

Factors Influencing the Perception of Website Privacy Trustworthiness and Users' Purchasing Intentions: The Behavioral Economics Perspective

Alisa Frik¹ and Luigi Mittone²

¹ University of California, International Computer Science Institute, Berkeley (CA), USA, afrik@icsi.berkeley.edu.

² University of Trento, Department of Economics and Management, Trento, Italy, luigi.mittone@unitn.it.

Received 25 October 2017; received in revised form 15 October 2018; accepted 17 October 2018

Abstract

In this study, we identified the factors that influence consumer purchasing intentions and their perceptions of the trustworthiness of the privacy-related practices of e-commerce websites. We produced a list of website attributes that represent these factors in a series of focus groups. Then we constructed and validated a research model from an online survey of 117 adult participants. We found that security, privacy (including awareness, information collection, and control), and reputation (including company background and consumer reviews) have a strong effect on trust and willingness to purchase, while website quality plays only a marginal role. Although the perception of trustworthiness and purchasing intention were positively correlated, in some cases participants were more willing to buy from a website that they judged as untrustworthy with regard to privacy. We investigated how behavioral biases and decision-making heuristics may explain the discrepancy between perception and behavioral intention. Finally, we determined which website attributes and individual characteristics impact customer's trust and willingness to buy.

Keywords: Online privacy, Security, Trust, Survey, Empirical model, Behavioral biases and heuristics

1 Introduction

With the development of the World Wide Web and mobile technologies, electronic commerce (e-commerce) has become the main driver of the digital economy. In 2017, the e-commerce market achieved US\$409.2 million revenue in the U.S. [130]. In Europe, 324 million online shoppers generated €329.6 billion e-commerce revenue in 2017 [34]. Despite these figures, the full potential of e-commerce has not yet been reached. In 2017 half of the European adult population did not shop online [34]. Therefore, an investigation of the factors that may help e-commerce to reach its full potential would be a useful and relevant exercise.

E-commerce generates extensive flows of information that include, but are not limited to, names, credit card details, and email and shipping addresses. Together with the benefits and reduced costs for vendors, e-commerce implies risks for consumers that range from nearly harmless to significantly harmful, including the tracking of online behavior and location, intrusive marketing, and data breaches. As a result, online shopping often triggers privacy concerns, which in turn negatively affect the behavioral intention of some consumers [32], [136]. The failure to address privacy concerns has inhibited online shopping acceptance [48] and has led to multi-million-dollar losses in online sales [105].

Often the risks and unfair data use practices cannot be detected beforehand, and sometimes even after the transaction has happened. Hence, engagement in economic exchanges requires trust [141]. According to social exchange theory, trust is one of the main business assets [155], [94]. Because e-commerce involves virtual buyer-seller interactions rather than real interactions, trust plays an even more crucial role in the online shopping context than in actual stores, and has therefore become an important factor driving online purchasing intentions [11]-[13], [26], [30], [46], [52], [65], [74], [77], [116], [135]. A lack of trust often prevents customers from completing e-commerce transactions [74], [78]. In contrast, consumers are more likely to accept the perception of vulnerability when the website is trustworthy [112]. A high level of trust propensity increases customer satisfaction and positively influences their willingness to re-purchase [21], which may further improve online sales. The provision of privacy-friendly services may contribute to the development of a good reputation and trust as one of the core elements mitigating the concerns related to online shopping [27], [28]. Because users often judge the trustworthiness of a commercial website based on an inspection of its surface elements [76], it is important to understand the cues that influence a user's beliefs about the credibility of a company, and how these beliefs affect their willingness to buy from the vendor's website.

The aim of this study was to investigate how consumer perceptions of company trustworthiness have developed with respect to privacy and the impact of these perceptions on subsequent purchasing intentions. We present a model that maps the influence of various website attributes and business practices on consumer perception of company trustworthiness with respect to privacy, and on consumer purchasing intentions. In contrast to other studies, we focused on trust in the particular domain of online information privacy rather than general trust in the company. Using focus groups, we calibrated a model and then empirically tested it in an online survey of 117 adult participants. We found that privacy (including awareness, information collection, and control practices), security, and reputation (including the company background and consumer feedback) have a strong effect on trust and willingness to buy, while website quality plays only a marginal role. Although the perception of trustworthiness and purchasing intention were positively correlated, in some cases participants were willing to purchase from websites that they considered to be untrustworthy. Moreover, we determined which factors, website attributes, and individual characteristics had the strongest effect on hindering or advancing trust and willingness to buy among consumers. Finally, we considered the mechanisms, behavioral biases, and cognitive heuristics, through which the proposed factors influence trust, to better understand how to de-bias the decision-making process and improve the accuracy of user judgments.

The paper is organized as follows. Section 2 reviews the related literature, and presents a research model and hypotheses. Section 3 describes the methodology. Section 4 provides an analysis of the results and a test of the hypotheses. Section 5 discusses the results, limitations, and need for future work, and section 6 summarizes the findings and provides a conclusion.

2 Previous Studies and Proposed Research Model

In this section, we present the main definitions and concepts used in the study, review previous work, and propose our research model and hypotheses.

2.1 Definitions and Concepts

In this study, we focused on business-to-consumer e-commerce, which is defined as electronic business transactions conducted by a company electronically through its website directly to the consumer [24]. Specifically, we considered online retailers, which represent the storefronts of independent merchants (*i.e.*, online versions of traditional stores) [121], rather than on e-marketplaces, which aggregate the products from multiple sellers [59]. This enabled us to avoid the potential confounder between the perception of trustworthiness toward a product manufacturer and a website selling their product. We defined the *perception of trustworthiness with respect to privacy* as a consumer's beliefs about the characteristics of a company and its website that indicate the level of trust

in an online vendor that is not engaged in opportunistic behavior such as selling, sharing with third parties without consent, or other misuse of a consumer's personal information. Our definition of the perception of trustworthiness was similar to the notion of privacy assurance in [91], based on [76], [124]. They define privacy assurance as an "attitude that reflects how strongly a customer feels that their private information will be kept private by a website with which the customer is interacting" [91] p. 756. Trust is expected to positively influence an individual's intention to conduct online transactions [118]. *Online purchase intention* is defined as a situation where a consumer is willing and intends to make an online transaction [110]. Although one may argue that willingness to buy a product does not always translate into an actual purchase, the theory of reasoned action [7], [38] and theory of planned behavior [5], [6] states that transaction intentions are positively correlated with actual transaction behavior. Therefore, we believe that purchasing intention is an acceptable and reliable measurement of behavioral intent in our study.

