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 Behavioral 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 personalized or tailored, based on user-related data stored in so called user profiles or user models. Although user profiling offers great benefits for both organizations and users, there are several 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

Introduction

In the past, the purchase or acquisition of services or products required that individuals were in contact with many different organizations, at different times and at different locations, providing each with the data they needed. Nowadays, since many of these services are offered electronically, the actual contact between the organization and the person seeking a service or product is often realized via the individual's personal computer (be it a desktop computer or a more mobile application such as a phone or PDA). Personal communication devices act as single access point to a variety of organizations, services and products.

When organizations have collected data about the individuals they are in contact with, they can use it intelligently for the planning and adaptation of messages, information or actions with or for the individual. In that case, the organizations use the data about current user characteristics or behavior to adapt information and communication to the targeted individual and to predict future behavior. Re-use of data collected or provided on earlier occasions strengthens the relationship between user and organization. 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 organization behind the application.

In order to make 'intelligent' use of user-related information, that is, to personalize products and services an organization needs to build a profile or user model of its customers or citizens. Cremers, Lindenberg and Neerincx [1] define a so-called user profile as:

A data record describing the user with his characteristics, abilities and needs and previous interaction experiences.

Although this definition captures elements that constitute a user profiling, we believe this definition is too narrow; far more information is needed to personalize services and product. For example, a person's traits may determine whether he is interested in a product or service right now or perhaps tomorrow. Therefore, we extend the definition and define the term user profile as follows [2]:

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

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).

User profiling might have several benefits for both organizations and users. Communication processes can become more efficient and effective, organizations are able to gain insight in user's behavior and perhaps even influence this behavior. Users are no longer overwhelmed with irrelevant information and services, and products can be personalized to meet the needs of users. However, trust, control and privacy concerns may impede the development of user profiling by organizations and its acceptance by individual users.

Trust

The first of the aspects influencing the acceptance of user profiling is Trust. Trust is generally accepted as a prerequisite for good personalization practice [3]. Users are not likely to reveal confidential information about themselves to an untrustworthy party, and they may be suspicious of data harvesting practices if they feel the information may be misused in some way. Research [4] demonstrated that lack of trust was the major reason for people not to adopt online shopping. Warkentin, Gefen, Pavlou, and Rose [5] studied the role of trust in the adoption of e-services. They found that trust in the organization using the technology and trust in governmental policies are important determinants for the adoption. 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. Brigss et al. [3] point to the fact that trust and personalization have a reciprocal relationship. Trust is not only a prerequisite for good personalization, good personalization also generates trust.

Trust is related to many other issues that appear to be critical for user profiling. Firstly, trust is influenced by the *locus of control* for the user profile [6]. 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 organizations in control are not primarily focusing on the users' interests.

Trust is also influenced by *privacy concerns*, and hence by the privacy policies realized in the user profile system. Concern about the privacy aspects of personal information shared on the Internet is correlated with increasing levels of Internet experience [7]: 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 [8], [9].

Problem with trust is that, besides its strong relationship with control and privacy, it is not an unitary concept. Corritore et al. [10] state that there is "a multi-dimensional family of trust concepts, each with a unique focus". Trust plays a role within a user profiling relationship in the following ways:

- the users' trust in the organization he or she is dealing with;
- the users' trust in the services or products that the organization is providing;
- trust in the systems the organization uses to interact and communicate with the user, including the user profiling system;
- communication (messages and interaction) that establish and reinforce trust; and
- the user's trust propensity in general, a personality trait.

The concept of trust has been studied in various disciplines, ranging from economics and political sciences to personality research and social psychology. Each of these disciplines 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 [11], [12], [13]. 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 [12]. 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 organizations that are perceived to share the trustor's values [14]. Social trust, a focus of attention in risk management research, involves little or no interaction, and is often a 'one-shot' affair [12]. 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 organizations.

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 behavior that is specific to the interaction [11]. This expectation is argued by some to be based on perceptions of the other's competence and honesty [15] or goodwill [16]. 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 and communication occurring between the organization and the user. This means that the user profile needs to be updated continously.

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 [17], for instance, used the term *characteristic trust* to denote trust based on social relations, comparable with Earle et al.'s [12] concept of social trust. In addition, Rotter [18] 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 [19] 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.

Of particular importance to the implementation and acceptance of user profiling are *organizational trust* and *system trust*, as interacting with an organization online involves both the organization itself, as well as a system which enables this interaction. Obtaining tax refunds online, for instance, involves the tax agency as the organization that enables and controls online interactions, as well as several interfaces that enable clients to submit information about their income and deductable expenses electronically.

Control

Alpert et al. [20] studied user attitudes regarding the personalization 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 [21] 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 organizations have access to their personal information;
- 92% of the respondents want to know how their personal information is used.

Byford [22] 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, building a

user interface that allows users to control the information in their profiles is a complicated problem. Especially if the interface provides controls that go beyond a very course level of granularity [23, p.69]. 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 that many users are aware of this facility [23] Reports of operators of personalization systems have indicated that users rarely take actions to proactively customize their online information [24].

