7 Condition 1 for effective use of user profiling: Trust[9]

7.1 Introduction

In April 2003, first-time visitors to on-line bookstore Amazon.com were greeted with the message that the retailer '…continues to show remarkably high levels of customer satisfaction. With a score of 88 (up 5 %) (according to theAmerican Customer Satisfaction Index)[10] it is generating satisfaction at a level unheard of in the service industry…'. Information such as this is commonly used in the world of e-commerce. Displaying objective test results aims at increasing trust, similar to, for instance, the use of testimonials: users may reason that if so many other people have positive experiences with this online retailer, this company can be trusted, and engaging in a transaction is likely to yield positive results for them as well. As only first-time visitors receive this message, this constitutes a simple example of user profiling: providing such trust-enhancing messages aims to counter potentially low trust of a specific group of potential customers, i.e. first-time visitors. Returning visitors, on the other hand, are not exposed to it. First-time customers of an online retailer such as Amazon.com are especially prone to feelings of uncertainty. They may be ignorant of the company's security measures, causing them to become reluctant to enter their credit card number, they may fear that their personal data will be made available to third parties, or they may be unsure whether the purchased product will meet their quality standard.

Apparently, displaying positive test results is deemed especially effective for establishing new customers' trust. Once these have been persuaded to take the first step and complete an online transaction, Amazon's arrows are aimed at maintaining, instead of merely establishing a relationship, which may well require different means.

This chapter aims at defining and characterising one of the most important prerequisites for the implementation and acceptance of user profiling: trust.

User trust is influenced by various sources. Trust in relation to user profiling will be influenced by:

- the users' trust in the organisation he or she is dealing with;
- the users' trust in the services or products that the organisation is providing;
- trust in the systems the organisation 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.

This chapter will address the following questions: what is trust and what is its role in the relationship between organisations and their audiences, specifically in users' interactions with e-commerce and web service organisations? What forms and sources of trust influence users' decisions to use ICT applications in general? What types of user-related information are relevant to establishing and maintaining user trust?

[9] Author: P.W. de Vries
[10] See: www.theacsi.org/

7.2 The role of trust

Trust is generally considered to be the mechanism that reduces feelings of uncertainty or risk that customers, clients or citizens might experience. Specifically, trust effectively limits the vast number of possible future interaction outcomes to only a relatively small number of expectations. This may allow for a more careful investigation of the remaining options, thus reducing both uncertainty and risk of the actor (Luhmann, 1979).

Trust is a relevant issue especially in the service industries, both off- and online. After all, one important reason for people to ask the help of a service provider is that they do not have the knowledge or skill to do it themselves. A lawyer, for instance, is typically hired by people who do not hold a law degree themselves, and are thus insufficiently familiar with legal matters. This may seem a straightforward deal: in return for money, companies or people deliver a service that clients cannot perform or produce themselves. The downside, however, is that clients' infamiliarity with the subject matter makes it virtually impossible for them to judge whether the service provider does a good job. The uncertainty that results from the inability to monitor the service process can only be compensated by a sufficient degree of trust of the client in the service provider.

Online interactions, such as e-commerce transactions, are also characterised by uncertainty. The exchange of the consumer's money and the requested goods or service, for example, do not necessarily occur simultaneously, which creates the opportunity for the seller to behave opportunistically by not fulfilling his or her part of the deal. Because the online seller will probably remain anonymous, this behaviour is largely beyond the control of the consumer (Grabner-Kräuter & Kaluscha, 2003). Therefore, if the consumer does not trust the seller to be honest, he or she will probably not order a product online. The same goes for online information systems. A low level of trust may cause online advice or results of information queries to be met with scepticism, if not to fall on deaf ears. Thus, a user with a low trust level must reduce uncertainty or risk by seeking additional information elsewhere to corroborate the information provided by the seller, or the transaction will not take place.

A sufficient level of trust is necessary for transactions to run to a satisfactory completion, and for information to be duly accepted, whether in an on- or offline (social) context. Segmenting users on the basis of their degree of trust may therefore be useful. Providing specific groups of users or individuals with trust-enhancing information, for instance, may cause them to initiate or continue an interaction, which may result in an actual purchase or an effective information exchange.