2.2 Research Model and Hypotheses

A number of models have been developed to understand what influences a user's online trust [11], [26]. However, most models view trust as a general concept, while our study focused on the privacy-related context of trust. The model most relevant to the scope of our study is the privacy-trust-behavioral intention model used in [90]. The empirical tests of this model showed that privacy has a strong impact on a user's trust in e-commerce, which in turn influences their behavioral intentions. However, our model differs from the one in [90] in several ways. First, we extended the number of privacy dimensions by including information collection, control, and awareness [95] instead of following the categorization of Fair Information Practices [45]. Second, we separated security and privacy features. Third, we included website quality and company reputation, both of which have also been shown to predict consumer trust. Finally, we used willingness to make a purchase as a behavioral intention measurement, because it has the most direct economic impact compared to website visits, recommendations, or positive remarks about a website, which were used in [90].

To estimate the trustworthiness of transactional partners, individuals rely on three main criteria: reputation, performance, and appearance [133]. Reputation is viewed as a retrospective of past behavior, performance as an overview of actual practices and present conduct, and appearance as self-presentation. Following this taxonomy, we included the four dimensions of antecedents of trust in our model: *privacy*, *security* (performance criterion), *website quality* (visual appearance criterion), and *reputation* (reputation criterion). We hypothesized that these factors, moderated by individual characteristics, influence the perceived privacy trustworthiness of the websites and the willingness of consumers to purchase from such websites. Figure 1 shows our research model. We will describe each of the factors and sub-constructs that comprise them in the next section. We will also discuss the related hypotheses.

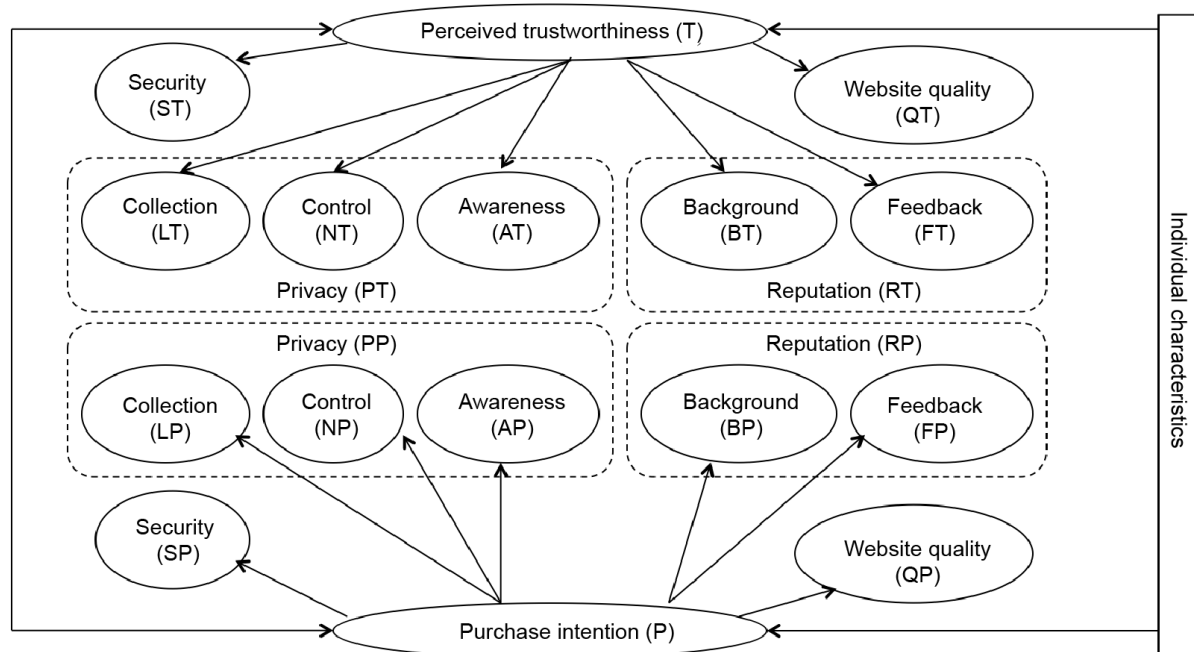


Figure 1: Research model

2.2.1 Construct Level

Appendix A presents the list of questionnaire items that we used in our model to construct the factors that affected perceived privacy trustworthiness (T) and purchasing intentions (P). We describe those factors below. (In the abbreviations of constructs the first letter represents the factor. For instance, Q stands for Quality, A stands for Awareness), and the second letter represents whether the impact of this factor was assessed with respect to perceived trustworthiness (T) or purchasing intention (P) based on the survey questions. See details in section 3.2.)

Privacy Most trust models comprise privacy and security as the main cogwheels of online shopping acceptance [73], antecedents of trust [74], [116], and the establishment of a reliable long-term loyal relationship between companies and customers. For example, privacy assurances decrease privacy concerns and increase trust [86], [89], [90], [98], [109], [154] and behavioral intentions [63], [99], [113], [139]. However, some studies have shown an insignificant [103], [148] and occasionally even negative [9] effect of privacy policies on trust. Bansal *et al.* [10] attribute the contradictory nature of the empirical evidence to the lack of attention given to the level of privacy concerns as a factor mediating the effectiveness of privacy assurance statements. In our model, we included a measure of the general level of privacy concerns as a control variable. We predicted a significant influence of privacy-related practices on the perception of trustworthiness and purchasing intention:

H1a: Privacy-related practices have a significant effect on the perceived trustworthiness.

H1b: Privacy-related practices have a significant effect on purchasing intention.

In the categorization of privacy factors, we followed the dimensions of the Internet Users' Information Privacy Concerns (IUIPC) scale [95], and therefore included collection, control, and awareness sub-constructs in the privacy construct. *Collection* considers the extent to which an individual is concerned about the amount of their personal data in the possession of others in relation to the perceived benefits and values of such sharing. *Control* is related to a consumer's freedom of choice and ability to actively control (e.g., approve, modify, opt-out, delete) their personal information [18]. Finally, *awareness* indicates passive control over personal information through an understanding and awareness of privacy-related organizational practices. It is related to transparency in the collection, storage, use, and sharing of the information.

