Computational Intelligence

AN INTERNATIONAL JOURNAL

Computational Intelligence, Volume 31, Number 2, 2015

UNDERSTANDING PERCEIVED TRUST TO REDUCE REGRET

ELISA COSTANTE,[1] JERRY DEN HARTOG,[1] AND MILAN PETKOVIĆ[1,2]

[1] *Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, the Netherlands*

[2] *Philips Research Laboratories, Eindhoven, the Netherlands*

Trust is fundamental for promoting the use of online services, such as e-commerce or e-health. Understanding how users perceive trust online is a precondition to create trustworthy marketplaces. In this article, we present a domain-independent general trust perception model that helps us to understand how users make online trust decisions and how we can help them in making the right decisions, which minimize future regret. We also present the results of a user study describing the weight that different factors in the model (e.g., *security*, *look&feel*, and *privacy*) have on perceived trust. The study identifies the existence of a positive correlation between the user's knowledge and the importance placed on factors such as security and privacy. This indicates that the impact factors as security and privacy have on perceived trust is higher in users with higher knowledge.

Received 18 December 2012; Revised 29 November 2013; Accepted 1 December 2013

Key words: perceived trust, trust decision, regret, security, privacy.

1. INTRODUCTION

The number and types of e-services available for end users are continuously increasing. Governments, institutions, and companies are moving their services to the Web. Activities such as tax declaration, prescription renewal, or shopping can be now easily accomplished online. While simplifying the execution of daily activities, the use of e-services also exposes the user to risks of cyber crimes such as frauds or identity theft. Users should be aware of the risks they face while using an e-service, and they should trust only those services that are worthy of trust. To this end, mechanisms that help the user in making the right trust decisions should be provided. Clearly, to make such mechanisms available, it is necessary to know how users make trust decisions, that is, how do they decide whether to trust an online service or not, and when a service is worthy of trust. In this article, we focus on the first interaction with a service; thus, no direct past experience with the service is assumed.

Trust is a complicated concept carrying many meanings (Ruohomaa and Kutvonen 2005). The Oxford English Dictionary defines trust as the "firm belief in the reliability, truth, or ability of someone or something." In sociology and psychology, trust is seen as the concept that governs most of the *human-to-human relationships* (Rotter 1971; Gambetta 2000). In business, trust is identified as one of the key factors for the development and maintaining of long-term cooperative relations (Ganesan 1994). In computer science, the computational value of trust (Marsh 1994) is used to organize agents' cooperation.

To deal with trust in the digital world, several attempts to adapt the concept of human-to-human trust to the online context have been made (Friedman, Khan, and Howe 2000). However, when the object of trust (*trustee*) changes in such a dramatic way (from a concrete person to an abstract object), also the models of trust have to change to adapt to the new context. For example, the signals of trust generally used to establish human-to-human relationships, such as physical aspects or body language, are missing when trust has to be established online. To understand online trust, we need to find analogous (or new) signals of

Address correspondence to Elisa Costante, Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands; e-mail: e.costante@tue.nl

trust and learn in which way they influence users' perceived trust. This understanding will allow the creation of mechanisms that help users in deciding whether to trust a Web service.

A large body of literature exploring the signals, or *factors*, affecting online trust exists (Beldad, de Jong, and Steehouder 2010). The main problem of existing solutions is that they typically focus on very specific context. This leads to similar models with many of the same factors being rediscovered many times in different disciplines and contexts. For example, different trust models applicable to e-commerce, e-health, or e-banking have been proposed (Kini and Choobineh 2000; Yousafzai, Pallister, and Foxall 2003; Faja 2006; Fruhling and Lee 2006; Azam, Qiang, and Abdullah 2012). Although such models are referred to different application domains, they consider factors of trust that largely overlap.

In this article, we propose to unify the work carried out on different areas under a general trust perception model (GTPM) that can be applied to different domains. The main idea is to have a set of factors of trust that encompasses those already presented in literature and to adapt the model to a specific domain by changing the weight of each factor. To show how one can determine such weight distributions, we performed a user study in four important domains, namely, e-commerce, e-banking, e-health, and e-portfolio. GTPM models the *perceived trust* in online services, that is, the degree to which a user perceives websites or e-services as trustworthy. The discussion of perceived trust and related concepts is further elaborated in Section 3.1.

A GTPM provides a framework describing how users make trust decisions and what can be done to help them in making decisions that reduce future regret. Regret is the feeling that arises when a trust decision turns out to be wrong; for example, the user is a victim of a fraud after using a Web service. As our user study reveals, factors such as the *look&feel* of a website often influence perceived trust more than factors such as *security* or *privacy*. Intuitively, a good-looking website with poor security is more risky for a user: If we want to reduce regret, such a website should be perceived less trustworthy than one with good security but with no attractive design. To better explain this situation, we introduce the following example.

Suppose that Alice is considering to use an e-commerce site for the first time. After browsing the site for a while, Alice decides to trust it because it looks very professional and easy to use. She does not put attention on whether the site uses security protocol, for example, https, and she only looks for the presence of a privacy policy to "be sure" that her personal data are protected. Finally, Alice chooses a product and makes a payment, and after a couple of days, she successfully receives her purchase.

Assume now that one of the following events takes place: (i) the website is a victim of an eavesdropping attack, and Alice's credit card number is stolen together with a considerable amount of her money; and (ii) Alice receives daily advertising e-mails because the website, as stated in its policy, shared her e-mail with all its partners. In both cases, Alice might regret her initial trust decision. In the first case, the trust decision might have been different if Alice would have given more importance to the security factor and looked for a more secure website (e.g., one using https where eavesdropping is more difficult to achieve). In the second case, the decision would have been different if the mere presence of a privacy policy would have not been seen as an indicator of high privacy protection.

Hence, we believe that trust decisions can lead to regret because of the existence of (i) a gap in the importance given to a factor before and after making a trust decision (e.g., Alice realizes she gave too much importance to look&feel and too little to security) or (ii) a gap between the *objective* value of a factor of trust and the value perceived by the user (e.g., the mere presence of a privacy policy perceived as indicator of high privacy protection). We refer to the first type of gap as the *factor importance gap* and to the second as the *factor indicator gap*. To meet our general goal of minimizing regret, both gaps need to be reduced.

In this article, we focus on the factor importance gap, and we hypothesize that the initial importance given to factors such as security and privacy can be increased by acting on the user's knowledge. To test this hypothesis, we perform a user study as described in Section 4. The factor indicator gap is introduced in our GTPM, but its further analysis is out of the scope of this work.

Thus, in this article, we provide the following main contributions:

- A literature review of the existing trust perception models (TPMs), with a special focus on the factors of trust defined by each model.
- A GTPM that describes how users make trust decisions. The model defines the existence of gaps between the *perceived* and the *objective* trustworthiness of a website and suggests that reducing such gaps can lead the users to reduce the regret due to bad trust decisions.
- Empirical and statistical evidence that (i) the weight users give to a factor changes according to the domain and (ii) by increasing the user's knowledge, it is also possible to increase the weight of the factors privacy and security. The aforementioned hypotheses are tested by analyzing the responses of more than 350 users that took part in our user study.

The remainder of the article is organized as follows. In Section 2, we present the related work; in Section 3, we show the GTPM and the way we obtained it; and in Section 4, we describe the user study we performed to test our hypotheses, its design, and its validation process. In Sections 5–7, we discuss the results of the user study, while in Section 8, we provide the conclusions. The questionnaire we developed for our user study is fully described in the Supporting information.

2. RELATED WORK

The definition of the term *trust* has been widely addressed in literature. Generally, trust can be seen as expectations (Deutsch 1962; Rotter 1980; Mui, Mohtashemi, and Halberstadt 2002), as vulnerability to the actions of others (Mayer, Davis, and Schoorman 1995), as probability that a certain beneficial (or at least not harmful) action will be taken by the trustee (Gambetta 2000), or as risk (Johnson-George and Swap 1982). In addition, trust is usually seen as a multidimensional concept (Mayer et al. 1995), that is, it can be modeled by using a set of factors, and it is often referred as being *context specific*, that is, related to a given domain or situation (O'Donovan and Smyth 2005).