The implementation of user profiling, however, also has major implications for user trust. User profiling implies requesting, collecting and storing user information, which very probably causes additional uncertainty. Users may feel highly uncomfortable about supplying the requested information and unsure as to whether their privacy will be honoured or violated. A privacy statement that is misinterpreted by the user, or simply overlooked, may make them feel exposed to the risk that their personal data are out in the open, for everyone to take advantage of.

This chapter provides an overview of current notions on the subject of trust. First, attention will be devoted to trust models that have proved influential in trust research, followed by a discussion on possible differences between trust between human partners on the one hand, and trust between a human and a non-human actor (application or system) on the other. Finally, the role of direct and indirect information in the formation

of trust will be examined. Suggestions for further research will be made in the final paragraph.

7.3 Forms of trust: general, social, interpersonal and organisational trust

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 Bhattacherjee, Devinney, & Pillutla, 1998; Earle, Siegrist, & Gutscher, 2002; Rousseau, Sitkin, Burt, & Camerer, 1998).

Even within the discipline of psychology, different theories of trust and its constituents exist. 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 (Earle et al., 2002). 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. From a user profiling perspective, it would be worth knowing what this stable trust level of an individual or group is, in order to predict whether interaction-specific trust may be built up; low general trust simply provides an insufficient feeding ground for other types of trust.

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 (Siegrist, Cvetkovich, & Gutscher, 2001). Social trust, a focus of attention in risk management research, involves little or no interaction, and is often a 'one-shot' affair (Earle et al., 2002). 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. It seems difficult, however, to determine which of the many values that people hold are relevant in a particular interaction between organisation and user, and what the correct way should be to convey these values.

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 (Bhattacherjee et al., 1998). This expectation is argued by some to be based on perceptions of the other's competence and honesty (Renn & Levine, 1991) or goodwill (Yamagishi & Yamagishi, 1994). 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 partners; in this case the organisations on the one hand and the users on the other. 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 (1986), for instance, used the term **characteristic trust** to denote trust based on social relations, comparable with Earle et al.'s (2002) concept of social trust. In addition, Rotter (1980) 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 (1995) 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 **organisational trust** and **system trust**, as interacting with an organisation online 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 deductable expenses electronically, or use calculation models to determine the financial consequencs thereof.

Both organisational trust and system trust can, to a certain extent, be viewed as special cases of social or interpersonal trust, as will be discussed in the next sections. Whereas the application of such trust antecedents as value similarity and intentionality to organisations is an easy step to make, for trust in systems this step is more difficult. After a brief discussion of the antecedents of organisational trust, it will be argued, however, that applying human-like concepts to systems is by no means far-fetched.

7.4 Trust in organisations

Researchers differ somewhat in their opinion on whether **trust in organisations** should be considered identical to or different from trust in persons. Most, however, appear to treat organisational trust as a special case of interpersonal trust. Mayer, Davis, and Schoorman (1995), for instance, presented a model in which the trust of one party in another is determined by the trustee's **ability**, **benevolence** and **integrity** (as perceived by the trusting party). The impact of each of these factors was argued to be moderated by the trustor's **propensity to trust**. As such, someone with a low trusting propensity would require more evidence of the trustee's ability, benevolence, and integrity before engaging in an interaction with the other party, than someone with a high propensity would.

Doney, Cannon and Mullen (1998) noted the importance for trust-building of perceived **intentionality**, i.e. an assessment of the trustee's motives, and **capability**, the former conforming to Mayer et al.'s benevolence and integrity, and the latter to ability. In addition, Doney et al. noted other processes that are relevant to the formation and building of trust, namely **calculative**, **prediction** and **transference processes**. The first process relates to the trustor calculating costs and benefits in case the trustee proves to be untrustworthy[11]. Prediction refers to the trustor's belief that the trustee's future actions can be predicted from past actions (also see Rempel, Holmes & Zanna's (1985) predictability, in the following section). Finally, transference processes entail trust to be transferred from a known entity to an unknown one.