Security Security perceptions indicate the extent of an individual's beliefs in a website's reliability against security threats [102]. Some studies include security features in the notion of privacy [90] or even use privacy and security interchangeably [122]. However, Bélanger *et al.* [12] found that security features had a greater effect on trust than privacy because security is a more concrete concept, which is easier to understand for users. Carlos Roca *et al.* [17] argued that due to their better familiarity with security technologies, relative ease of recognition of key features (e.g., certificates, encryption keys, password-composition requirements), and the inclusion of some privacy guarantees in security assurance, the perception of privacy has a smaller impact on the trust of experienced users compared to inexperienced users. Therefore, in our study we separated the impact of privacy from the impact of security features, and controlled for the technical and Internet experience of the participants.

Security issues are a serious concern among online shoppers [120], [140]. A number of studies have included security system assurances as antecedents of trust perception [137], [116] and purchasing intention [102].

H2a: Security features have a significant effect on the perceived trustworthiness.

H2b: Security features have a significant effect on purchasing intention.

Website quality Although privacy and security policies, and seals are designed to directly influence privacy perceptions, they have been shown to be more effective when combined with other, more peripheral, cues, such as brand image and website quality [91], [98]. The appeal of a website's design is related to the visual presentation and structure of the website [10], which is indicative of website quality [152] and company expertise and professionalism, and develops trusting beliefs [31], [96], [146]. Egger [36] assumed that a consumer's trust in online business starts to form even before any online interaction has taken place. Trusting beliefs are positively correlated with the absence of errors on a website [11], accurate, current, and complete information [75], and correct spelling, grammar, and syntax [80]. Because users tend to believe that online advertising follows the norms of the websites containing a particular advert [131], we included the presence of suspicious banner adverts as a factor influencing the assessment of website quality.

Another reason why cues demonstrating website quality are important antecedents of the perception of trustworthiness is explained by signaling theory. Poor website quality or slow performance does not enforce a user's belief that the company behind that website will do any better in privacy and security protection, or in delivering services to customers [10], [127]. On the other hand, positive beliefs about a company's reliability, integrity, and professionalism are also related to the amount of time, effort, and money that the company has invested in the development and maintenance of a high-quality website, which is expected to impact other organizational practices including those related to privacy and security [33], [122], [125]. Therefore, we predicted that:

H3a: Low website's quality will negatively affect the user's perceived trustworthiness.

H3b: Low website's quality will negatively affect the user's purchasing intention.

Firm's reputation Reputation (or vendor image), as a result of social evaluation and judgment, is a significant factor influencing the perception of a website's trustworthiness [111], [128], [137], [74], [101] and purchasing intention [145]. The reputation of the company may serve as heuristic, signaling the reliability [46], [52] and quality [33] of the firm.

H4a: A good reputation will positively affect the user's perceived trustworthiness.

H4b: A good reputation will positively affect the user's purchasing intention.

In our study, the reputation construct was comprised of two sub-constructs: a firm's *background*, and consumer *feedback* about the company and its products. We included the background aspects in the model because brand image and familiarity are important conditions of trust in e-commerce [13], [126], [92]. They reduce uncertainty [46] and concerns [53], and increase perceived security control [122]. Displaying information about the company on the website, especially related to its offline presence (e.g., physical address, contact details), reduces the uncertainty regarding the otherwise *faceless* e-commerce activity [76], [96], [83], [10]. We included the feedback aspects in the model, because customer reviews [80], [93], third-party assessments (e.g., rating services [138]), perceptions of social presence [47], [29], [57], and, in particular, word-of-mouth within social networks [83] have been shown to increase trust.

2.2.2 Item Level

In addition to measuring the impact of the main constructs on the perception of trustworthiness and purchasing intention, we were interested in testing the subtle differences between closely related aspects, e.g., between online vs. offline sources of a company's ranking, or between publishing customer reviews on the company's own website vs. publishing on an independent website. We explored the differences between the following groups of related items: consumer feedback (Feedback items 1, 2, and 5), ranking source (Feedback items 3 and 4), access conditions (Collection items 4 and 5), source of information for recommendations (Collection items 2 and 3), tracking (Collection items 1 and 3), and application permissions (Control items 4 and 5) (appendix A).

Consumer feedback Online review credibility is positively related to the quality of argument made in reviews [22]. Because unbiased pieces of information are more likely to be trusted [127], we predicted that:

H5a: Customer feedback on independent websites has a stronger impact on the perceived trustworthiness and purchasing intention than user reviews on the company's own website.

About 30% of favorable reviews are fraudulent [88] and the authors of such manipulated opinions are often paid to promote companies and their products [61], [62], [81], [97], [143]. Consumers, being aware of opinion fraud, may suspect that overly positive reviews are fraudulent. Therefore, as proof of their objectivity, a moderate amount of negative information in consumer reviews increases their credibility [67]. Such two-sidedness of exposure to both positive and negative aspects may lead to a belief change, inducing fewer counterarguments and decreasing source derogation [72]. However, in judgment and decision-making tasks individuals tend to rely more on negative than positive information [39], [56], [104], [150], possibly because negative information is perceived as more instructive and useful than positive information [4]. Negative reviews have a greater impact on the intent to purchase [151]. Therefore, we predicted that:

H5b: Mixed (both positive and negative) customer feedback has less impact on the perceived trustworthiness and purchasing intention than solely positive reviews on the company's own website.

Ranking source When a source of information is perceived as reliable and shows expertise on a topic, consumers tend to give a higher level of credibility to its content [117], [79]. The ability of online media to aggregate information enhances its credibility [70], [42], [104]. However, the "authority heuristic" [58], [132] suggests that users may perceive traditional (offline) sources of information as primary or official, and therefore develop a higher level of trust toward them compared to online sources. Traditional sources of information are more unbiased and accurate due to the established professional standards and social pressure [40], while website content is not always subject to editorial review and factual verification [41]. Hence, given the similar content in both sources, offline sources of information may have a higher level of reliability and credibility than online sources.