Despite claims such as "people trust people, not technology" (Friedman et al. 2000), the idea of extending the concept of trust to the digital world got the attention of many, leading to the development of computational (Marsh 1994) and human-to-computer (Muir 1987; Madsen and Gregor 2000; Lee and See 2004; Atoyan, Duquet, and Robert 2006) models of trust. The human-to-computer models mainly aim at identifying the factors affecting trust, such as usability (Atoyan et al. 2006; Hoffman, Lawson-Jenkins, and Blum 2006), reliability and competence (Madsen and Gregor 2000), and security and privacy (Hoffman et al. 2006).

The explosive growth of e-services has increased the interest of researchers toward the study of how humans establish trust with online transactional systems such as websites or Web applications. According to Camp (2003), for such systems to be trusted, they need to be "designed for trust," that is, accounting for factors such as privacy, security, and reliability from the very beginning. Corritore, Kracher, and Wiedenbeck (2003) detected reputation, usability, and risk as determinant factors of trust in websites. McKnight, Kacmar, and Choudhury (2004), focusing on trust in e-commerce services, asserted that users go through two different stages before using an e-commerce service: an introductory stage, where they explore the website, and an exploratory stage, where they decide whether to make any transaction using it. The quality of a website, such as the absence of presentation flaws, also seems to influence the trust and the willingness to buy in the e-commerce setting (Everard and Galletta 2003). Trust also seems to be influenced by the user's knowledge (Hoffman et al. 2006). Additionally, misconceptions about security and privacy might lead to a false perception of trust (Flinn and Lumsden 2005). It is still not clear whether a deeper knowledge, for example, on security mechanisms, increases (Jiang, Chen, and Wang 2008) or decreases (Hoffman, Novak, and Peralta 1999) the general trust in e-services. In this article, we provide evidence that deeper knowledge increases the impact that privacy and security factors have in determining the trust in an e-service.

Studies on trust are generally based on a theoretical TPM, accounting for several factors—or antecedents—of trust. An in-depth literature review on the antecedents of trust is available in Beldad et al. (2010). The general hypothesis at the basis of a TPM is that such antecedents positively or negatively influence the perceived trust. This hypothesis is usually validated by means of a user study that experimentally determines which factors are actually taken into account before trusting. Every trust model applies to a specific domain and category of users. Trust models in the area of human-to-human (Mayer et al. 1995), human-to-aid systems (Muir 1987; Atoyan et al. 2006), human-to-computer (Madsen and Gregor 2000), and human-to-e-services (Corritore et al. 2003) relationships can be found in the literature. Specifically to the area of human-to-e-services, TPMs about e-commerce (Kini and Choobineh 1998; McKnight, Cummings, and Chervany 1998; McKnight, Choudhury, and Kacmar 2000; McKnight and Chervany 2001; McKnight, Choudhury, and Kacmar 2002; Everard and Galletta 2003; Hsu 2008), e-banking (Yousafzai et al. 2003; Lee, Kang, and McKnight 2007), and e-health (Faja 2006; Fruhling and Lee 2006; Sillence et al. 2007) exist.

In Table 1, we give an overview of the existent TPMs. Each row represents a TPM and each column one factor of trust; a cross indicates that the factor is part of the model and that its influence on perceived trust has been experimentally validated by the related work. Note that authors may use different terms to refer to the same factor (e.g., disposition to trust or dispositional trust): In the table, we try to unify this naming. The last row of the table indicates the percentage of analyzed TPMs accounting for the corresponding factor. Factors of trust can be of two types: user related, if relative to trustor's characteristics (e.g., *user's knowledge* and *disposition to trust*), or website related, if indicative of a property of the trustee. In the following, we give a brief explanation of the meaning of each factor.

User-related factors

- *User's knowledge (UK)* refers to the expertise the user has with regard to the information technology (IT) and security field (e.g., his level of knowledge/skills about the use of the computer and the Web, or matters such as https and privacy policies);
- *Disposition to trust (DT)* is a characteristic related to the personality of the user, representing the user's general predisposition to trust the world (McKnight and Chervany 2001).

Website-related factors

- *Risk* expresses the degree to which the use of the website can bring loss or damages to the user.
- *Reliability&availability* represents how good the website is in performing its functions and keeping them available for users.

TABLE 1. The Trust Perception Models in the Literature.

Reference	Risk	Reliability & availability	Third-party seals	Privacy	User's knowledge	Security	Disposition to trust	Quality and look&feel	Reputation	Brand name	Usability
Muir (1987)	x	x								x	
Mayer et al. (1995)	x						x			x	
Atoyan et al. (2006)											x
Madsen and Gregor (2000)										x	x
Corritore et al. (2003)	x		x				x	x	x		
Hoffman et al. (2006)		x		x	x	x			x		x
Camp (2003)		x		x		x					
Fruhling and Lee (2006)		x					x	x		x	x
Faja (2006)					x			x			x
Sillence et al. (2007)			x					x	x	x	
McKnight et al. (2000)	x		x		x		x	x	x		
Kini and Choobineh (2000)	x	x				x	x	x		x	x
Everard and Galletta (2003)								x			
Suh and Han (2003)			x			x					x
Cheung and Lee (2003)	x			x		x	x			x	
Jones (2008)			x					x			
Hsu (2008)			x	x	x	x	x	x	x		
Yousafzai et al. (2003)	x			x		x				x	
Azam et al. (2012)				x		x	x				
San-Martín and Camarero (2012)				x		x		x	x		
Rate (%)	35	25	30	35	20	45	40	50	30	40	35

- *Third-party seals* refers to the presence of trusted third-party logos and certificates on the pages of the website.
- *Privacy* refers to the way the website deals with user's personal data.
- *Security* refers to the set of mechanisms applied by the website to secure user's transactions and data (https, encrypted storing, vulnerabilities assessment, and fixing procedures).
- *Quality and look&feel* captures characteristics such as good design, attractive user interface, and absence of syntactic and semantic errors.
- *Reputation* refers to the way the website is seen by others.
- *Brand name* says how well the brand behind the website is known. This factor encompasses other factors such as *competence*, *integrity*, and *benevolence*, characteristics that are often associated to well-known brands.
- *Usability* refers to the ease of use of the functionalities provided by the website.

The results of the literature study presented in Table 1 show that existing TPMs share a significant number of factors of trust (e.g., half of the analyzed TPMs list quality and look&feel as an important aspect). New models keep being developed (Azam et al. 2012; San-Martín and Camarero 2012), and the factors overlap with existing models continues, justifying the need for a general model that could be easily adapted to different domains.

3. THE GENERAL TRUST PERCEPTION MODEL

In this section, we describe our GPTM, built by unifying the factors of trust used in existing solutions. Because the GTPM is not bound to any specific domain, it is possible to describe user's perceived trust in different context by simply changing the factor's weight. The model also describes how users make trust decisions and gives hints on how such decisions can be driven to reduce regret. The GTPM provides the benefits of (i) having a single model that can be adapted to different domains and (ii) unifying the work carried out in different areas of research. We will start by providing the definition of trust (and its related concepts) as intended in the remainder of this article in Section 3.1, while we will describe the GTPM in Section 3.2.

3.1. Definitions

The term *trustor* is usually referred to the person that establishes a trust relationship. In this article, with the term *trustor* we refer to the end user, while the term *trustee* is used to refer to the website the user is considering to use. Note that a *website* can be a very complex object; similarly to Li et al. (2012), we restrict our scope to a specific *transaction* between the user and the website, which could only refer to a small part of the website.