[11] For most researchers and theorists, however, this assessment of costs and benefits represents the element of risk that is a prerequisite for, rather than an antecedent of trust; trust implies a willingness to be vulnerable, i.e. to engage in a situation typified by an unfavourable cost-benefit assessment.

This transference of trust may be especially important for user profiling. If transference indeed happens, then the likelihood that a user accepts his or her data to be gathered and entered into a user profile probably depends on the trust he or she has in the organisation. For example, a user may decide to buy groceries online via the site of a particular supermarket, and allow a user profile to be constructed because he or she has the opinion that the brick-and-mortar version of the supermarket represents a decent company. Likewise, the positive impression of the national tax service may be reason to submit tax statements online instead of by conventional mail, and allow personal data to be collected to speed up next year's submission.

Zaheer, McEvily and Perrone (1998) defined interpersonal and interorganisational trust as different constructs. In doing so, they conceptualised organisational trust as 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.

From the perspective of user profiling, this overlap of organisational with interpersonal and social trust, suggested by Zaheer, McEvily and Perrone (1998), is of major importance. It implies that the trust of a user in an organisation can be based on inferred **value similarity**, as well as on direct interactions. Thus, one may perceive a health insurance company as untrustworthy, simply because a value such as making profit may not match that of the user, who is merely interested in receiving good coverage for medical expenses. The situation may be different, however, if an organisation covers medical expenses without the objective of making a profit. At the same time, judgements of organisational trust may also be based on direct interactions, with positive experience leading to increased trust, and negative experiences to decreased trust. In principle, these two bases of trust could both enhance or attenuate one another. It is up to researchers in the field of organisational trust to determine which base of trust will prove to be superior.

7.5 Trust in systems

The concept of **system trust** can also be seen as a special case of interpersonal trust. Like interpersonal trust it refers to expectations about the 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 or a group of humans, but rather an object, i.e. the system with which a user is in interaction.

The concept of trust as it is studied in the context of (online) human-system interactions relies to a large extent on trust models that originated in personality (Rempel et al., 1985) and sociology research (Barber, 1983). Whereas the former strictly deals with interpersonal relationships, albeit applied by others to a more technical domain, the latter specifically deals with both humans and non-humans as interaction partners.

Rempel, Holmes and Zanna (1985) presented a theoretical model that describes how interpersonal trust develops in close relationships. According to them, there are three stages through which trust between people develops, namely predictability, dependability, and faith. **Predictability** begins when each partner observes the other's behaviour. If one partner repeatedly fulfils his or her promises, the other will view this as predictability. Predictability may be influenced by a number of factors. Among them are the consistency of recurrent behaviour, stability of the social environment, and knowledge of functional reinforcements and restraints on behaviour. When the partner has witnessed enough consistently performed behaviour, trust moves to the next stage,

dependability, which refers to the other's general traits instead of the predictability of specific behaviour. After a partner is seen to behave predictably, he may be labelled dependable or reliable. The final category, **faith**, evolves as partners grow confident that their relationship will last. Decisions on faith represent a shift from expectations about a partner's current traits to expectations about his or her general motives concerning the present and future value of the relationship.

Barber (1983) also noted the importance of observed behaviour, be it human or system behaviour. He defined trust as a taxonomy of three specific expectations, namely expectations of persistence of natural and moral social orders, technically competent role performance, and fiduciary obligations and responsibility. **Expectations concerning the persistence of natural and moral social orders** entail beliefs that others are, and will continue to be good or decent. The **expectation of technically competent role performance**, Barber argued, is not only central to trusting others who perform actions or services for us, but is also at the very heart of trust in human-system interactions. Finally, **expectations of fiduciary obligations and responsibility** represent a basis for trust when the user's technical competence is exceeded by the interaction partner, or referent's, or is unknown to him or her. Unable to form a judgement based on the referent's competence, the user is forced to rely on the referent's moral obligation not to abuse the power he has. As such, it offers the possibility to trust an unknown hospital physician based on the thorough educational system that this person is assumed to have undergone, and the high ethical standards this is accompanied by.