H5c: A high rating of a firm in the traditional media has a stronger positive effect on the perceived trustworthiness and purchasing intention than a high rating in online sources.

Access conditions Because take-it-or-leave-it offers do not allow consumers to access or use the services without the provision of personal information, some users provide false personal data [114] or abandon the website [37]. Hence, users are expected to dislike take-it-or-leave-it offers more than situations in which they have freedom to choose the level of information disclosure.

H5d: Users have a higher perceived trustworthiness and purchasing intention toward websites that allow access to content without having to input personal information compared to websites that do not grant such permission.

Source of information for recommendations Tracking through cookies and browser history induces privacy concerns [147]. The perceived risk of online behavioral tracking may negatively affect the long-term relationships between online sellers and buyers [64], especially when consumers are uninformed about such practices [142]. Aguirre *et al.* [3] found that click-through-rates (CTR) are lower when data for personalized online advertising is collected in a covert (as opposed to overt) manner. Therefore, due to the high sense of vulnerability we expected users to generally dislike covert information collection practices more than proactive information provision.

H5e: Websites that explicitly ask users to share information about their tastes and preferences receive a higher perceived trustworthiness and purchasing intention than those that implicitly collect such information using tracking technologies.

Tracking The majority of users consider targeted adverts based on third-party tracking harmful, annoying, and *pushy*, while the degree of trust is higher toward first-party tracking practices [100]. Therefore, we predicted that:

H5f: Third-party tracking has a more negative effect on the perceived trustworthiness and purchasing intention than first-party tracking.

Application permissions Aguirre *et al.* [3] found that the CTR dropped once users realized that personal information was collected without consent. This observation provides evidence of the importance of user control over data and awareness about practices involving the processing of personal information. Taylor *et al.* [136] argued that the level of control over personal information does not have a significant effect on trust, but mediates the negative relationship between privacy concerns and behavioral intentions.

H5g: The perceived trustworthiness and willingness to purchase from websites that grant control over the extent of personal information collection are higher than for the websites that do not provide such control.

Intercorrelations Chen and Barnes [20] showed that the perceived usefulness, privacy, and security trigger initial online trust, which then determines the intent to purchase. A similar relationship between trust and behavioral intent was found in [90]. Therefore, we expected that users that developed a perception of trust toward a company would be more willing to purchase a product or service from its website.

H6: The perceived trustworthiness is positively correlated with purchasing intention.

We discuss the methodology for testing the model in the next section.

3 Methodology

Based on the relevant literature, we made a preliminary selection of key attributes and discussed them during two focus group sessions. A focus group is an exploratory technique widely used in market research, which uses a moderated discussion to collect qualitative data from a small group of people regarding their opinions, beliefs, perceptions, and attitudes about a certain topic. The least prominent factors were screened out. Then we surveyed 117 participants from the Mobile Territorial Lab (MTL) community. The MTL community was created by the Telecom Italia SKIL Laboratory, which is used as an experimental environment for human-behavior analysis and interaction studies. The survey was sent to all 128 members of the MTL community. Eventually, 117 out of 128 people (91,4%) completed the survey in full. We asked them to read a list of 32 statements about the characteristics of firms and various aspects of their websites (hereinafter, *items*), and rate their perception of trustworthiness and purchasing intention. The main advantage of using the MTL community for the survey was its wide demographic profile compared to the use of students, in terms of age, education level, employment status, and income. Moreover, this method has a relatively low cost of recruitment because community members are paid a flat rate on a monthly basis and are ready to participate in studies at any time. As a result, in contrast to most academic studies conducted with students, we recruited survey respondents among adult Italian Internet users, who were representative of the general population. Our sample was also representative of the European online shopper population [123]. Appendix B summarizes their demographics and responses to the final questionnaire. Sixty-three percent of the participants were females, 89% were 36+ years old, half had at least a bachelor's degree, while one third had a high school diploma or less, and 67% had a full-time job.

3.1 Focus Group

Two focus group sessions were conducted in December 2014 in the Cognitive and Experimental Economics Laboratory at the University of Trento, Italy. During these approximately one-hour sessions, groups of 6 and 7 students, respectively, were asked in an interactive setting about their perceptions, opinions, beliefs, attitudes, concerns, and habits towards e-commerce and online privacy. Participants were free to express their opinion and

talk with other members. Following the rules and principles of the focus group technique, a moderator and an assistant administrated the discussion. We chose not to conduct focus groups with MTL members to avoid a priming effect and potential bias in their responses to the main survey. Therefore, for the focus groups we invited students, who were easy, fast, and cheap to recruit, and are commonly used in such research. The focus groups only played an auxiliary role to calibrate the list of statements for the survey. We did not base our conclusions or the results of model validation on these observations.

Participants expressed fairly high level of privacy concerns, including the statement, I'm not famous, but I'm concerned about my personal life and information. Although one participant said: Who cares about privacy nowadays! others found the topic relevant and one of the most important, fundamental, and central issues affecting Internet use. In general, participants were quite pessimistic about the current state of privacy and referred to it as a utopian and disappearing concept.

In reaction to instances of online privacy violations, the majority of participants described their discomfort, anger, irritation, fear, anxiety, and embarrassment, while a few admitted their preparedness for such consequences (I would not be surprised, One should expect that). Few participants felt they had the control and ability to protect their data from such violations (It would be partially my fault, I should have protected my privacy). As barriers to the acceptance of online shopping, respondents indicated the potential hazard of fraud, fishing, identity theft, data misuse, and a general absence of trust.

After the discussion, several statements were added to the list, e.g., about password creation requirements (Security item 2), and social network widgets were incorporated into the website's design (Feedback item 6). Some statements were corrected and clarified. For example, the discussion of positive customer reviews considered their source and nature. Participants were skeptical about companies that only received positive feedback, suspecting that it was a falsification of reviews or that unpleasant reviews had been deleted. Thus, we included three different items based on this feedback: positive reviews on the company's own website (Feedback item 5), and both positive and negative reviews on the company's own website (Feedback item 2) and on independent websites and forums (Feedback item 1). The qualitative results obtained in the focus groups confirmed the relevance of the topic, while discrepancies among participant opinions and attitudes confirmed the need for an in-depth investigation of the issue.

