can collect data about their clients and use it intelligently for the planning and adaptation of messages, information or actions with or for the individual. In that case, the organisations use the data about current user characteristics or behaviour to adapt information and communication to the targeted individual and to predict future behaviour. Well known commercial examples of online personalisation are portals like My Yahoo (yahoo.com) or recommender systems like the online bookseller Amazon (amazon.com) has created.

Re-use of data collected or provided on earlier occasions can strengthen the relationship between user and organisation and increase the effectiveness and efficiency of communication both for the user and the organisation. A good user-experience during the contact will lead to (more) satisfaction about the application used, e.g. e-commerce or e-services, and more importantly, to a (more) positive image of the organisation behind the application [1].

In order to make 'intelligent' use of user-related information, that is, to personalise products and services an organisation needs to build a profile or user model of its customers or citizens. We define a user profile as follows:

A user profile is a (structured) data record, containing user-related information including identifiers, characteristics, abilities, needs and interests, preferences, traits and previous behaviour in contexts that are relevant to predicting and influencing future behaviour [38].

Some categories of user-related information concern stable, unalterable 'properties' of the user, such as name, age and gender. Other categories relate to properties that can easily alter over time (e.g. developing new preferences or abilities) and context (e.g. having a need for information during international travel, but not during national travel).

A number of social and psychological factors, however, reduce the acceptability of user profiling. A majority of users expresses privacy concerns about the use of personal data on the Internet, as will be discussed further on in this paper. This leads, for example, to websites like www.bugmenot.com were you can obtain a login name and password to various websites (like nytimes.com) without having to register. The sense of control of about one's own user profile is another important factor. Organisations sometimes collect and distribute data about individuals without the users knowing and wanting this. As Alpert et al. [3] show, users want to be in control. A third major factor influencing acceptance is trust. In order for user profiling to be successful, users have to trust user profiling.

Many organisations have tried to deal with trust, control and privacy issues. For example, websites try to take away privacy concerns by means of a privacy statement or seal. Other organisations offer users the possibility to control their own user profile, in line with the EU directive on the protection of personal data [16]. This paper discusses the concept of informed consent, mentioned in the directive, as a strategy to address trust, control, and privacy concerns in user profiling.

In the remainder of this paper, trust, control and privacy will be discussed more thoroughly, and then informed consent will be presented and discussed in detail.

2 Trust

The first of the psychological aspects influencing the acceptance of user profiling is Trust. A number of theorists have proposed trust to be a mechanism that enables people to deal with situations of uncertainty or risk. Luhmann [26], for instance, argued that trust effectively limits the number of possible behavioural outcomes associated with dealing with other people to only a relatively small number of expectations. Limiting the investigation of all possible outcomes of an interaction to only a few, may result in more careful investigation of the realistic option, which may reduce both uncertainty and risk of the actor. In a similar vein, Anthony Giddens [21] used the term trust for situations where knowledge about the other party, i.e., the trustee or referent, is absent.

In light of the above it is not surprising that trust is generally accepted as a prerequisite for good personalisation practice [6]. Users are not likely to reveal confidential information about themselves and may be suspicious of data harvesting practices if they fear that this information could be misused in some way, and that they, consequently, put themselves at risk by doing so. Research [23] demonstrated that lack of trust was the major reason for people not to engage in online shopping. In addition, Warkentin, Gefen, Pavlou, and Rose [40], found that trust in the organisation using the technology and trust in governmental policies are important determinants for the adoption of e-services. They state that trust is a crucial enabler affecting purchase intentions, inquiry intentions and the intention to share personal information. The latter intention, of course, is especially relevant in user profiling. Briggs et al. [6] point to the fact that trust and personalisation have a reciprocal relationship. Trust is not only a prerequisite for good personalisation, good personalisation also generates trust.