Trustworthiness is a property of the trustee indicating how worthy of trust the trustee is. Clearly, an object can be worthy of trust in a specific situation but not in another (Ermisch et al. 2009). However, what changes is not the object (which remains the same) but the trustor that is evaluating the trustworthiness in that specific situation. Therefore, we make a clear distinction between the trustworthiness and the (perceived) trust. *Trustworthiness* is a property of the trustee, seen as a vector of "various factors" of trust (Josang, Ismail, and Boyd 2007), while the *perceived trust* represents the trustworthiness in the eye of the trustor. Perceived trust depends on the importance the trustor gives to certain factors of trust and on the trustor's personal characteristics, such as her general disposition to trust and her knowledge.

Both trustworthiness and perceived trust depend on a set of factors of trust representing the dimensions of trustworthiness. In the following, with the term *factors of trust* we refer to the *website-related factors* presented in Section 2. This list of factors can be either extended, if a new factor needs to be introduced, or reduced, by giving zero weight to a factor. We assume that each factor f is somehow quantifiable; that is, it is possible to associate a numerical value v_f to it. Although for some factors it is more natural to have nominal values, for example, a label such as *low*, *medium*, or *high* for the factor *usability*, we assume that some form of conversion to the numeric scale is possible.

A *trust indicator* is a way of representing one or more factors of trust, to help the user in making trust decisions. For example, the *https padlock* is a trust indicator for the security factor, while *scores* (e.g., 95%) or *feedback* (e.g., three or five stars) could be indicators for reputation. Trust indicators help the user in associating a value to a factor of trust: Such value can be directly expressed by the indicator (e.g., five stars for reputation) or inferred by the user (e.g., the presence of the *https* lock means high security).

On the basis of the perceived trust, the user makes *trust decisions*; that is, she chooses whether the perceived trust is enough to start a transaction with the trustee. Unfortunately, trust decisions are often made without spending enough time to gather all the data on trustworthiness (Colquitt, Scott, and LePine 2007). To judge whether the right decision was made, the *a posteriori trust*, that is, the trust the user perceives after the transaction occurred, has to be taken into account. A posteriori trust depends on events, such as frauds, that did (or did not) happen. In case the a posteriori trust is different from the trust perceived before the transaction, the user can experience feelings of *regret*, that is, a discrepancy between what she has done and what she feels she should have done (Festinger 1957; Halpern 1989).

Regret can occur either because a positive trust decision (using the service) is betrayed by the trustee (Marsh and Briggs 2009) or because a negative trust decision (declining the use of the service) is erroneous (e.g., the website not chosen was actually trustworthy and the benefit of using the service was missed by the user). Computational concepts of regret and "regret management" are introduced in Marsh and Briggs (2009) and Etalle, den Hartog, and Marsh (2007).

3.2. The Model

In Figure 1, we present our GTPM, which aims at capturing the trust decision-making process and at understanding how trust decisions can be driven to minimize regret. Let us assume that Alice is our user and that, for each factor of trust, the website has a given value (v_f) representing the objective value of that factor, for example, how secure it is, what is its reputation, and how good it is in managing privacy. It is important to notice there could be a gap between the *objective value* of a factor (v_f) and the value perceived by Alice (v'_f). For example, the website may have a very *poor* management of users' personal data (it sells them to third parties without anonymizing it), but Alice may perceive the privacy management as very *good* (she saw that a privacy policy is published on the website, and for her, this is enough). We refer to this gap between the *objective value* and the *perceived value* of a factor as the *trust indicator gap*. If n is the number of factors, the perceived trustworthiness (PTW) can be expressed as a vector of perceived values.

$$PTW = \left(v'_1, v'_2, \ldots, v'_n\right) \tag{1}$$

The users' perceived trust (PT) is influenced by the perceived trustworthiness and users' characteristics such as the personal disposition to trust (DT), measurable with specific scales (Christie and Geis 1970; Rotter 1971), and the vector of importance ($W = (w_1, w_2, \ldots, w_n)$) the user gives to each factor of trust. The vector of importance

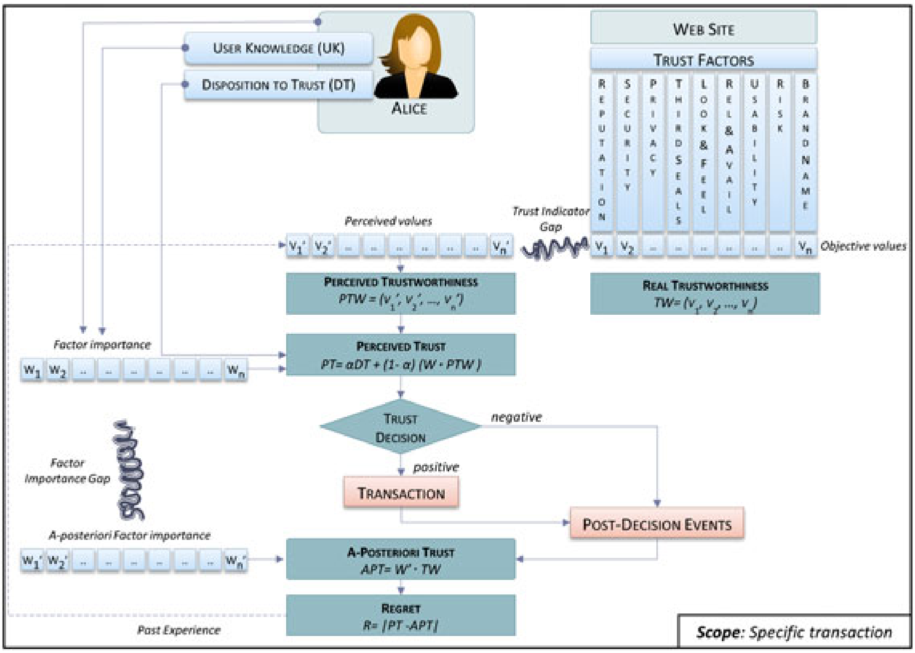

FIGURE 1. General trust perception model.

W for e-banking, e-commerce, e-health, and e-portfolio is defined with our user study and presented in Section 5. Perceived trust is formalized in Equation (2), where $\alpha \in [0, 1]$ is the relative importance of the two components.

$$PT = \alpha * DT + (1 - \alpha) * (W \bullet PTW) \qquad (2)$$

We believe users make trust decisions according to their perceived trust. For example, they might trust a website because it has a good design and great usability and they associate such characteristics with trust.

After a trust decision has been made, feelings of regret can arise both if the decision is positive (use the website to perform a transaction) or negative (do not use it). Both actions lead to postdecision outcomes that can be good (e.g., the product is delivered on time) or bad (e.g., the product has been delivered, but the user realizes her e-mail address is now available to advertising companies). These events enable the user to evaluate the a posteriori trust, that is, the level of trust she has after obtaining more information about the objective trustworthiness of the trustee. The user could realize, for example, that she did not give the right weight to privacy and that in the future, she should give more importance $\left(w_f'\right)$ to the fact that the website keeps personal data private, for example, by carefully reading a privacy policy or by using mechanisms that improve the privacy trust indicators (Costante et al. 2012). We refer to the gap between the importance of a factor before and after the trust decision as the factor importance gap.

We capture the user's regret as the difference between perceived trust and a posteriori trust. In formulas,

$$R = |PT - APT| \qquad (3)$$

To minimize regret, we need to make the user-perceived trust resemble the a posteriori trust as close as possible; that is, we need to reduce both the trust indicator gap and the factor importance gap.

The trust indicator gap can be reduced by diminishing the difference between v_f and v'_f; that is, trust indicators should be able to communicate to the user the objective value of a factor of trust. Let us consider the https padlock as trust indicator for the security factor. This indicator just says that the transaction channel is encrypted, meaning that, for example, a man in the middle attack cannot be easily performed. However, the padlock does not say that an attacker cannot enter the database of the website and access users' personal data (if those are not well protected) or that the certificate has not been compromised (e.g., the DigiNotar case[1]). A user that gives high importance to security, but evaluates it by the mere presence/absence of the padlock, can still regret his decision if her data are stolen. In this case, the main problem is that the padlock is insufficient as trust indicator for security because it does not communicate the security objective value. This is a clear case of the trust indicator gap.