7.5.1 Trust in other people versus trust in systems

Generally, models of system trust used by many researchers do not explicitly distinguish between human and non-human actors. Some researchers, however, have put this assumed equality of interpersonal trust and system trust to the test.

Lerch and Prietula (1989), for instance, investigated how attributions of qualities to agents, i.e. a human or a system providing financial management advice, influenced trust on the part of the operator. They found that **source pedigree**, i.e. the source being a human novice, a human expert or a computer, played an important part in the formation of trust. Interestingly, their results suggest that although participants' levels of trust in an expert system did not differ from their trust in a human novice offering the same advice, the information used to form these judgements differed. In addition, although trust in the human expert's advice was greater than in the human novice, the information used seemed to be the same. Specifically, if the source was human, participants did not seem to use their judgements of agreement with each individual piece of advice to update trust levels when an unpredictable, negative event occurred. Contrarily, agreement judgements regarding such an event were incorporated in their final trust judgement if the source of advice was an expert system.

Waern and Ramberg (1996) conducted two studies in which they compared trust in advice given by humans or by an expert system but found contradictory results. In a study requiring participants to solve problems in a matrices test, they found that human advice on the correct answer was trusted more than computer advice, whereas in a study concerning car repair problems they found opposite results. Waern and Ramberg argued that these findings may well be explained by differences in the **particular task** and participants' **background knowledge**. Compared with the first study, the task in the second study was more difficult and required domain-specific, rather than general,

knowledge about cars, which may have caused participants to place more trust in computer-generated advice than in advice from humans.

Lewandowsky, Mundy and Tan (2000) argued that in process control tasks a person's trust in automation is positively linked to **system performance**, in the same way as when humans operators interact with a human partner. Different from control delegation between humans, however, Lewandowsky et al. argued that switching to automatic control implies that the person delegating control still bears ultimate responsibility for the quality of the process' outcomes. Because this responsibility is recognised by system operators, the occurrence of errors may affect their self-confidence. Contrarily, in situations in which humans interact with one another and switch control of task performance, the responsibility is shared. This distributed responsibility may cause a human operator's **self-confidence** to be more resilient to the occurrence of errors. Indeed, in their study Lewandosky et al. found that self-confidence remained largely unaffected by errors during manual operation in the human-human condition. They also found no evidence indicating that people are more reluctant to delegate control to a human collaborator than to automation, and concluded that '…the moment-to-moment dynamics of trust between people who share tasks within a complex environment resemble those observed between human operators and automation' (2000, p.121).

Earle, Siegrist and Gutscher (2002) proposed a dual-process model of cooperation between partners in interaction, in which a distinction between the concepts of trust and confidence is made. According to them, trust is a relationship between an agent and another (presumed) agent, and is based on **social relations**, **group membership**, and **shared values**. Confidence, on the other hand, concerns agent-object relations, and is proposed to be a belief concerning the occurrence of expected future events, based on experience or evidence. Another difference, according to Earle et al. is the centrality of **emotions** to trust, and the attempt to avoid them in confidence.

7.5.2 Attributing intentionality to systems

Central to some of the ideas mentioned above is the contention that the difference between trust in humans and non-humans lies in the **attribution of concepts as traits, reasons, intentions, and values** to the entity-to-be-trusted. Lerch and Prietula (1989), who found that the same advice was trusted more when it was given by a human expert rather than a computer or a human novice, argued that this phenomenon was caused by users' attributing a trait as dependability to human experts, but not to human novices and expert systems. In a similar vein, Lewandowsky et al. (2000) argued that trust between humans and automation is asymmetrical, because people may not be willing to attribute values, motivation and personal goals to machines. Although Earle et al. (2002) did not exclude the possibility that people may take certain objects to be agents, their distinction between confidence and trust appears to favour a similar distinction between trust in other humans and trust in non-human entities based on the inference of agency; given sufficient interaction, people attribute agency (value similarity, intentions, reasons) to other people, but probably not to systems. Interaction with systems will probably not encourage judgements to go beyond the mere prediction of behaviour from objective evidence, such as perceived causes.