Trust, however, is not a unitary concept. It has been studied in various disciplines, ranging from economics and political sciences to personality research and social psychology, each of which may treat the concept differently with regard to whether trust is seen as a dependent, independent or interaction variable, whether it is static or dynamic, or whether it is studied on the institutional, group or individual level (for an overview see [5], [15], [31]). The next paragraphs discuss various forms of trust.

The concept of *general trust*, or generalised interpersonal trust, for instance, relates to the trust people have in most other people, or in strangers, and is treated as a stable characteristic of both individuals and groups [15]. As such, general trust can be seen as a necessary prerequisite for other forms of trust to develop; without a general sense of trust, a user would not be willing to enter interactions of any kind.

Contrary to general trust, *social trust* is based on social relations and shared values. The actors at which this type of trust is directed are more concrete than with general trust; specifically, they are persons or organisations that are perceived to share the trustor's values [33]. Social trust, a focus of attention in risk management research,

involves little or no interaction, and is often a 'one-shot' affair [15]. Value similarity may be inferred after shooting only a quick glance at the trustee; simple cues, such as skin colour or gender may be enough for the trustor to infer that if the trustee looks similar, he or she may also hold similar values. If user profiling is aimed at establishing social trust, the profile should contain information about the relevant values that the profiled person holds about social issues, persons and organisations.

Interpersonal trust is established and maintained in and through interaction and communication. It is a kind of trust much studied in social psychology where it is treated as an expectation of the other's behaviour that is specific to the interaction [10]. This expectation is argued by some to be based on perceptions of the other's competence and honesty [29] or goodwill [41]. If a user profile contained the information on the basis of which interpersonal trust can be predicted, it should be fed with information about the interactions occurring between the organisation and the user. This means that the user profile needs to be updated continuously.

Different labels for and distinctions between types of trust are found in the literature of the different fields. However, most are analogous to the typology described above. Zucker [43], for instance, used the term *characteristic trust* to denote trust based on social relations, comparable with Earle et al.'s [15] concept of social trust. In addition, Rotter [30] distinguished between *dispositional* and *relational trust*, the former relating to others in general, the latter based on interaction with a particular other. *Propensity to trust*, proposed by Mayer, Davis and Schoorman [28] as a stable characteristic affecting the likelihood that someone will trust, may be thought of as a general willingness to trust others, and as such, it bears a strong resemblance to general trust.

Online interaction with an organisation involves both the organisation itself, as well as a system which enables this interaction. Obtaining tax refunds online, for instance, involves the tax agency as the organisation that enables and controls online interactions, as well as several interfaces that enable clients to submit information about their income and deductible expenses electronically. *Organisational trust* and *system trust* are, therefore, of particular importance to the implementation and acceptance of user profiling. The former is a type of trust that partly overlaps the categories of social and interpersonal trust: it has an organisation or group as its referent, as does social trust, and at the same time is based on interactions, as is typical of interpersonal trust (e.g., see Zaheer, McEvily and Perrone [42]. The latter, system trust can be seen as a special case of interpersonal trust. Like interpersonal trust it refers to expectations about behaviour of a specific other, rather than a group of others or strangers. In the case of system trust, however, the referent is not a human partner, but rather an object, i.e. the system with which a user is in interaction.

In sum, acceptance of user profiling is influenced by the user's trust propensity in general, trust in the organisation he or she is dealing with, and trust in the systems the organisation uses to interact and communicate with the user, including the user profiling system.

Trust is related to many other issues that appear to be critical for user profiling. Firstly, trust is influenced by the *sense of control* about the user profile [4]. When end users feel that they themselves or a trusted third party representing them controls the user profile and its applications, they will trust user profiling more than when they

feel that the organisations in control are not primarily focusing on the users' interests, or, put differently, do not share the user's values.