On the other hand, let us assume there is a way to precisely measure the level of security offered by a website, for example, according to the results of penetration testing, and that a new indicator with such *security level* is shown to the user. If the user does not give high importance to security (w_{security} is very low), she will use the website even though it has poor security. If something goes wrong, for example, her credit card is stolen, the user will still experience regret. In this case, the problem is due to the factor importance gap; that is, the trustor gives a level of importance to a factor that is not confirmed by the postdecision events.

Because the understanding of the factor importance gap is the main focus of this article, we developed the user study presented in Section 4. With this study, we want to understand which factors have the higher impact on trust decisions. Also, the study aims at discovering whether it is possible to manipulate the *factor importance* by acting on the user's knowledge, for example, if the higher importance of the security factor corresponds to the higher knowledge (better understanding of security risks).

Understanding what happens after the trust decision is made, and in which situations users experience regret, requires a different user study, with the goal of understanding whether transactions and external events influence a posteriori trust and a posteriori factor importance. This study is part of our future work and thus out of the scope for this article.

Finally, recalling that our model focuses on the first interaction with a website, note that *past experience* is only accounted as a feedback line going from regret to perceived trustworthiness and impacting future trust decisions with the same website.

4. THE USER STUDY

According to our GTPM, to reach the overall goal of minimizing regret, it is necessary to reduce both the trust indicator gap and the factor importance gap. Because the focus of this article is on the factor importance gap, we carried out a user study with the main objectives of (i) understanding how the importance of a factor changes in four different domains, namely, e-health, e-commerce, e-banking, and e-portfolio; and (ii) understanding whether the factor's importance can be manipulated by acting on the user's knowledge. Understanding the importance of factors in the domains we analyzed provides interesting insights on which signals are important for the user to trust. This knowledge can help in the development of trust indicators that are more effective. For example, if the study reveals that users give poor importance to security, new security indicators (e.g., more visible, more

[1] http://www.itpro.co.uk/635833/certificate-authority-confirms-hack-after-gmail-attack

attractive, and effective) can be developed. On the other hand, if a relationship between user's knowledge and factors' importance exists, this could help in reducing the factor importance gap: Users do not need to have a bad experience before realizing they do not give the right importance to some factors (e.g., security and privacy) because it is sufficient to act on their knowledge. Thus, we carried out a user study that aims at testing the following hypotheses:

Hypothesis 1. The importance the same user gives to a factor w_f is different for different application domains.

Hypothesis 2. The importance of a factor w_f is correlated to the user's knowledge in the IT security field.

Hypothesis 3. The importance associated to privacy and security factors increases if users are trained and informed about privacy and security topics.

The user study is carried out by means of a questionnaire, which is fully described in the Supporting information. The questionnaire is composed of 10 questions, divided in three sections: one to gather demographic information about the respondents, one to evaluate their knowledge, and the last to measure the weight respondents associate to each factor of trust in different domains. Measuring the factor's weight distribution in other domains can be carried out by adapting question number 9 to reflect those domains.

The validity of the questionnaire has been confirmed by applying the content validity method (Lynn 1986). We asked a panel of experts from the TAS3 project Consortium[2] to review and rate each item (question) of the survey. The items rated as relevant remained untouched, while the others were deleted or adjusted according to the reviewers' feedback. A pilot study, monitoring five respondents while answering the questionnaire, was also performed. This helped in rephrasing unclear questions, verifying and eliminating the presence of bias, and adding details to terms seen as vague (e.g., quantifying *very often* to mean *at least once a month*). In the remainder of this section, we present the questionnaire, and we discuss the three different parts it is composed of, namely, the sample frame, the user's knowledge, and the factors' importance.

- *The sample frame*—The population of our survey is represented by users of e-services such as e-banking, e-commerce, e-portfolio, and e-health. The "Digital Report 2009" (Statistics Netherlands 2009) reveals that 89% of Dutch Internet users, aged 25–44 years, use e-banking services; that the typical online shopper is high educated, aged 25–44 years; that 19% (aged 12–74 years) use the Internet to look for a job; and that 30%, aged 55–64 years, surf the Web to look for health-related information. People with this characteristics can be considered samples of our population. The first part of the questionnaire contains questions about gender, age, educational level, and job position of the respondents, to verify whether the respondents group reflects the sampling frame of our study.
- *The user's knowledge*—Questions in this part of the questionnaire aim at capturing the user's knowledge in the IT security field. Users are asked to judge their own knowledge and ability on IT security-related topics, such as computer and Internet usage, privacy policies, and https. A four-item scale is used for the answers (each item has a numerical value associated): no knowledge (0.00), limited knowledge (0.33), good knowledge (0.66), and expert knowledge (1.00). The global UK for a user is computed as the average of the values associated to the user's answers.

[2] http://vds1628.sivit.org/tas3/

- *Factors' importance*—Another part of the questionnaire is the one aiming at measuring the weight users give to each factor of trust. This is carried out by verifying how much attention users dedicate to each of them. Respondents were presented with a service usage scenario in each of the settings (e-banking, e-commerce, e-portfolio, and e-health) and asked to answer questions assuming it was the first time they used the specific service. Questions were formulated in such a way as to verify the influence each factor has on perceived trust. To test the importance of the factor look&feel, for example, we ask the user whether the design aspects of the website (e.g., attractive colors), or the use of professional icons, influence his trust in it. Let Q_f be the set of questions used to measure the weight of the factor f. For each question $q \in Q_f$, respondents were allowed to choose among four optional answers: *never*, *almost never*, *very often*, and *always*; to each option is associated a numerical value: (in the order) 0.00, 0.33, 0.66, and 1.00. The value of the answer to the question q is denoted as v_q. To compute the weight w_f of each factor $f \in FS$, we averaged the answers given to each question q in Q_f.

With the same questionnaire, we carried out three different experiments; the results of which are described in the remainder of this article. The contributions of the experiments are as follows:

- *Experiment A* shows the results we obtained by asking randomly selected students and employees from the Eindhoven University Technology (TU/e) to fill in the questionnaire. This experiment, with a relatively large sample frame (335 respondents), is discussed in Section 5. These results extend earlier work presented in Costante, Hartog, and Petkovic (2011).
- *Experiment B* shows the results of a reliability test, proving the questionnaire we built is reliable, that is, it gives similar results with a similar sample (but different respondents) as described in Section 6.
- *Experiment C* shows the difference in users' responses when users are trained on the importance of security and privacy and when they actually use a service (in experiment A, the service is only described). Results and discussion of this experiment are provided in Section 7.

5. EXPERIMENT A: FACTOR IMPORTANCE BASICS

For this experiment, a Web interview methodology was used to ask subjects to take part in our research. The subjects were selected among employees and students of the TU/e. This sample frame cover the spectrum of knowledge because people with both low and high IT security expertise are part of the sample. The TU/e has about 6000 students and 4000 employees. To obtain enough responses for statistically significant results and account for lost e-mails and uncooperative subjects, about 1600 e-mails were sent to e-mail addresses selected from the TU/e internal mailing list. During the sample selection, the percentage of students (about 60% of the whole) and staff (about 40% of the whole) has been maintained. The subjects selected by our pseudo-random procedure received an e-mail and a reminder 1 week later, explaining the scope of our research and inviting them to participate by filling the online questionnaire. In the e-mail, they were also informed of the anonymous nature of the questionnaire.