However, empirical evidence has yet to show that the attribution of concepts such as values, intentions or goals allows for a valid distinction between system trust and interpersonal trust. One could argue that the development of system trust to the point where such attributions are made is a mere matter of **interaction duration and**

complexity. Rempel et al. (1985) argued that the level of dependability is reached only after the trustor has observed a sufficient amount of predictable behaviour. As such, interpersonal trust is assumed to develop from observation of objective information (the other's behaviour) to a stage in which attributions are made, i.e. dependability. In the light of this notion, the contention that trust in systems seems to be based on different information than trust in humans, as implied by Earle et al. (2002), may not necessarily stem from conceptual differences, but rather from differences in developmental stages. In other words, system trust may indeed be based on different information than interpersonal trust, but perhaps only because the former has not yet had the opportunity to evolve into the same developmental stage as interpersonal trust. Not only may our interactions with systems be less frequent than those with other people, but trust-relevant information may also be more available in social interaction than in human-system interactions (for a discussion, see Ronald & Slipper, 2001). Differences in the frequency of interactions as well as the amount of trust-relevant information available per interaction may cause system trust to develop more slowly than interpersonal trust. Given sufficient time and interaction, system trust may also become based on trait inference, i.e. that users attribute traits such as dependability to the systems they interact with. An important implication of this possibility for user profiling would be that this stresses the need to distinguish between regular and extremely experienced users. If the attribution of traits indeed becomes more likely with experience, that would imply that users do not adjust their opinion or judgement of a system on the basis on anomalies encountered while in interaction, but instead rely on their attributions, which may be formed on the basis of considerable interaction experiences and hence are relatively stable.

Attribution of causality to system behaviour, which is supposed to build confidence rather than trust (according to Earle et al., 2002), can probably only develop when the system's inner workings are relatively straightforward. Systems that are considerably more complex may make it hard, if not virtually impossible, for a user to establish cause-and-effect relations. If causes remain obscure to users, they may turn to less objective information such as emotions, and may be less reluctant to attribute traits such as dependability, competence and agency to the system, thus transcending Rempel et al.'s (1985) stage of predictability.

The observation that system trust comes down to predicting future outcomes after observation of behaviour, does not exclude the possibility that, given time and complexity, it will evolve to a stage analogous to trust in a human actor. The fact that most people are aware that systems cannot actually hold traits, values or intentions in the same way humans do, is by no means detrimental to this conclusion. In fact, research by Nass and Moon (2000) clearly indicates that individuals mindlessly apply social rules and expectations to computers, although every single one of them articulated awareness that a computer is not a person, and does not warrant attributions or treatment as such. For instance, after being exposed to a virtual agent with social cues (in this case a Korean or Caucasian video face), persons with the same ethnical background as the virtual agent perceived it as being more attractive, persuasive, intelligent and trustworthy, compared with participants with a different ethnicity, just as they would have if they had been dealing with a real person. As Nass and Moon put it: ’Once categorised as an ethnically marked social actor, human or nonhuman was no longer an issue’ (2000, p.86).

Indeed, value similarity and other human-like concepts as a basis for trust may not be restricted to interpersonal relationships. Similar phenomena can be found outside this context. It may, for instance, be comparable to selectivity, a principle thought to underlie trust in media, as some media researchers argue (Kohring & Kastenholz, 2000). Thus,

one may trust the content of a particular newspaper because its perceived social or political stance matches one's own, which becomes apparent from the selection of and reporting on news items. In a similar vein, the output of relatively complex systems may depend on a hierarchy of decision rules; a route planner, for instance, may favour a particular strategy for determining routes during rush hours, whereas another strategy is selected in the quiet evening hours. A change in the prioritisation of decision rules that causes output patterns to change, could be interpreted by the user in the same way he or she interprets changes in the behaviour of another human to be indicative of intentions.