Trust is also influenced by *privacy concerns*. Concern about the privacy aspects of personal information shared on the Internet is correlated with increasing levels of Internet experience [20]: the more experienced internet users are more worried about privacy issues. There is considerable resistance among many Internet users to engage in business-to-consumer transactions over the Web, primarily due to concerns about privacy and the trustworthiness of the Internet [2], [39]. Findings of Chellappa & Sin [8] also stress the relationship between trust and privacy. In an empirical study, they found that both trust and privacy factors correlate significantly with the likelihood of using personalised services. Also they found that privacy and trust were correlated. Factors building trust (like familiarity and past experiences) led to lower privacy concerns.

3 Control

Alpert et al. [3] studied user attitudes regarding the personalisation of content in e-commerce websites. In their study, the users expressed their strong desire to have full and explicit control of personal data and interaction. They want to be able to view and edit (update and maintain) their personal information at any time.

A study by Roy Morgan Research [32] shows that 59% of the 1524 Australian respondents state that their trust in the Internet increases when they feel they have control over their personal information. The study also showed that:

- 91% of the respondents want to be asked for explicit permission before companies use their information for marketing purposes;
- 89% of the respondents want to know which persons and which organisations have access to their personal information;
- 92% of the respondents want to know how their personal information is used.

User control obviously is a critical condition for user acceptance of profiling and personalisation. However, the study cited does not answer the question whether the users themselves should host the user profile themselves, nor whether trusted third parties can resolve the users' anxiety about control issues.

Byford [7] perceives personal information as a property or asset of the individual ('Byford's property view'). The user is the owner of his or her personal information. In Byford's property view, individuals see privacy as the extent to which they control their own information in all types of Internet exchanges. The property aspect of the exchange manifests itself in the users' willingness to trade personal information for valued services such as free e-mail or special discounts from merchants.

A user profiling system that is not supported by a good system for user control of personal information is bound to lead to acceptance problems. However, creating the interaction and the related user interface that allow users to control the information in their profiles is a complicated problem, especially if the control goes beyond a very course level of granularity [11]. Although users have indicated they want to be in

control of their personal data, very little users make use of possibilities websites offer to control personal information. A number of ecommerce web sites give users access to their profiles. However, it is not clear whether users are aware of this facility [11, p.69]. Reports of operators of personalisation systems have indicated that users rarely take actions to proactively customise their online information [27].

4 Privacy concerns

Violation of privacy is one of the most important concerns of Internet users. As much as 70 – 84 % of all participants in various surveys indicated that privacy concerns made them resist providing personal data. They are especially aware of privacy issues concerning personal data, such as name, addresses and income. Also, 24-34 % of people in the surveys indicated to have provided false or fictitious information, when asked to register [12], [18], because of concerns about privacy violation. In commercial contacts (on-line shopping) those privacy concerns play an even more important role than in other systems for tailoring information or communication. As much of 91 % of respondents indicated that they were concerned about businesses sharing user data for purposes other than the original purpose for collecting the data [37]. Although many Internet users are not well-informed about the means of collecting usage data (web surfing behaviour data), such as spyware and cookies, almost everybody (91%) indicates to feel uncomfortable about being tracked across websites [22].

All these figures indicate that privacy and personal data protection are of the utmost importance to almost all Internet users. However, this does not mean that they understand the implications of their concerns and act upon it. Only 10% of respondents in a survey had their browsers installed in such a way that it rejected cookies [18]. In a study of Spiekermann et al. [34] even users with self-reported strong privacy concerns readily disclosed personal and sensitive information on a web site. Although people express concern about privacy, they easily give up on privacy because of convenience, discounts and other incentives, or a lack of understanding of the consequences. Obviously there is a difference between concerns and attitudes at one hand and actual secure behaviour at the other hand.