A total of 335 valid responses were collected. Incomplete responses were ignored. Because the percentage of those was below 20%, this does not affect our final results (Mcdonald, Thurston, and Nelson 2000). To check the presence of common method variance, that is, the "variance attributable to the measurement method rather than to the constructs the measures represents" (Podsakoff et al. 2003), Harman's one-factor test was conducted. No single factor with covariance bigger than 50% emerged from the test, indicating that common method variance does not constitute a problem for our study.

The respondents' group is composed of 76% male and 24% female. Although this is representative for the population at the TU/e, this gender skew might represent a problem for the generalization of the results that should be taken into account. The age distribution, divided for gender, is presented in Figure 2. The graph shows the percentage of the males component (respectively females) falling in each of the age categories. In each category, men and women are almost equally represented, although there is a lack of respondents 65 years or older. This is mostly due to the community sampled and to the fact that retirees are not included. Figure 3 shows the educational level of our respondents, that is formed for 60% of students and 40% of employees, matching the sample frame.

5.1. Factors' Importance

The importance given to a factor of trust in different settings is presented in Figure 4 with a comparative graph. The graph is divided into three bands of equal width: low, medium, and high. We can notice that the factors' importance distribution is similar between e-commerce and e-banking and between e-portfolio and e-health. This intuition is confirmed by the Mann–Whitney test, which shows that the distribution of the factor's weight is not the same across the two groups of scenarios.

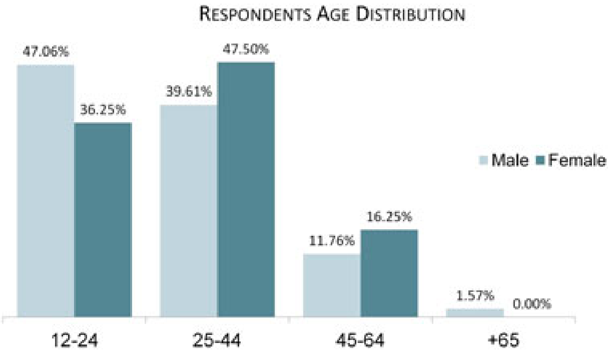

FIGURE 2. Respondents' age distribution, split by gender.

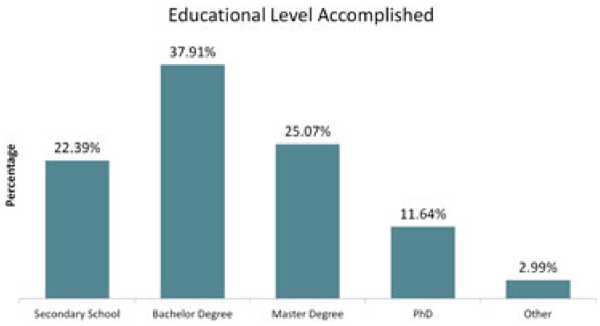

FIGURE 3. Respondents' educational level.

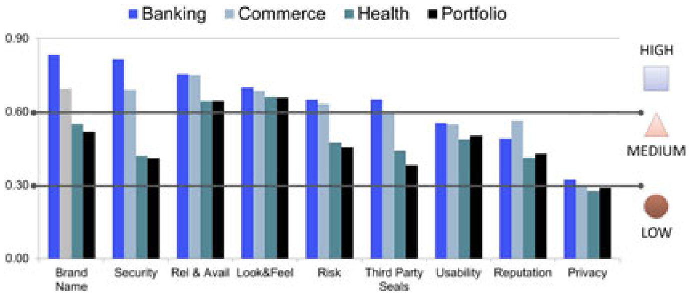

FIGURE 4. Factor's weight distribution in the different domains.

These results confirm Hypothesis 1; for e-banking and e-commerce, the importance of factors is significantly different from the importance for e-health and e-portfolio.

If we consider the importance each factor has in different domains, we can see that the reliability&availability and look&feel are the only factors in the high band for every scenario, suggesting that frequent error messages and crashes influence the perceived trust. Other highly important factors are brand name and security, followed by risk and third-party seals, but only for e-banking and e-commerce. The high importance of brand name in e-banking seems to support the idea that trust in traditional (offline) banking influences trust in the online banking (Lee et al. 2007).

The weight given to security, risk, and third-party seals significantly drops in the e-health and e-portfolio scenarios. Given the sensitiveness of the data collected in such domains, it is a strong recommendation to stress the importance of such factors to the users, for example, by improving the impact of the relative indicators. The motivation behind the drop of the weight given to the risk factor may be because in these scenarios, the risk (in terms of money loss) is less tangible than in the others. Also, note that e-health and e-portfolio are still not well-known services: 15.8% of our respondents had previously used, at least one time, e-health services, while e-portfolio services had been used by only 1.5% of our sample (vs. the 96.7% of e-banking and 71.9% of e-commerce). This may also explain why third-party seals are not important: Users probably do not know what kind of seals to expect from these new upcoming services.

The factors usability, reputation, and privacy show no considerable differences among scenarios; only the reputation is slightly higher in e-commerce probably because it is the domain with the highest presence of automatic reputation systems (e.g., eBay). For the other scenarios, it seems that users do not really look for external opinions: 59% of them said they never (or almost never) verify the reputation of an e-banking, and 45% does not bother to ask their friends about what kind of experience they had with it. This can be explained by the fact that users do not like to manually collect and evaluate feedback on their own, but not necessary that they would not like to use automatic systems providing them with the reputation of the service (a fact confirmed by the success of reputation systems such as Tripadvisor[3]). Another reason for the low importance given to reputation in e-banking can be that users already know the brand and base their online trust on this; thus, they do not have the need to check reputation.

The importance of the factor privacy is the lowest in each scenario. Note that we measured the weight of privacy by asking whether or not users read the privacy policy stated by a website; that is, privacy policy has been considered as the privacy indicator. We think

[3] http://www.tripadvisor.com/

the low weight of privacy in this case is a typical example of trust indicator gap: The fact that few respondents are interested in reading the privacy policy of a website does not necessarily means users are not interested in their privacy but, most probably, that privacy policies, as main current *privacy indicators*, are not enough to capture the real privacy value.

The main take-home message of these results is that reliability&availability and look&feel are the factors that impact trust perception the most in all the domains we considered. To avoid that fraudulent and malicious website manage to be trusted by end users by "appearing" trustworthy, the impact that other factors, such as security and privacy, have on trust perception has to be improved. We believe this can happen by (i) educating end users, for example, by increasing their knowledge in security risks; and (ii) improving trust indicators. The first of the two hypothesis is tested in the following experiment.

5.2. User's Knowledge

To verify Hypothesis 2, it is necessary to first measure the user's knowledge and check whether there is a correlation with the weight given to specific factors. To measure the user's knowledge (UK), we asked the users to answer questions related to their expertise on IT security topics, as explained in Section 4. Cronbach's alpha test was conducted to calculate the reliability of the scale. The item–total correlation is above 0.5 for each item (values above 0.3 are acceptable), and the Cronbach's alpha value, for all the items we used to build UK, is 0.9, proving the reliability of our scale. UK is the average of the value associated to each given answer. The minimum registered value for UK (ranging in [0,1]) is 0.07, while the maximum is 0.87.

The graph in Figure 5, obtained using a clustering technique to classify the users according to their knowledge, shows that an increase in knowledge level clearly increases the importance associated to the factors brand name, security, risk, and privacy. This graph refers to the e-commerce domain, but the trend is similar in the other domains as can be seen from the correlation coefficients shown in Table 2. The table gives the correlation analysis between the importance of the factors and the user's class of knowledge. We used Spearman's nonparametric correlation test because the normal distribution assumption was not verified by our sample. Note that there is a positive correlation between the user's knowledge and the importance of the factors security and privacy in all the domains. This suggests that a user with higher IT security knowledge will give more importance to security and privacy while making trust decisions. The positive correlation also exists for brand name and risk in the e-commerce and e-banking scenarios. The results presented in this table are complementary to those shown in Costante et al. (2011): The main difference is that here the value for the factor importance is absolute and not relative (no normalization has been applied).