The inference of such traits as intentions, however, is little understood. It is possible, therefore, that users interpret the available information differently than intended by the designer of a system or webpage, and this may have dire consequences for the implementation and acceptance of user profiling. Acceptance of user profiling may be greatly enhanced if companies or organisations are explicit and honest about what they intend to do with the accumulated user data, and provide justifications for doing so, instead of leaving the inference of intentions up to the user.

7.6 Direct and indirect information as a basis for trust

A trusting person, Yamagishi and Yamagishi noted '… overestimates the benignity of the partner's intentions beyond the level warranted by the prudent assessment of the available information' (Yamagishi & Yamagishi, 1994, p.136). In other words, trust involves the extrapolation of insufficient information in order to reduce uncertainty. Indeed, trust is not blind; trust requires whatever information is available in order to evolve. Whereas Rempel et al. (1985) focused exclusively on observed behaviour as a source of information, Barber (1983) specifically noted the possibility that trust-relevant information can be obtained through other channels as well, an idea that was picked up by researchers such as Muir (1987), and Lee and Moray (1992). Following Barber's ideas, they incorporated the system's designer and his assumed motives and intentions in system trust theory. This means that system trust can be established by trusting the person or organisation behind the system. Users build up their view of the trustworthiness of the organisation behind the system by communicatiing and interacting with that organisation, but also by events and experiences outside the context of the use of the system.

The view that both direct and indirect information can influence system trust, was further elaborated on by Numan (1998; Also see Arion, Numan Pitariu & Jorna, 1994). Similar to other researchers, they considered direct information to be first-hand knowledge, derived from one's own experiences about what the system is good at and what not, allowing for assessments of **consistency of performance**, or **predictability** (cf. Zuboff's (1988) 'trial-and-error experience', Lee and Moray's (1992) 'performance' and Rempel et al.'s (1985) 'predictability', for instance). Indirect information, on the other hand, constitutes information about the system that is obtained from others, i.e. information that is not based on one's own direct interactions with a system. Numan, for instance, proposed that trust can be based on **observing someone else interacting with a system**. Behaviours that can be interpreted as trusting behaviour may induce the observer to conclude that the system is trustworthy. Likewise, one could base trust on 'second-hand experiences', i.e. the experiences of others, in the form of recommendations or reported interactions with a system.

7.6.1 Indirect information

Partcularly in first-time interactions, the information available on which to build trust might be minimal; novice users, after all, do not have an extensive body of interaction experiences at their disposal. According to some theorists, such a lack of prior interactions implies that initial trust is low (for instance, see Blau, 1964), which would provide a major obstacle to adoption or acceptance of user profiling, or system advice and e-commerce, for that matter. After all, deciding to engage in interaction with an unknown e-commerce company requires a high level of initial trust to reduce uncertainty. As McKnight, Choudhury, and Kacmar (2002) argued, however, the mere fact that a potential consumer has not yet had any interaction with an online vendor does not necessarily mean that initial trust is low. In initial relationships, McKnight et al. argued, people may use whatever information is available; as such, initial trust can be influenced by a host of factors, such as **perceived website quality**, **reputation**, **third party endorsements**, e.g. by a professional medical association in the case of a medical website, but also on an individual's propensity to trust others (McKnight, Cummings, & Chervany, 1998). In addition, McKnight et al. noted the importance of institution-based trust, which refers to a belief in technical and legal structures upholding proper online conduct (2002). If such information yields sufficient initial trust, a first-time consumer may be persuaded to engage in a transaction (also see McKnight et al., 1998, in the context of organisational relationships).

7.6.2 Direct information

Direct experience is gained by actually interacting with the system and may, over time, yield information about the system's behaviour. Repeatedly yielding satisfactory output, the system may be perceived as predictable, consistent and stable, thus enabling users to anticipate future system behaviour (e.g. see Lee & Moray, 1992; Rempel et al., 1985, in the context of interpersonal trust; Zuboff, 1988). Also relevant in this context, however, may be that direct experiences seem to play a role in a more subtle way. Woods, Roth, and Bennett (1987), for instance, found that when the technicians that took part in their studies did not wait until unequivocal right/wrong feedback became available to them to form a trust judgement, but rather followed their own judgements on the plausibility of the system's 'line of reasoning' as it was fed back to them. Apparently, people sometimes judge the quality of system advice on feedback regarding the process that led to that advice.