Yet, the privacy concerns of users imply that organisations should approach the process of user profiling with extreme caution. Effective user profiling depends on the correctness of information and on the willingness of user to provide data to the organisation. Technical solutions such as good privilege regulations, and regulatory solutions like required privacy policies, could help to secure privacy and thus to reduce privacy concerns. But we assume that they will not work without accompanying measures to address the users' attitudes. Creating trust, giving users control, and requesting informed consent are essential conditions for solving the privacy issue. The organisation, as the initiator of collecting user data and user profiling, should take the initiative to protect and secure the users' privacy. Common practice of organisations is to add a privacy statement to websites and consider the problem solved. As Kobsa & Teltzrow [24] show, privacy statements are hardly read, let alone comprehended by the visitors of websites. Their research shows that the

design of privacy statements (like the user interface) might help in alleviating users' privacy concerns.

Loeb [25] distinguishes three types of privacy concerns: regarding protection of the user profiles and queries, regarding protection of the person's web usage history and regarding protection of the actual information if the delivery takes place over public networks.

Wang et al. [39] distinguish four types of privacy threats:

- improper acquisition of information (e.g. uninvited tracking of the users' web usage);
- improper use of information (e.g. distribution of data to third parties);
- privacy invasion (e.g. spamming a mailbox with uninvited direct mailings);
- improper storage and control of personal information (e.g. no opting-out, no means to remove incorrect or unwanted information)

It is still unclear which of the privacy threats and concerns mentioned are (most) influential for acceptance of user profiling. But an overview of studies regarding privacy and personalisation on the Internet does show that users have significant concerns over the use of personal information for personalisation purposes on the Internet [36]. CyberDialogue [13] found that 82% of all Internet users say that a website's privacy policy is a critical factor in their decision to purchase online. Even more salient is that 84% of the respondents have refused to provide information at a website because they were not sure how that information would be used.

The fact that there is a concern, however, does not necessarily imply that users don't provide any information. The lack of trust in privacy policies moved a large majority of users to give false or fictitious information over the Internet, and thus protect their privacy [12], [37]. According to research conducted by the Winterberry Group, this development is increasingly becoming a problem for the collection of user-related information [14]. Two aspects of data quality seem to interfere here: whether the personal data collected are an accurate, adequate and reliable representation of the user, and whether they are used in an acceptable, appropriate and allowable way.

5 An integral solution to address control, trust and privacy concerns: Informed consent

Trust, control and privacy are strongly related concepts. Paying attention solely to establishing a trustworthy relationship between users and the supplier of personalised services and products is fruitless when no attention is paid to privacy and control issues. It might well be possible that a user does trust the organisation offering personalisation, but feels his privacy is being threatened when supplying personal information and therefore does not use the personalised e-services of that organisation. For example; Chellappa and Sin [8] found that "while vendors can do little to positively influence consumers' concern for privacy directly, our analysis sheds light on the possibility for them to indirectly affecting consumers' privacy concerns through trust building". On the other hand, enabling users to exert control over their own information, may increase trust and, thus, reduce privacy concerns.

Informed consent, a mechanism that enables users to exert control, is a requirement under the EU Data Protection Directive of 1995 (95/46) and the subsequent directive 2002/58 on privacy and electronic communications.

The 1995 and 2002 directives describe consent of a user as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." The consent seems to be defined in a negative way: it offers protection from intrusion. The 2002 directive even suggests that consent can be dealt with sufficiently by ticking off a checkbox on a web site. This conception of informed consent does not create possibilities for building and managing trust, or for users who see their personal information as a commodity they want to use for identity management with interested organisations.

In the health care sector informed consent on the use and application of personal data is defined more extensively, compared to the definitions of the EU directives. Patients have the legal and ethical right to be informed about what will happen to their body, and make informed decisions about the intervention or treatment before it is started.

Informed consent is the process by which a fully informed user participates in decisions about his or her personal data. It originates from the legal and ethical right the user has to direct what happens to his or her information, and from the ethical duty of organisations using personal data to involve the user in the control, use and maintenance of these data.[1]

Sreenivasan [35] argued that informed consent in medicine consists of two parts: a duty to obtain the voluntary agreement of patients or trial participants before treatment or enrolment, and a duty to disclose adequate information to the patient or participant before seeking this agreement.