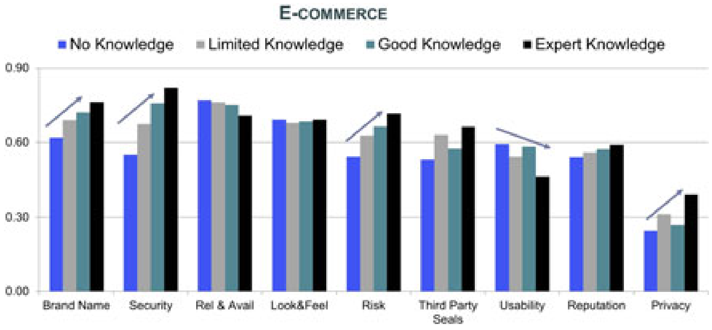

FIGURE 5. Factor's weight in the e-commerce domain, by class of knowledge.

TABLE 2. Spearman's Correlation Test.

	e-banking	e-commerce	e-health	e-portfolio
Security	0.292**	0.278**	0.150**	0.219**
Privacy	0.142**	0.128*	0.183**	0.221*
Brand name	0.218**	0.146**	0.061	0.097
Risk	0.171**	0.192**	0.045	0.102
Third-party seals	0.154**	0.102	0.032	0.074
Usability	−0.091	−0.119**	−0.064	−0.076
Reputation	−0.015	0.088	0.099	0.080
Reliability&availability	−0.026	−0.092	−0.067	−0.099
Look&feel	−0.009	−0.013	−0.009	−0.019

*Correlation is significant with $p < 0.05$.
**Correlation is significant with $p < 0.01$.

6. EXPERIMENT B: RELIABILITY OF THE QUESTIONNAIRE

Ideally, each survey question should be clear, unambiguous, mean the same thing to everyone, and provide a reliable measurement (of the importance of a factor, the knowledge of a user, etc.).

Reliability of measurement, that is, the extent to which repeatedly measuring the same property produces the same results, can be validated by repeating the same measurement on the same subject at different moments. The time between measurements should not be too small to prevent the measurement being influenced by memory and not too large to avoid changes in the measured quantity, which may change over time. Because the respondents in our settings are anonymous, it is difficult to carry out a reliability test in this way. To avoid this problem, but still provide an indication of the reliability of the questionnaire, we performed the test by asking a small group of new respondents to fill in the questionnaire and by comparing the results we obtained in this way with the ones of the online survey.

The new group consisted of 12 IT experts, gathered in a panel for the evaluation of the TAS3 project. Because the panel members were selected on the basis of their high expertise in IT and security, they all fall in the class of *expert* knowledge. We compared the answers of these certified experts with the answers given by the users classified as expert in the online study.

Figure 6 reports the results of the comparison, based on the seven valid responses collected from the expert panel. For each scenario, we present the difference among the weight given to the factors by the two groups. The factors with a circle are the ones for which no statistically significant similarity between the responses on the two groups was found (based on the Mann–Whitney test for independent samples).

Most of the factors show similarity; that is, the test revealed no significant difference in mean scores. Exceptions are look&feel in the e-banking and third-party seals in both e-banking and e-commerce, to which the panel experts give considerably less importance, and reliability&availability in e-health, to which the experts of the panel give considerably higher importance. Finally, the panel members give a high importance to security in all setting. Because the panel members are all IT experts facing security problems on a daily basis, security cannot be less than a top priority to them. Moreover, because the experts from the panel will have even more expertise than the average expert class user from the survey, this higher importance of security confirms the trend expressed in Table 2 (higher

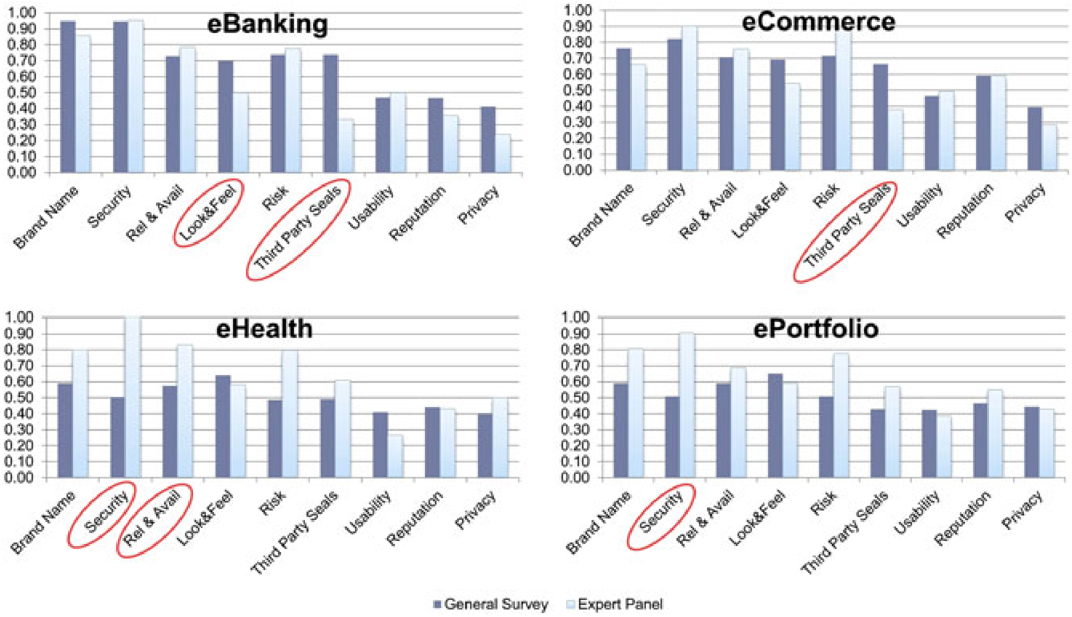

FIGURE 6. Comparison of the results obtained in the online survey and during the expert panel. The importance of factors with a circle differs between the two groups.

knowledge corresponds to higher importance of security). In all, we can conclude that this experiment supports that the questionnaire is a reliable measurement tool.

7. EXPERIMENT C: THE IMPACT OF USER COACHING

The results presented in Section 5 give us two main conclusions: (i) the importance of trust factors is different in different domains and (ii) higher user's knowledge corresponds to higher importance associated to security and privacy. In the experiment described in this section, we demonstrate that if users are coached about the importance of security and privacy, then the weight of those factors will increase. To verify this, we asked a new group of respondents to fill in the questionnaire after they have been trained and they have used a specific e-service. While in the online survey respondents were only provided with a description of the scenario, in this setting, we ask them to use an e-service (specifically an e-portfolio service) before completing the survey. The respondents were recruited during a series of workshops, which have been made in the context of the TAS3 project. During the workshop, the participants were coached, guided, and monitored during their activities. At the end of the live session (they were asked to use the service and to perform some tasks), they were provided with the questionnaire, which was slightly modified to fit the context. An additional question was also added to the questionnaire giving the following main changes:

- The questions regarding the factor importance are only related to the e-portfolio scenario.
- The questions are rephrased to reflect the fact that respondents fill in the questionnaire after experiencing a live session of an e-portfolio service ("did you" instead of "would you").
- A new question for the privacy factor has been added. Because we believe the question used before ("Would you read the privacy policy stated by the website?") does not assess the importance of privacy but the validity of privacy policies as privacy indicators, we

rephrased it by asking whether "the way the website manages your personal data influence your trust in it." The previous question is maintained so we can compare the weight of privacy in the two cases.