3.2 Survey

Attitudes toward privacy are heterogeneous and context-dependent [1]. Therefore, in this study, instead of asking for personal opinions, we surveyed more durable socially held judgments to better understand what is the *common knowledge* regarding the types of cues that trigger the perception of trustworthiness rather than individual preferences. Therefore, we used an incentivized elicitation method [82], in which participants were explicitly informed that the best strategy was to answer what they believe the majority of participants would choose rather than express their personal opinions, because more accurate *guesses* would be rewarded. Due to the incentivizing of choices this method was expected to elicit accurate decisions.

Subjects were asked to read a list of items describing the attributes of hypothetical firms operating in the online market and their websites (appendix A). Firms were assumed to be retailers of homogeneous products and services. The order of items was randomized across the participants. Participants were told that each item described the company completely, so that no other characteristics should be considered beyond the description provided. This enabled the level of credibility attributed to each aspect to be assessed separately, avoiding any potential interaction effects. After reading each statement, participants answered two questions on a 12-point Likert scale. The response categories were sorted into six groups as shown in Table 1.

We surveyed the participants to determine their demographics, prior Internet experience, acceptance of online shopping, technological literacy, privacy attitudes, concerns, and trust disposition through an exit questionnaire (appendix B) and used them as control variables in a statistical analysis.

After collection of the responses one statement and a related question were selected at random. The score and category chosen by the majority of survey respondents were determined. Participants who chose the *most popular* response for the selected item entered the raffle and 10 winners were picked at random. They received a USB flash drive of 32 or 16 Gb (with a market price of 20 and 13 Euro, respectively) depending on whether they assigned the exact same score as the majority of respondents or only the same category, but with a slightly different score.

Table 1: Survey questions

In your opinion, how trustworthy with respect to privacy would the website of this company appear to the majority of people?		In your opinion, how likely is it that other people will purchase products and services from the website of this company?	
Category	Score	Category	Score
Very untrustworthy	1-2	Very unlikely	1-2
Untrustworthy	3-4	Unlikely	3-4
Somewhat untrustworthy	5-6	Somewhat unlikely	5-6
Somewhat trustworthy	7-8	Somewhat likely	7-8
Trustworthy	9-10	Likely	9-10
Very trustworthy	11-12	Very likely	11-12

4 Results

The highest evaluations of the perception of trustworthiness and purchasing intention were assigned to the items that ensured privacy and the adoption of security practices, third-party certificates, and high ratings in the media, together with company's reputation, background, and variety of secure payment options (appendix C). The lowest scores were assigned to the hypothetical websites that had a low quality of content and design, actively encouraged users to connect various accounts with the company's website, stored users' personal details without consent, offered recommendations based on personal information about the user, and were involved in third-party data sharing.

4.1 Statistical Analysis

We used two-step structural equation modeling (SEM) to test our research model. In the first stage, we developed the measurement model, while in the second stage we evaluated the full structural model [49]. First, we ran SEM estimations on groups of items as endogenous observed variables and predicted the indices for sub-constructs as latent variables. Then we ran SEM estimations using the predicted values of sub-constructs as endogenous observed variables, and surveyed demographic characteristics and other covariates as exogenous observed variables. Finally, we predicted the indices for perceived trustworthiness (T) and purchasing intention (P) as latent variables. Appendix E summarizes the details of SEM path estimation and shows that the reliability of the measurement model was sufficient for all constructs and sub-constructs, except website quality. For the assessment of reliability we conducted a confirmatory factor analysis with Varimax rotation (appendix D). Using the Kaiser extraction criterion we retained only factors with an eigenvalue of more than 1 for each construct. The resulting factor loadings were high (0.54-0.91) and the degree of uniqueness was within an acceptable level of less than 0.6 (0.18-0.6), for all items except LT1, QT1, QP1, QT3, and QP3. The internal consistency of the resulting indices was good, Cronbach's $\alpha > 0.7$ (0.84-0.93), except for the website quality. Appendix F shows that the research model achieved a satisfactory level of goodness of fit. Discriminant validity defines the extent to which an item diverges from other items that theoretically should not be related. Discriminant validity exists if the AVE exceeds the shared variance measured as a squared correlation for each pair of constructs and sub-constructs [44], [54], [14]. All constructs except the index of website quality (QT) satisfied the convergent validity criteria, but the discriminant validity criteria were not satisfied for all pairs of constructs and sub-constructs (appendices E and G). Moreover, privacy, security, and reputation indices, including feedback and awareness, are often strongly correlated. Therefore, we included the covariance between them in the path estimation model.

4.2 Relationship between Perceived Trustworthiness and Purchasing Intention

The correlation and covariance coefficients (appendix G) indicated a significant positive relationship between the perceived trustworthiness and purchasing intention, at the aggregate level (*i.e.*, between T and P) and at the sub-construct level (*i.e.*, between ST and SP, QT and QP, *etc.*): pairwise correlation coefficients for each item were also positive and significant at the 0.01 level and varied between 0.59 and 0.88, with an average of 0.74. This finding supports H6, regarding the positive relationship between the perceived trustworthiness and purchasing intention.

The positive correlation indicated that participants were generally more likely to purchase from a trustworthy website and less likely to purchase from an untrustworthy website (Figure 2). However, in some cases, the perception of trustworthiness and behavioral intentions were misaligned by the participants. Specifically, in 14.3% of all cases, the participants reported a positive intention to buy from privacy untrustworthy websites. The presence of famous brands, widgets for social network websites, a *social login* (*i.e.*, the ability to access the vendor's website using a social

network account), a request for permission to access geographical location, a request for information about tastes and preferences, inferences about such information using tracking technologies, and remembering the user's address for future deliveries had no or a negative effect on the perception of trustworthiness; however, these features positively affected purchase intention. On the other hand, in 2.83% of all cases, the participants reported negative intentions to buy from a website regardless of its trustworthiness, for example, when a company's website demonstrated a privacy policy and imposed password-composition requirements. We discuss the potential interpretations of this observed misalignment in section 5.