According to Friedman, Millet and Felten [19], informed consent in Web privacy policies comprises *disclosure, comprehension, voluntariness, competence,* and *agreement.*

Disclosure refers to providing accurate information about the benefits and harms that might reasonably be expected from the action under consideration. What is disclosed should address the important values, needs and interests of the individual. *Comprehension* refers to the individual's accurate interpretation of what is being disclosed. This component raises the question: What criteria must be satisfied in order to say that something has been adequately comprehended? For example: does a user understand the privacy statement? Why (not)? *Voluntariness* means that an individual only should participate voluntary, there may be no control about an individual's actions and the action may not be coerced. *Competence* refers to possessing the mental, emotional and physical capabilities needed to be capable of giving informed consent. Children, for example, might not be mentally and emotionally capable to judge whether or not to provide personal information on websites. Finally, a*greement* refers to a reasonably clear opportunity to accept or decline to participate [19]. This not only implies the opportunity to choose whether or not to participate at all, but also

[1] See: http://eduserv.hscer.washington.edu/bioethics/topics/consent.html.

to the opportunity to choose to stop or continue the participation at any time. This means, for user profiling, that the individual should have the full control at all time.

In both Sreenivasan's [35] and Friedman et. al.'s [19] work, control and information are considered central to informed consent. Accurate information about the potential benefits and harm, provided by competent sources, should aim at comprehension of that information, and, thus, pave the way for voluntary agreement with the suggested treatment of the patient (or disagreement). The same should apply to organisations operating outside the medical world, such as providers of e-services. These organisations have much to gain from implementing informed consent in their online interactions with customers. When users are informed whether personal information will be collected, and, if so, how it will be used, they can assess the chances of their information-sharing leading to unpleasant consequences of any kind, which greatly reduces their uncertainty.

As is illustrated by the examples mentioned in the above, the effect of informed consent is twofold. First, users are informed about the procedures that will be employed by the organisation they are dealing with. This, in fact, reduces the uncertainty that users may experience when engaging in online interactions, and, consequently reduces the need for high levels of trust (cf. [26], [9]). Furthermore, informed consent enables users to exert control and retain ultimate responsibility over what they feel is sensitive information. This may well cause users to think less negatively about information gathering, and, more importantly, the intentions of the organisation: by implementing informed consent, organisations may communicate that they have their users' best interests at heart, which would greatly increase user trust in the organisation (cf. *social trust*, [15], [33]).

When informed consent is perceived and realized as a process that involves users in the control of their personal data, it offers promising perspectives for an integral strategy to deal with trust, and privacy concerns, thus increasing acceptance.

Based on the experiences with informed consent in the field of medicine, we propose that the following elements should be addressed in an informed consent procedure regarding user profiling.

1. The nature of the personal data collected for the sake of user profiling.
2. The organisation's objectives with user profiling and its prospective effects for the user. This includes the sharing of data with other organisations, and their respective objectives for user profiling (cross-domain user profiling).
3. The alternatives when no data are collected, or when no user profiling is applied. Also, the alternatives when particular types of user-related information are rejected, or when particular applications of user profiling are refused.
4. Relevant risks, benefits and uncertainties related to user profiling, for the various alternatives.
5. Assessment of the user's understanding of the information.
6. Explicitly stated acceptance or declining by the user, for all or particular types of user-related information, and for all or particular applications of user profiling.

The consent must be voluntary, and the user must have the competence to understand the information and its consequences, or the right to decide on the use of one's own personal information is void. Therefore, special attention must be paid to

those groups in society that do not have easy access to ICT. Both the procedure and the information on user profiling should be explained in layperson terms. The user's understanding and acceptance must be assessed along the way, not only at initial adoption of user profiling.