Privacy concerns

Violation of one's privacy is one of the most important concerns of Internet users. An overview of studies regarding privacy and personalization on the Internet shows that users have significant concerns over the use of personal information for personalization purposes on the Internet [31]. As much as 70 – 84 % of all participants in various surveys indicated that privacy concerns made them resist to provide 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 [25], [26], because of concerns about privacy violation.

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 [25], [27]. According to research conducted by the Winterberry Group, this development is increasingly becoming a problem for the collection of user relation information [33]. It also makes it apparent that many users are reluctant about user profiling.

In commercial contacts (on-line shopping) the 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 [27]. Cyber Dialogue [32] found that 82% of all Internet users say that a website's privacy policy is a critical factor in their decision to purchase online.

All these figures indicate that privacy and personal data security 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. Although many Internet users are not well-informed about the means of collecting usage data (web surfing behavior data), such as spyware and cookies, almost everybody (91%) indicates to feel uncomfortable about being tracked across websites [28]. However, only 10% of respondents in a survey had their browsers installed in such a way that it rejected cookies [26]. In a study of Spiekermann et al. [29] even users with self-reported strong privacy concerns readily disclosed personal and sensitive information on a web site. Obviously there is a difference between concerns and attitudes at one hand and actual secure behavior at the other hand.

Yet, the privacy concerns of users imply that organizations 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

organization. Technical solutions, such as good privilege regulations, could help to some extend to secure privacy and thus to reduce privacy concerns. The organization, as the initiator of collecting user data and user profiling, should take the initiative to protect and secure the users' privacy.

Loeb [30] 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. [8] 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 privacy threats and concerns are (most) influential for acceptance of user profiling. But it is clear that privacy is important for the users' acceptance of internet, and hence for acceptance of user profiling.

A solution to Address Control, Trust and Privacy Concerns: Informed Consent

The studies on trust, control and privacy concerns have shown that these issues are not straightforward and easy to deal with. For example, people express the desire to be in control, but when given this possibility, they don't use it. People express privacy concerns, but nevertheless provide all kinds of personal information to organizations they might not even trust. Trust, control and privacy are strongly related concepts. Paying attention solely to establishing a trustworthy relationship between users and the supplier of personalized 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 organization offering personalization, but feels his privacy is being threatened when supplying personal information and therefore does not use the personalized e-services of that organization. Striving to informed consent might be a strategy to deal with trust, control and privacy concerns and thus increasing acceptance.

Informed consent enables users to make informed decisions about whether they want to participate in user profiling. The term is known from the world of medicine. 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. Parallel to definitions from the health care sector, we can define informed consent on the use and application of personal data as follows:

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 organizations using personal data to involve the user in the control, use and maintenance of these data.[1]

Sreenivasan [34] states 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.

Friedman, Millet and Felten [35] state that informed consent in Web privacy policies comprises the following elements:

- Disclosure
- Comprehension
- Voluntariness
- Competence
- 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.

Agreement refers to a reasonably clear opportunity to accept or decline to participate [35]. This not only implies the opportunity to choose whether or not to participate at all, but also to the opportunity to choose to stop or continue the participation at any given time. This means, for user profiling, that the individual should have the full control at all time.

Translated in a procedure in parallel to the medical world, 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 organization's objectives with user profiling and its prospective effects for the user. This includes the sharing of data with other organizations, 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.

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

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 organizations 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 [36]. This strongly conflicts with the public's interest and might even be a violation of European privacy and personal information protection laws.

Informed consent requires efforts from organizations; they have to start a dialogue with their users about e.g. the control of the user profile. Organizations 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 help to assess control, trust and privacy issues in user profiling.

References

1. Cremers, A. H. M., J. Lindenberg, and M. A. Neerincx. Apples or Oranges: a user-centred framework for cooperative user profile management. *7th WWRF Meeting*, Eindhoven, the Netherlands, 2002.
2. van der Geest, T.M., van Dijk, J.A.G.M., and 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. Enschede: Telematica Instituut
3. Briggs, P., B. Simpson, and A. De Angeli. Personalisation and Trust: A reciprocal Relationship? In: *Designing Personalized user experiences in eCommerce*, edited by C.-M. Karat, J. O. Blom and J. Karat, 2004.
4. Hoffman, D. L., T. P. Novak, and M. Peralta. Building consumer trust online. Communications of the ACM 42: 80-85, 1999.