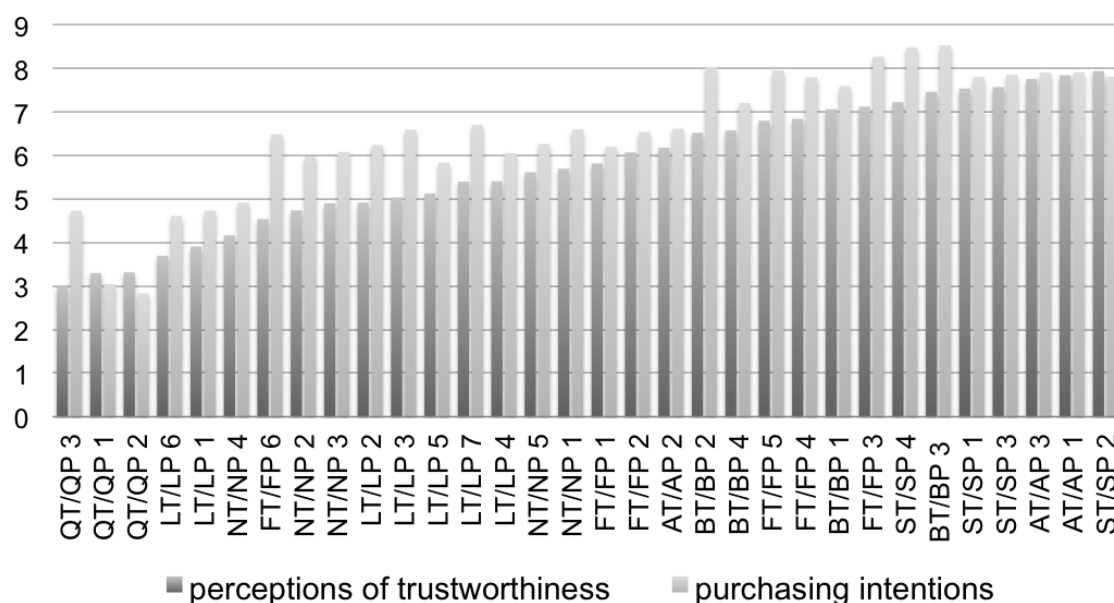


Figure 2: Mean values of the perception of trustworthiness and purchasing intention. Likert scale scores by item

4.3 Factors Influencing Perceived Trustworthiness and Purchasing Intention

In this section, we report the results on the relation between different factors, perceived trustworthiness and purchasing intention.

4.3.1 Construct Level

Standardized path coefficients (Table 7) suggest that all sub-constructs had a significant effect on the perception of trustworthiness and purchasing intention at the 0.001 level, except for the quality of website. QT had the smallest effect on trust, although it was significant at the 0.05 level. QP did not significantly influence purchasing intention. Therefore, our findings provided support for H1, H2, and H4 for both the perception of trustworthiness and purchasing intention, and for H3 regarding the effect on trust. As shown in appendix C, a website's compliance with security regulations resulted in the highest positive perception of trustworthiness and purchasing intention, followed by awareness about the privacy practices employed, company background, and customer feedback. Poor website quality resulted in the lowest negative perception of trustworthiness and purchasing intention, followed by the collection and control of personal information.

Companies with positive feedback and a strong background were considered to be more trustworthy, leading to a greater willingness to purchase from their websites. Moreover, ensuring consumer awareness about security and privacy protection, by providing informational notices (e.g., about the use of cookies or practices related to the collection, storage, sharing, and use of personal data), demonstrating proof of compliance with privacy and security protection standards and regulations approved by independent authorities (such as an Extended Validation (EV) certificate and privacy seals), and enforcing password-composition requirements further improved the perception of trustworthiness and purchasing intention. However, invasive practices of data collection and providing users with limited control over this information (or poor communication of the opportunities for such control) led to a negative assessment of trustworthiness and a subsequent low purchasing intention. Although insufficient investment of time, money, and effort in website design and lack of attention to the quality of content did not have a significant direct impact on the willingness to purchase, it may have an indirect effect through a negative influence on the perception of trustworthiness because of the correlation between trust and purchase intention demonstrated earlier.

In line with the low discriminant validity and high correlation indices, the covariance between some pairs of sub-constructs in our model was also significant (Table 8). A company or website collecting users' personal information was perceived to be more trustworthy if it had a positive reputation, including both a positive background and

feedback from other consumers, and provides users with control over the information collected. Similarly, practices involving the collection of personal information (e.g., for feeding the recommendation system, credit card details, and shipping addresses for future orders and transactions) would increase purchasing intention when accompanied by control over the information collected. Such control may further enhance the positive effect of consumer feedback on the perception of trustworthiness and willingness to purchase.

4.3.2 Item Level

We tested the differences between different factors on item level (Table 2).

Consumer feedback. Although one might find the presence of solely positive feedback about a company on its website (FT5 and FP5) subjective or indicative of fake reviews, on average participants assigned a higher rating for trustworthiness and purchasing intention to such companies than to firms that had both positive and negative feedback. For the firms with both positive and negative feedback, having reviews on the company's own website (FT2 and FP2) was not statistically different from such reviews on independent websites or forums (FT1 and FP1).

Therefore, regardless of the fact that solely positive feedback is often fraudulent, subjects tended to trust it more than a mixture of positive and negative reviews. Although it is easier for companies to manipulate reviews on their own websites than on independent forums, the study participants did not trust the independent websites more. Hence, our results support H5b but not H5a.

Ranking source. The source of information about the company was important when determining purchasing intention, but not for the perception of trustworthiness. A respondent's willingness to purchase tended to rely on the use of traditional media, such as TV and radio (FT3 and FP3) as the source of information about a company's ratings and reputation rather than on online channels (FT4 and FP4). This may be because website users are more experienced and familiar with traditional media, and feel more confident in relying on those sources, and the content published in traditional media is more likely to go through editorial review and approval [70]. Hence, H5c was supported for purchasing intention but not for the perception of trustworthiness.

Access conditions. Average scores for both the perception of trustworthiness and purchasing intention for websites with restricted access conditions (LT5 and LP5) did not significantly differ from those of websites employing more privacy-friendly practices (LT4 and LP4), providing no support for H5d. This might be because the restriction of access conditions is now a common practice, and thus does not raise strong concerns. Some online vendors require customers to create accounts on their websites. Such accounts not only help sellers to monitor customer activity, but also allow consumers to keep track of their own transactions, save and compare products in the shopping cart, and save personal information for future transactions. Therefore, consumers may perceive benefits from registering on a certain website that sometimes outweigh the corresponding privacy concerns.