Informed consent is a critical condition from the perspective of the individual user, but it might not always be in the interest of organisations to inform the public about the collection and use of user-related information. According to Business Week[2] 88% of users want sites to garner their consent when personal information is collected. According to a report from the Federal Trade Commission, 59% of websites that collect personal identifying information neither inform Internet users that they are not collecting such information nor seek the user's consent [17]. This strongly conflicts with the public's interest and is a violation of European privacy and personal information protection laws.

Informed consent requires efforts from organisations; they have to start a dialogue with their users about e.g. the control of the user profile. Organisations have to inform their users about their privacy status and the consequences of engaging in user profiling. Benefits, however, are numerous; users are well informed and are able to make proper decisions, raising levels of trust, assuring privacy and dealing with the control of the user profile. Little empirical data is available that deals with informed consent and user profiling. It is necessary to research the dimensions of informed consent. What factors determine informed consent? Do people understand consent? When do we call someone "informed"? Do people oversee the consequences of their consent? Both qualitative and quantitative research methods might be used to explore the dimensions of informed consent and the many ways in which it can be presented to the public and their effect on control and privacy concerns. Such studies can help us to assess the impact of control, trust and privacy issues on user profiling.

References

1. Accenture: Leadership in Customer Service: New Expectations, New Experiences. Accenture, (2005)
2. Aldridge, A., Whithe, M., Forcht, K.: Security considerations of doing business via the Internet: cautions to be considered. Internet Research, 7(1) (1997) 9-15
3. Alpert, S.R., Karat, J., Karat, C.-M., Brodie, C., Vergo, J.G.: User attitudes regaring a User-Adaptive eCommerce Web Site. User Modelling and User-Adapted Interaction, 13(4) (2003) 373-396
4. Araujo, I., Araujo, I.: Developing trust in Internet commerce. In: 2003 conference of the Centre for Advanced Studies on Collaborative research. Toronto, Canada, (2003)
5. Bhattacherjee, A., Devinney, T.M., Pillutla, M.M.: A formal model of trust based on outcomes. Academy of Management Reviw, 23(1998) 459-472

[2] See: http://www.businessweek.com/2000/00_12/b3673010.htm.

6. Briggs, P., Simpson, B., De Angeli, A.: Personalisation and Trust: A reciprocal Relationship? In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing Personalized user experiences in eCommerce. (2004)
7. Byford, K.S.: Privacy in Cyberspace: constructing a model of privacy for the electronic communications environment. Rutgers Computer and Technology Law Journal (24) (1998) 1-74
8. Chellappa, R.K., Sin, R.: Personalization versus Privacy: An Empirical Examination of the Online Consumers' Dilemma. Information technology and management, 6(2-3) (2005)
9. Coleman, J.S.: Foundations of social theory. Harvard University Press, Cambridge (1990)
10. Corritore, C.L., Kracher, B., Wiedenbeck, S.: Online trust; concepts, evolving themes, a model. International Journal of Human-Computer studies, 58(2003) 737-758
11. Cranor, L.F.: I Didn't buy it for myself: Privacy and ecommerce personalization. In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing Personalized user experiences in eCommerce. Kluwer Academic Publishers, Dordrecht (2004)
12. Culnan, M.J., Milne, G.R.: The Culnan-Milne survey on consumers & online privacy notices: Summary of Responses. In: Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices. Washington DC, (2001)
13. CyberDialogue: Online consumer personalization survey. The personalization consortium, Wakefield (2001)
14. Direct Marketing: Anonymous Web Browsing Threatens Profiling Practices of E-marketers. (2001)
15. Earle, T.C., Siegrist, M., Gutscher, H.: Trust and confidence: A dual-mode model of cooperation. Western Washington University, WA, USA (2002)
16. European Union: Charter of Fundamental Rights of the European Union (Article 8(1)). Nice (2000)
17. Federal Trade Commission: Privacy online: Fair information practices in the electronic marketplace. (2000)
18. Fox, S., Raine, L., Horrigan, J., Lenhart, J., Spooner, T., Carter, C.: Trust & Privacy Online: Why Americans want to rewrite the rules. The Pew Internet & American Life Project, Washington DC (2000)
19. Friedman, B., Millet, L., Felten, E.: Informed consent online: A conceptual model and design principles. UWCSE Technical Report, 00-12-2(2000)
20. George, J.F.: Influences on the Intent to make Internet purchases. Internet Research, 12(2) (2002) 165-180
21. Giddens, A.: The consequences of modernity. Stanford University Press, Stanford, CA (1990)
22. Harris Interactive: A Survey of consumer privacy attitudes and behaviors. Harris, Rockester, NY (2000)
23. Hoffman, D.L., Novak, T.P., Peralta, M.: Building consumer trust online. Communications of the ACM, 42(4) (1999) 80-85
24. Kobsa, A., Teltzrow, M.: Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data sharing and Purchase Behavior. In: Martin, D. and Serjantov, A. (eds.): Privacy Enabling Technologies, Springer Verlag Lecture Notes in Computer Science. (2004)