Lee and Moray (1992) hypothesised that besides automation **reliability**, also **process** should be considered as a trust component of direct experiences. Process is used to denote an understanding of the system's underlying qualities or characteristics. Whereas in humans this might encompass stable dispositions or character traits, in a more technological domain this could be interpreted as rules or algorithms that determine how the system behaves. Others have come up with mental models to denote understanding of a system (e.g. see Caroll & Olson, 1988; Sebrechts, Marsh, & Furstenburg, 1987).

Such understanding of how a system arrives at a solution to a problem presumably increases user trust. One aspect important in this respect is **consistency**; users may conclude there is a reason for the system's process feedback to show a particular recurrent pattern. For example, someone using a route planner may request advice on a number of different routes and subsequently find that the system persists in favouring routes that use a ring road to those that take a shortcut through the city centre (or vice versa). The user may, subsequently, infer that although the shortcut through the centre

seems faster, the system may disregard it because it is prone to dense traffic. Although such explanations do not necessarily match the system's actual procedures, they may facilitate the formation of beliefs about what is happening 'inside' the application. Indeed, research by Dzindolet, Peterson, Pomranky, Pierce, and Beck (2003) has shown that participants working with a 'contrast detector' to find camouflaged soldiers in terrain slides, trusted the system more, and were more likely to rely on its advice when they knew why the decision aid might err, compared with those who were ignorant of such causes. Although Dzindolet et al.'s (2003) studies provide additional, empirical support for the idea that a sense of understanding is beneficial to trust, their participants did not obtain this information from their own direct experiences with the device, but received it from the experimenter. Research by de Vries, Midden and Bouwhuis (de Vries, 2004) strongly suggests that users gain understanding by actually observing system behaviour, as both Lee and Moray's (1992) concept of 'process' and mental model theory entails.

These findings support the conclusion drawn in an earlier section that it is important for user profiling to be accepted if users understand what will happen with the personal data they are requested to enter for the sake of creating a user profile.

7.7 Discussion

Trust is an important concept in situations that are characterised by uncertainty and risk. In fact, it determines whether consumers are willing to extrapolate what little information they have and subsequently place themselves in a vulnerable position. As such, trust is highly relevant to all actors who wish to construct user profiles in order to enhance the efficiency of online interactions by tailoring the information given to them.

Users may indeed feel they are putting themselves in a vulnerable position by allowing their existing user profile to determine what information they will be presented with. One of the risks they run concerns their perceived privacy; in the eyes of users, their data may be sold to third parties who may use it to send them personalised promotion material or unsolicited e-mails. As a result, users may have the unpleasant feeling that a part of them is 'out in the open' for everyone to take advantage of. Worse still, the constructed profile may contain information about such issues as a user's health that, if it ends up in the hands of health insurers, it may make it impossible for him or her to get cheap medical insurance. Another risk concerns the idea that users may feel deprived of information that they would have had at their disposal if they had had a different profile. It could happen, for instance, that users, whose profiles indicate that they are not novices, automatically skip information that is considered only relevant to novices.

However small these risks might seem in the eyes of the proponents of user profiling, they are real and relevant; feelings of risk that are not compensated by trust may cause the users to seek their information elsewhere, provided they actually have a choice. If an alternative is not readily available, however, insufficient levels of trust may cause the user to engage in additional processing of information, such as looking for related material that corroborates the information already provided. This, in fact, decreases the efficiency of the interaction, and, consequently, user satisfaction.

7.7.1 Antecedents of trust

Several factors that are likely to influence trust have come to light in the previous sections. The two concepts most relevant to user profiling, trust in organisations and trust

in systems, received special attention. Table 7.1 lists the main antecedents of both types of trust. It is important to realise, however, that the list of antecedents presented here may not be complete. Compared with trust in systems, where the role of recommendations and reputation, for example, is increasingly realised, research in organisational trust has so far largely neglected the role of indirect information. Nevertheless, information about organisations that is received from someone else, such as by word-of-mouth, might be of influence to trust in those organisations. In other words, Table 7.1 might give the impression that several factors are exclusive to the domain of system trust, but this may merely be a result of a somewhat different focus of research in this particular field, compared with research in organisational trust. It is, therefore, a good possibility that the factors listed here apply to both kinds of trust.