Sources of information for recommendations. Explicitly asking people about their preferences (LT2 and LP2) did not result in different trustworthiness and purchasing intention scores than the use of obscure tracking technologies to gather such information about users (LT3 and LP3), providing no support for H5e. Because the scores of perception of trustworthiness were negative for both items, we concluded that respondents disliked both the implicit and explicit collection of information about their tastes and preferences.

Application permissions. In support of H5g, providing an opportunity to at least partially edit the list of permissions before installation of a company's mobile application (NT5 and NP5) significantly improved both the perception of trustworthiness and purchasing intention compared to a take-it-or-leave-it offer (NT4 and NP4). While respondents were unlikely to purchase from an application that inevitably accessed their personal data, the opportunity to edit the access permissions resulted in a willingness to make a purchase. Therefore, companies may benefit from enforcing privacy-friendly policies, not only on their websites but also in their mobile applications.

Appendix H summarizes the results of hypothesis testing. Our findings suggest that companies should pay close attention to the way they design and implement their practices. For example, to build trustworthy relationships with customers and positively affect purchasing intention, companies should avoid negative feedback, not through the manipulation of reviews and fraud but through service improvement and by satisfying the needs of consumers. Both independent forums and branded websites are effective in building trust. Firms should also enhance a user's privacy and provide control over their personal information, e.g., by introducing privacy-friendly policies and editable lists of access permissions, and by limiting the collection of the user's personal data. Although Internet media is gaining power, overtaking, and sometimes even substituting for, offline channels in their ability to build reputation and trust, companies should not forget to sustain and promote their image in traditional media, which still has a strong influence on purchasing intentions according to our results.

Table 2: Test of the differences between factors. N=117.

Factors	T-test ($\Pr(T > t)$)	Wilcoxon rank-sum test ($\text{Prob} > z $)	Statistical power
Consumer feedback			
FT1 and FT5	0.00	0.00	0.83
FP1 and FP5	0.00	0.00	0.97
FT2 and FT5	0.00	0.01	0.55
FP2 and FP5	0.00	0.00	0.96
FT1 and FT2	0.15	0.13	0.13
FP1 and FP2	0.10	0.06	0.16
Ranking source			
FT3 and FT4	0.14	0.18	0.12
FP3 and FP4	0.03	0.03	0.24
Access conditions			
LT4 and LT5	0.21	0.25	0.12
LP4 and LP5	0.39	0.14	0.09
Sources of information			
LT1 and LT3	0.00	0.00	0.99
LP1 and LP3	0.00	0.00	1.00
Application permissions			
NT4 and NT5	0.00	0.00	0.99
NP4 and NP5	0.00	0.00	0.96

4.4 Robustness Check

We introduced the individual characteristics of the surveyed respondents as observed exogenous covariates in the second stage of the SEM estimation. We found that females and older subjects tended to have a lower perception of trustworthiness. Those who used real names instead of pseudonyms on Facebook were more disposed to trust, while the number of connections (friends) on Facebook was negatively correlated with T and P. The use of a real identity and a large number of connections in online social networks were signals of low privacy concerns and a high general disposition toward trust.

The number of years that a subject had used the Internet positively influenced both the perception of trustworthiness and purchasing intention, in line with [25]. Carlos Roca *et al.* [17] explained that experienced Internet users may be more familiar with security technologies and therefore feel more comfortable about trusting online shopping websites.

Subjects without full-time employment and concerned about privacy tended to have a lower perception of trustworthiness and purchasing intention. This finding further supported our claim about the important relationship between privacy, trust, and purchasing intentions, suggesting that companies pay rigorous attention to customer concerns and ensure protection of their personal data.

We observed that although almost half of the respondents recognized the EV certificate as a symbol of website compliance, only 72% of them understood correctly what this certificate means. (Because participants had access to various sources of information during the survey and had an opportunity to locate the correct explanation, the rate of correct answers indicated a lower bound). This misalignment may indicate potential misconceptions and misbeliefs about privacy and security signals. A qualitative analysis of the responses shows that some subjects wrongly believed that a website with a green padlock in the URL address bar will require registration for access or will constantly guard the privacy of users. Moreover, familiarity with privacy seal authorities, recognition of the EV certificates green padlock, and the actual understanding of its meaning did not significantly affect T and P. These findings are in line with previous studies, which show that websites possessing independent certificates are actually more likely to be untrustworthy than uncertified websites [35]. Thus, users tend to follow heuristics and shortcuts in relying on these assurances, without verification of authenticity and not always understanding the meaning of certification [124], [85], or directly rely on cues [125], [134] even when they are not credible or interpretable [33], [119], [122].

Similarly, 41% of the participants misunderstood the concept of web cookies, calling them *informative windows*, *user feedback sent to the website to guarantee monitoring of use*, *files that permit a faster access to the Internet*, *some form*

of advertising, or simply treats and sweets. One of the respondents correctly drew the connection between cookies and the subsequent receipt of targeted advertising, but erroneously concluded that one must enable cookies to avoid privacy invasion.

These findings suggest that the level of *privacy literacy* and awareness is relatively low and consumer education is required. Misunderstandings may lead to the distortion of consumer expectations and the subsequent exploitation of such beliefs for fraudulent or malicious purposes. The improvement of the communication of privacy- and security-related information to consumers is important not only for policy makers and privacy advocates, but is also beneficial for the business because it enhances the perception of trustworthiness and contributes to an increase in purchase intention.

5 Discussion, Limitations, and Future Work

In this section we provide interpretation of the results, discuss the limitations, and propose the directions for future work.

5.1 Behavioral Interpretation

Consumers initially engage in e-commerce with the primary goal of purchasing a product or service, not of protecting their personal information. Customer activity on an e-commerce website is built around choosing a product and the check-out process, with activity buttons and filters enabling navigation through products and prices, while privacy-related information is often limited to a long document written in legal language, which is difficult to understand for a person without an appropriate educational level, and tends to be hidden in one of the secondary sections of the website. Moreover, in uncertain situations people tend to rely on contextual cues [2], [69]. Websites are usually in control of such cues, e.g., the website design, architecture, and content, and the structure of the information presented to the user. Because a website's primary goals are business-oriented, they may highlight shopping benefits, and draw less attention to (or even deliberately drive it away from) the potential privacy concerns and issues. Therefore, according to the prominence-interpretation theory [43], a lower salience of privacy-related factors compared to shopping-related factors may trigger the dominance of privacy-related factors at the moment of the purchasing decision.