A total number of 17 completed surveys were collected during the workshops. Although this number of responses is not enough to provide statistically relevant results, they can be used to confirm or deny the results and our intuitions coming from the analysis of the online survey. Figures 7 and 8 show the differences between the participants to the survey and the respondents to the workshops. Note that the first group of participants are on average older (the workshop focused on graduated professionals while the survey population included many students) and with a higher educational level (50% of the workshops' respondents has at least a master's degree). The respondents frame consist for 75% of employees and for 25% of employers. Applying the Mann–Whitney test for independent samples does not show any relevant difference between the average knowledge in the two groups. However, as shown in Figure 9, the factor's weight changes in a significant way for security, reputation, usability, and reliability&availability. The fact that security and reputation are more important is likely due to the training that the participants received; special focus is given during the whole workshop to the secure management of personal data and a reputation system is in place in the demo service. During the development of the e-portfolio service, a large effort was made to make it easy to use, which may contribute to the higher importance given to the

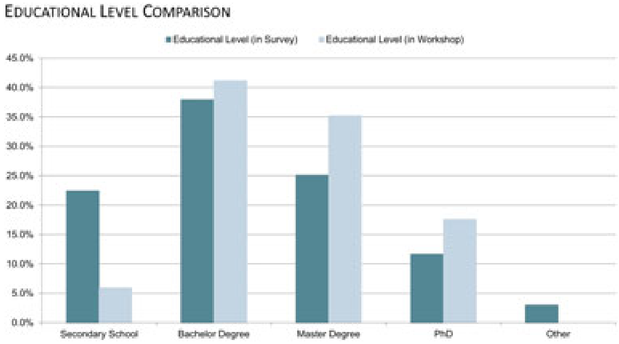

FIGURE 7. Educational level comparison between the respondents to the survey (dark color) and to the workshop (light color).

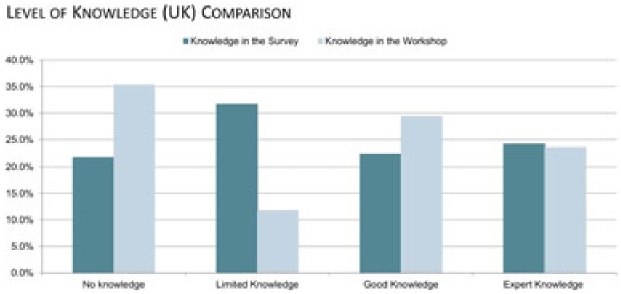

FIGURE 8. Level of knowledge comparison between the respondents to the survey (dark color) and to the workshop (light color).

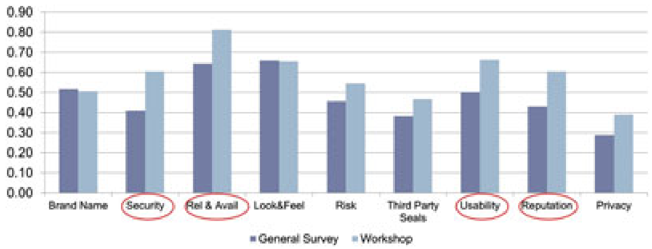

FIGURE 9. Comparison between the importance associated to each factor of trust in the survey (dark color) and in the workshop (light color). The circle means the average is statistically significantly different according to the Mann–Whitney test.

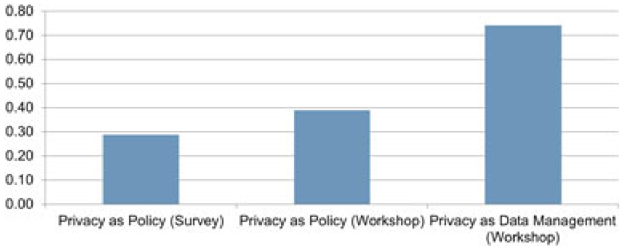

FIGURE 10. The impact of computing the weight of privacy in two different methods: as related to privacy policy or to the importance of personal data management.

usability factor. The other factors, when compared to the results obtained with the survey, show only small variation, confirming the results of the survey and indicating that these results are generalizable to other populations.

Another relevant result obtained during this experiment is the one presented in Figure 10: Here, we compare the importance associated to the privacy factor, when computed in two different ways: (i) as the importance given to privacy policies or (ii) as the importance associated with the way personal data are managed. The results clearly confirm our intuition: The importance of privacy measured in the survey was consistently lower, not because users do not consider privacy important but because they do not consider it worthwhile to read privacy policies. The main message of this result is that users do care about privacy (the privacy factor is the second most important factor if its weight is computed using the second question), but privacy policies are not the right trust indicator.

8. CONCLUSIONS

In this article, we present a GTPM describing the way users make trust decisions and what can be done to help the user in making trust decisions that minimize regret. We suggest that to minimize regret, both the trust indicators gap and the factor importance gap need to be reduced. With our user study, we demonstrate that factors of trust have different importance in different scenarios and that there is a positive correlation between user's knowledge and the weight given to security and privacy. Thus, the factor importance gap can be reduced by educating the user on the importance security and privacy have in making trust decisions. Our experiments also demonstrate the reliability of our questionnaire that can be used to define the factor's weight distribution in other domains.

We have also looked at the trust indicators gap, and we suggest that improving the way trust indicators communicate the value of trustworthiness can reduce such gaps. As future work, we plan to carry out a different user study, aiming at understanding whether different trust indicators (which help to reduce the trust indicator gap), for example, for privacy or security, make a real difference in the way users make trust decisions and thus reduce the overall regret.

ACKNOWLEDGMENTS

This work has been partially funded by the THeCS project in the Dutch National COMMIT program and by the EU FP7 project AU2EU.

REFERENCES

ATOYAN, H., J. R. DUQUET, and J. M. ROBERT. 2006. Trust in new decision aid systems. *In* Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine. ACM Press: New York, pp. 115–122.

AZAM, A., P. F. QIANG, and M. I. ABDULLAH. 2012. Consumers' e-commerce acceptance model: antecedents of trust and satisfaction constructs. *In* 2012 IEEE Business, Engineering & Industrial Applications Colloquium (BEIAC). IEEE: New York, pp. 371–376.

BELDAD, A., M. DE JONG, and M. STEEHOUDER. 2010. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, **26**(5): 857–869.

CAMP, L. J. 2003. Designing for trust. Trust, Reputation, and Security: Theories and Practice, **35**(3): 203–209.

CHEUNG, C. M. K., and M. K. O. LEE. 2003. An integrative model of consumer trust in internet shopping. *In* European Conference on Information Systems (ECIS), Naples, Italy.

CHRISTIE, R., and F. L. GEIS. 1970. Studies in Machiavellianism. Academic Press: Waltham, MA.

COLQUITT, J. A., B. A. SCOTT, and J. A. LEPINE. 2007. Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. The Journal of Applied Psychology, **92**(4): 909–927.

CORRITORE, C. L., B. KRACHER, and S. WIEDENBECK. 2003. On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies, **58**(6): 737–758.

COSTANTE, E., J. D. HARTOG, and M. PETKOVIC. 2011. On-line trust perception: what really matters. *In* 1st Workshop on Socio-technical Aspects in Security and Trust (STAST), Milan, Italy, pp. 52–59.

COSTANTE, E., Y. SUN, J. DEN HARTOG, and M. PETKOVIC. 2012. A machine learning solution to assess privacy policy completeness. *In* 10th Annual ACM Workshop on Privacy in the Electronic Society. ACM Press: New York.

DEUTSCH, M. 1962. Cooperation and trust: some theoretical notes. *In* Nebraska Symposium on Motivation. *Edited by* M. R. JONES. University of Nebraska Press: Lincoln, pp. 275–320.

ERMISCH, J., D. GAMBETTA, H. LAURIE, T. SIEDLER, and S. C. NOAH UHRIG. 2009. Measuring people's trust. Journal of the Royal Statistical Society: Series A (Statistics in Society), **172**(4): 749–769.

ETALLE, S., J. DEN HARTOG, and S. P. MARSH. 2007. Trust and punishment. *In* Proceedings of the First International Conference on Autonomic Computing and Communication Systems, Rome, Italy, pp. 1–6.