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

5. Warkentin, M., D. Gefen, P. A. Pavlou, and G. M. Rose. Encouraging citizen adoption of e-Government by building trust. Electronic Markets 12: 157-162, 2002.
6. Araujo, I., and I. Araujo. Developing trust in Internet commerce. *2003 conference of the Centre for Advanced Studies on Collaborative research*, Toronto, Canada, 2003.
7. George, J. F. Influences on the Intent to make Internet purchases. *Internet Research* 12: 165-180, 2002.
8. Aldridge, A., M. Whithe, and K. Forcht. Security considerations of doing business via the Internet: cautions to be considered. *Internet Research* 7: 9-15, 1997.
9. Wang, H., M. K. O. Lee, and C. Wang. Consumer Privacy concerns about Internet marketing. *Communications of the ACM* 41: 63-70, 1998.
10. Corritore, C. L., B. Kracher, and S. Wiedenbeck. Online trust; concepts, evolving themes, a model. *International Journal of Human-Computer studies* 58: 737-758, 2003.
11. Bhattacherjee, A., T. M. Devinney, and M. M. Pillutla. A formal model of trust based on outcomes. *Academy of Management Reviw* 23: 459-472, 1998.
12. Earle, T. C., M. Siegrist, and H. Gutscher. Trust and confidence: A dual-mode model of cooperation. Western Washington University, WA, USA:, 2002.
13. Rousseau, D. M., S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: A cross discipline view of trust. *Academy of Management Reviw* 23: 393-404, 1998.
14. Siegrist, M., G. T. Cvetkovich, and H. Gutscher. Shared Values, social trust, and the perception of geographic cancer clusters. *Risk Analysis* 21: 1047-1053, 2001.
15. Renn, O., and D. Levine. Credibility and trust in risk communication. In: *Communicating risks to the public*, edited by R. E. Kasperson and P. J. M. Stallen. Dordrecht: Kluwer, 1991, p. 175-218.
16. Yamagishi, T., and M. Yamagishi. Trust and commitment in the United States and Japan. *Motivation and Emotion* 18: 130-166, 1994.
17. Zucker, L. G. Production of trust: Institutional sources of economic structure 1840-1920. In: *Research in organizational behavior*, edited by B. M. Staw and L. L. Cummings. Greenwich, C.T.: JAI Press, 1986, p. 53-111.
18. Rotter, J. B. Interpersonal Trust, trustworthiness, and gulibility. *American Psychologist* 35: 1-7, 1980.
19. Mayer, R. C., J. H. Davis, and F. D. Schoorman. An integrative model of organizational trust. *Academy of Management Reviw* 20: 709-734, 1995.
20. Alpert, S. R., J. Karat, C.-M. Karat, C. Brodie, and J. G. Vergo. User attitudes regaring a User-Adaptive eCommerce Web Site. *User Modelling and User-Adapted Interaction* 13: 373-396, 2003.
21. Roy Morgan Research. Privacy and the community [Online]. http://www.privacy.gov.au/publications/rcommunity.rtf [December, 10th, 2001].
22. Byford, K. S. Privacy in Cyberspace: constructing a model of privacy for the electronic communications environment. *Rutgers Computer and Technology Law Journal*: 1-74, 1998.
23. Cranor, L. F. I Didn't buy it for myself: Privacy and ecommerce personalization. In: *Designing Personalized user experiences in eCommerce*, edited by C.-M. Karat, J. O. Blom and J. Karat. Dordrecht: Kluwer Academic Publishers, 2004.
24. Manber, U., A. Patel, and J. Robinson. Experience with personalization on Yahoo! *Communications of the ACM* 43: 35-39, 2000.
25. Culnan, M. J., and G. R. Milne. The Culnan-Milne survey on consumers & online privacy notices: Summary of Responses. *Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices.*, Washington DC, 2001.
26. Fox, S., L. Raine, J. Horrigan, J. Lenhart, T. Spooner, and C. Carter. Trust & Privacy Online: Why Americans want to rewrite the rules. Washington DC: The Pew Internet & American Life Project, 2000.
27. UMR. Privacy Concerns Loom Large. Study Conducted for the Privacy Commissioner of New Zealand. [Online]. http://www.privacy.org.nz/privword/42pr.html [15-02, 2001].

28.Harris Interactive. A Survey of consumer privacy attitudes and behaviors. Rockester, NY: Harris, 2000.
29.Spiekermann, S., J. Grossklags, and B. Berendt. E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. *ACM Electronic Commerce 2001 conference*, 2001, p. 38-47.
30.Loeb, S. Architecting personalized delivery of multimedia information. *Communications of the ACM* 35: 39-47, 1992.
31.Teltzrow, M., and A. Kobsa. Impacts of User Privacy preferences on personalized systems: acomparative study. In: *Designing personalized user experiences for eCommerce*, edited by C.-M. Karat, J. O. Blom and J. Karat. Dordrecht: Kluwer Academic Publishers, 2004.
32.CyberDialogue. Online consumer personalization survey. Wakefield: The personalization consortium, 2001.
33.Direct Marketing. Anonymous Web Browsing Threatens Profiling Practices of E-marketers. *Direct Marketing* 64:, 2001.
34.Sreenivasan, G. Does informed consent to research require comprehension. *The Lancet* 362: 2016-2018, 2003.
35.Friedman, B., L. Millet, and E. Felten. Informed consent online: A conceptual model and design principles. *UWCSE Technical Report* 00-12-2, 2000.
36.Federal Trade Commission. Privacy online: Fair information practices in the electronic marketplace [Online]. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [04-01, 2000].