25. Loeb, S.: Architecting personalized delivery of multimedia information. Communications of the ACM, 35(12) (1992) 39-47
26. Luhmann, N.: Trust and Power: Two works by Niklas Luhmann. John Wiley & Sons, Chichester (1979)
27. Manber, U., Patel, A., Robinson, J.: Experience with personalization on Yahoo! Communications of the ACM, 43(8) (2000) 35-39
28. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Academy of Management Reviw, 20(1995) 709-734
29. Renn, O., Levine, D.: Credibility and trust in risk communication. In: Kasperson, R.E. and Stallen, P.J.M. (eds.): Communicating risks to the public. Kluwer, Dordrecht (1991) 175-218
30. Rotter, J.B.: Interpersonal Trust, trustworthiness, and gulibility. American Psychologist, 35(1980) 1-7
31. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: A cross discipline view of trust. Academy of Management Review, 23(1998) 393-404
32. Roy Morgan Research: Privacy and the community. (2001)
33. Siegrist, M., Cvetkovich, G.T., Gutscher, H.: Shared Values, social trust, and the perception of geographic cancer clusters. Risk Analysis, 21(2001) 1047-1053
34. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In: ACM Electronic Commerce 2001 conference. (2001) 38-47
35. Sreenivasan, G.: Does informed consent to research require comprehension. The Lancet, 362(December 13) (2003) 2016-2018
36. Teltzrow, M., Kobsa, A.: Impacts of User Privacy preferences on personalized systems: acomparative study. In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing personalized user experiences for eCommerce. Kluwer Academic Publishers, Dordrecht (2004)
37. UMR: Privacy Concerns Loom Large. Study Conducted for the Privacy Commissioner of New Zealand. (2001)
38. van der Geest, T.M., van Dijk, J.A.G.M., Pieterson, W.J. (eds.): Alter Ego: State of the art on user profiling. An overview of the most relevant organisational and behavioural aspects regarding User Profiling. Telematica Instituut, Enschede (2005)
39. Wang, H., Lee, M.K.O., Wang, C.: Consumer Privacy concerns about Internet marketing. Communications of the ACM, 41(3) (1998) 63-70
40. Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M.: Encouraging citizen adoption of e-Government by building trust. Electronic Markets, 12(3) (2002) 157-162
41. Yamagishi, T., Yamagishi, M.: Trust and commitment in the United States and Japan. Motivation and Emotion, 18(1994) 130-166
42. Zaheer, A., McEvily, B., Perrone, V.: Does trust matter? Exploring the effects of interorganizational and interpersonal trsut on performance. Organizational Science, 9(1998) 141-159
43. Zucker, L.G.: Production of trust: Institutional sources of economic structure 1840-1920. In: Staw, B.M. and Cummings, L.L. (eds.): Research in organizational behavior. JAI Press, Greenwich, C.T. (1986) 53-111