EVERARD, A., and D. F. GALLETTA. 2003. Effect of presentation flaws on users perception of quality of on-line stores web sites: is it perception that really counts? *In* Second Annual Workshop on HCI Research, Seattle, WA, p. 60.

FAJA, S. 2006. E-health : an exploratory study of trust building elements in behavioral health web sites. Journal of Information Science and Technology, **3**(1): 385–390.

FESTINGER, L. 1957. A Theory of Cognitive Dissonance. Stanford University Press: Palo Alto, CA.

FLINN, S., and J. LUMSDEN. 2005. User perceptions of privacy and security on the web. *In* The Third Annual Conference on Privacy, Security and Trust, St. Andrews, Canada, pp. 14–26.

FRIEDMAN, B., P. H. KHAN, and D. C. HOWE. 2000. Trust online. Communications of the ACM, **43**(12): 34–40.

FRUHLING, A. L., and S. M. LEE. 2006. The influence of user interface usability on rural consumers' trust of e-health services. International Journal of Electronic Healthcare, **2**(4): 305–321.

GAMBETTA, D. 2000. Can we trust trust. *In* Trust: making and breaking cooperative relations. Department of Sociology, University of Oxford: Oxford, UK, 213–237. Available at: http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.

GANESAN, S. 1994. Determinants of long-term orientation in buyer-seller relationships. Journal of Marketing, **58**(2): 1–19.

HALPERN, D. F. 1989. Thought and Knowledge: An Introduction to Critical Thinking. Lawrence Erlbaum Associates, Inc: Mahwah, NJ.

HOFFMAN, D. L., T. P. NOVAK, and M. PERALTA. 1999. Building consumer trust online. Communications of the ACM, **42**(4): 80–85.

HOFFMAN, L. J., K. LAWSON-JENKINS, and J. BLUM. 2006. Trust beyond security. Communications of the ACM, **49**(7): 94–101.

HSU, C. J. 2008. Dominant factors for online trust. *In* International Conference on Cyberworlds 2008. IEEE: New York, pp. 165–172.

JIANG, J. C., C. A. CHEN, and C. C. WANG. 2008. Knowledge and trust in e-consumers' online shopping behavior. *In* 2008 International Symposium on Electronic Commerce and Security. IEEE: New York, pp. 652–656.

JOHNSON-GEORGE, C., and W. C. SWAP. 1982. Measurement of specific interpersonal trust: construction and validation of a scale to assess trust in a specific other. Journal of Personality and Social Psychology, **43**(6): 1306.

JONES, K. 2008. Trust in consumer-to-consumer electronic commerce. Information & Management, **45**(2): 88–95.

JOSANG, A., R. ISMAIL, and C. BOYD. 2007. A survey of trust and reputation systems for online service provision. Decision Support Systems, **43**(2): 618–644.

KINI, A. D., and J. CHOOBINEH. 1998. Trust in electronic commerce: definition and theoretical considerations. *In* Proceedings of the Thirty-First Hawaii International Conference on System Sciences. IEEE: New York, pp. 51–61.

KINI, A. D., and J. CHOOBINEH. 2000. An empirical evaluation of the factors affecting trust in web banking systems. *In* Proceedings of the Sixth Americas Conference on Information Systems, Long Beach, CA, pp. 185–191.

LEE, J. D., and K. A. SEE. 2004. Trust in automation: designing for appropriate reliance. Human Factors, **46**(1): 50–80.

LEE, K. C., I. KANG, and D. H. MCKNIGHT. 2007. Transfer from offline trust to key online perceptions: an empirical study. IEEE Transactions on Engineering Management, **54**(4): 729–741.

LI, F., D. PIEKOWSKI, A. VAN MOORSEL, and C. SMITH. 2012. A holistic framework for trust in online transactions. International Journal of Management Reviews, **14**(1): 85–103.

LYNN, M. R. 1986. Determination and quantification of content validity. Nursing Research, **35**(6): 382.

MADSEN, M., and S. GREGOR. 2000. Measuring human-computer trust. *In* 11th Australasian Conference on Information Systems, Brisbane, Australia, pp. 6–18.

MARSH, S., and P. BRIGGS. 2009. Examining trust, forgiveness and regret as computational concepts. *In* Computing with Social Trust. *Edited by* J. GOLBECK. Springer: London, pp. 9–43.

MARSH, S. P. 1994. Formalising trust as a computational concept, Ph.D. thesis, University of Stirling, Stirling, UK.

MAYER, R. C., J. H. DAVIS, and F. D. SCHOORMAN. 1995. An integrative model of organizational trust. Academy of Management Review, **20**(3): 709–734.

MCDONALD, R. A., P. W. THURSTON, and M. R. NELSON. 2000. A Monte Carlo study of missing item methods. Organizational Research Methods, **3**(1): 71–92.

MCKNIGHT, D. H., and N. L. CHERVANY. 2001. What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. International Journal of Electronic Commerce, **6**(2): 35–59.

MCKNIGHT, D. H., V. CHOUDHURY, and C. KACMAR. 2000. Trust in e-commerce vendors: a two-stage model. *In* Proceedings of the Twenty First International Conference on Information Systems, Brisbane, Australia, pp. 532–536.

MCKNIGHT, D. H., V. CHOUDHURY, and C. KACMAR. 2002. Developing and validating trust measures for e-commerce: an integrative typology. Information Systems Research, **13**(3): 334–359.

MCKNIGHT, D. H., L. L. CUMMINGS, and N. L. CHERVANY. 1998. Initial trust formation in new organizational relationships. The Academy of Management Review, **23**(3): 473–490.

MCKNIGHT, D. H., C. J. KACMAR, and V. CHOUDHURY. 2004. Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business. Electronic Markets, **14**(3): 252–266.

MUI, L., M. MOHTASHEMI, and A. HALBERSTADT. 2002. A computational model of trust and reputation. *In* Annual Hawaii International Conference on System Sciences, Big Island, HI, pp. 2431–2439.

MUIR, B. M. 1987. Trust Between Humans and Machines, and the Design of Decision Aids, Vol. 27. Elsevier: Amsterdam, the Netherlands.

O'DONOVAN, J., and B. SMYTH. 2005. Trust in recommender systems. *In* Proceedings of the 10th International Conference on Intelligent User Interfaces. ACM Press: New York, pp. 167–174.

PODSAKOFF, P. M., S. B. MACKENZIE, J. Y. LEE, and N. P. PODSAKOFF. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology, **88**(5): 879–903.

ROTTER, J. B. 1971. Generalized expectancies for interpersonal trust. American Psychologist, **26**(5): 443.

ROTTER, J. B. 1980. Interpersonal trust, trustworthiness, and gullibility. American Psychologist, **35**(1): 1–7.

RUOHOMAA, S., and L. KUTVONEN. 2005. Trust management survey. *In* Procedings of the iTrust 3rd International Conference on Trust Management, Rocquencourt, France, pp. 77–92.

SAN-MARTÍN, S., and C. CAMARERO. 2012. A cross-national study on online consumer perceptions, trust, and loyalty. Journal of Organizational Computing and Electronic Commerce, **22**(1): 64–86.

SILLENCE, E., P. BRIGGS, P. R. HARRIS, and L. FISHWICK. 2007. Developing trust practices for e-health. *In* Trust in E-services: Technologies, Practices and Challenges. IGI Global: Hershey, PA, pp. 235–258.

STATISTICS NETHERLANDS. 2009. The digital economy 2009. Available at: http://www.cbs.nl/NR/rdonlyres/E4311D6B-6BE6-4996-A4AB-804FC0A07A4C/0/2009p38pub.pdf.

SUH, B., and I. HAN. 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce, **7**(3): 135–161.

YOUSAFZAI, S. Y., J. G. PALLISTER, and G. R. FOXALL. 2003. A proposed model of e-trust for electronic banking. Technovation, **23**(11): 847–860.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of this article at the publisher's website.