Trust in systems	**Trust in organisations**
Agreement	
Predictability, consistency	Prediction
Reliability, stability, dependability, competence	Ability, capability
Value similarity	Value similarity
Intentionality	Benevolence , integrity, intentionality
Recommendations, endorsements	
Perceived website quality	
Occurrence of (outcome) failures	
Understanding, process	
	Calculation
	Transference

Table 7.1: Overview of the antecedents of system trust and organisational trust, as identified in this chapter

One important antecedent shared by both types of trust is predictability or consistency of observed behaviour. According to Rempel, Holmes and Zanna (1985), this constitutes the first step in the development of trust. The next step would be the inference of reliability, dependability, competence and capability. Instead of referring to observed behaviour, these antecedents are actually attributions, i.e. assumed qualities of the system itself. At an even higher level, concepts such as value similarity, intentionality, benevolence and integrity may come into play. Organisations who want to increase user trust, either in the organisation itself or in the (online) systems utilised by them, should consider these factors. Predictability or consistency in communication with the user, or in organisational behaviour in general, for instance, is beneficial to the development of trust. On this basis, several attributions about system or organisation may be formed, ranging from relatively low-level attributions of characteristics, such as competence and reliability, to more human-like attributions, such as intententionality, values or intergrity. However, such inferential processes are little understood and, if left to the user, might run in a different direction than anticipated. Organisations would therefore be wise to make information about their values, intentions, etc., explicit, so as to prevent users from engaging in uncontrollable and unpredictable inferential processes themselves.

Other factors, specifically aimed at countering low initial trust in e-commerce settings, are such aids as recommendations, endorsements and perceived website quality. Although these factors are mentioned in system trust literature, and not in that of organisational trust, it is not unlikely they apply to the latter as well.

The occurrence of failures made by a system or an organisation, such as transaction mishaps or supplying users with inaccurate information, cannot be fully prevented. Measures should therefore be taken to provide a buffer against them; making values or intentions (more) explicit, or simply providing a means to users to understand the functioning of system or organisation, may make user trust less susceptible to occurring failures.

Special care is warranted by interactions that can be characterised as computer-mediated communication; in such cases, a computer application mediates the communication between a customer and the company or organisation. Whereas in direct interactions between customer and company the success of an interaction depends on the trust of the former with regard to the latter, in such mediated interactions also a third factor has to be taken into account: the application itself. Thus, the customer's trust may be directed at both the focal system and the organisation that operates the website. If either of these trust judgements falls below a certain threshold, the interaction is likely to cease. It is, for instance, possible that a brick-and-mortar bookstore is well-known and trusted by its customers but that those same customers are hesitant to buy a book online from the same store.

In addition, perceptions of application and organisation may influence one another. Indeed, web-based organisations often try to influence customer trust by displaying endorsements by independent, trustworthy third parties, e.g. by a professional medical association in the case of a medical website (Briggs, Burford, De Angeli, & Lynch, 2002; Corritore, Kracher, & Wiedenbeck, 2003; McKnight et al., 1998; for studies on the role of indirect information in different domains, e.g. see Meijnders et al., 2004; Standifird, 2001). As such, a customer's trust in the advice generated by an online public transportation travel planner may increase if he or she learns that a trustworthy partner, such as the national railway company, is also participating in the enterprise. However, it could also happen that a negative impression of either of the two causes the other to become less trusted as well (transference of trust, e.g. see Doney et al., 1998).

Employing user profiling places high demands on trust calibration. For online interactions, whether financial transaction or information acquisition, to run to a satisfactory conclusion, users' initial trust levels need to be correctly ascertained so as to ensure that low trust users receive information aimed at reducing existing uncertainty and feelings of vulnerability.