The trust relationship between online vendors (trustees) and consumers (trustors) is often asymmetric. Such a relationship typically takes the form of a take-it-or-leave-it offer. In a more heterogeneous market, consumers could deny access to their personal data and choose another company that provides similar services without the requirement to reveal extensive amounts of personal information. However, the proliferation and acceptance of invasive permission settings as a common business practice often leaves consumers without a choice. This has created a user-website asymmetry, in which consumers are more dependent on the conditions created by the website than the company are dependent on consumer choices. With an increase in the dependency of trustors on trustees, the trustors decrease their cognitive effort and search for information that is required for an accurate credibility assessment. The trustor positively judges ambiguous information and is inclined to engage in an initial level of trust [149], discounting some concerns that may accompany such a decision.

The credibility people tend to give to expected costs against expected benefits can be implied by the decision to trust [133]. A similar calculative approach has been used in the privacy domain and is described as "privacy calculus" [28], [32], [87]. However, people often fail to perform such calculations, for example due to immediate gratification (or present) bias, which refers to an individual's preference for a short-term return [8], [106], and the discounting of future costs and benefits [107], [66]. A website remembers personal details for future transactions or to recommend products based on behavioral tracking, with the goal of speeding up and facilitating the shopping experience. Moreover, the outcome of a purchasing transaction occurs immediately, while the outcomes of the risk taken in relation to privacy are uncertain in magnitude, value, probability, and time [68]. Therefore, people may be willing to buy from websites where privacy cannot be assured at the cost of privacy risks, if these websites offer services that facilitate the online shopping process in general.

Finally, a combination of various factors is a tradeoff per sé. In our experiment we asked subjects to consider each factor independently, but real-life decisions are influenced by the simultaneous impact of multiple factors and their interactions. Consider, for example, a website that requests some personal information to create an account and remembers credit card details for future transactions, but imposes strict password-composition requirements, ensures compliance with privacy regulations, and demonstrates security certificates. The request for personal information may create a privacy concern, but compliance with the privacy regulations and strict password-composition requirements mitigate them, assuring consumers that their information will be processed securely. Similarly, the presence of security certificates mitigates security concerns and assures consumers that the credit card details they provide will be stored securely and are protected from unauthorized access or use. Therefore, the final decision to purchase depends on the outcome of the interaction between negative and positive aspects.

5.2 The Effects of Cognitive Heuristics and Biases

Although some of the factors investigated have similar effects, the underlying mechanisms leading to these results may differ. To better understand the decision-making process behind the assessment of trustworthiness, we analyzed it through the lens of cognitive science and considered what behavioral heuristics drive certain effects in our study. The theory of bounded rationality [129] has a great potential to explain the process that brings various factors into action to change online trustworthiness perceptions. The notion of bounded rationality refers to the limitations imposed by the nature of the human mind and exogenous conditions, and claims that individuals are constrained to make a decision using limited computational resources and time [50]. This argument is further supported by the limited capacity model [84] and prominence-interpretation theory of online credibility [43]. Due to their finite cognitive capacity individuals select only salient attributes for processing messages, which require an optimal level of cognitive effort to achieve a sufficiently efficient outcome [115]. To reach a balance and make an adaptive choice people often employ cognitive heuristics [58], [104], [132]. Although such mental shortcuts and rules-of-thumb sometimes result in biased decisions [144], more cognitively demanding information-processing strategies have been shown to be equally or even less effective when attempting to make a perfectly rational decision due their complexity [50], [51].

First, the expectancy violation heuristic arises in situations where a website's content does not conform to user expectations [104] and as consequence of arousal, distraction, and increased attention to the violation [16] the perceived trustworthiness of that website is reduced. In our study, the effect of this heuristic was illustrated by the situation in which: 1) website quality and design did not match the standards and norms (e.g., if orthographic and typographic errors, broken links, or suspicious banners were present); 2) the website provided unsolicited information or services (which is also aligned with the intrusiveness heuristic [132]); 3) the company's products appeared on unrelated websites or notifications about the use of cookies popped up unexpectedly or 4) when a company presented third-party website links, offered social network recommendations, or tracked a user's activities on the web, and remembered their personal information, e.g., address, credit card details, login and passwords.

Second, the reputation heuristic is based on a consumer's tendency to rely on familiar sources and alternatives rather than on unrecognized ones [50]. In our study, people driven by this heuristic attributed a higher level of trustworthiness to websites that carried products with reputable names and to companies that had operated for many years and had a description of their history on the websites. This indirectly enhances the effect of the presence of names and photos of key staff members on the company's website, providing proof of the existence of real people behind the intangible web interface. The reputation heuristic itself may be a product of the authority heuristic, which suggests that the degree of being an official authority or an information source is an important criterion in a credibility assessment [58], [132]. In our study, the effect of the authority heuristic was triggered by the presence of independent third-party seals and security features.

Third, the endorsement heuristic [58] or conferred credibility [42], is related to confirmation bias and consensus [19] or the bandwagon heuristic [132], under which people perceive a source of information as trustworthy without scrutinizing the content if others already trust it. In our study, reliance on consumer feedback, reviews, online and offline ratings, and recommendations from friends in online social networks influenced credibility perceptions through the endorsement heuristic. The impact of recommendations from friends is additionally supported by the liking/agreement heuristic [19], which suggests that individuals are likely to believe that people they like possess correct beliefs and tend to agree with their opinions.

The group of heuristics, which includes reputation, authority, endorsement, and agreement, is generally related to the notion of social proof [23] or social confirmation, which suggests that if other users trust, use, and recommend a particular website, then one can rely on their opinions and perceive the website as trustworthy. However, such a strategy is not perfect, because it may lead to a misconception between credibility and popularity [104], and in certain cases, to an erroneous reliance on fraudulent information from manipulated opinions and fake reviews [61], [62]. Therefore, it is important to assess the reliability of user-generated information, e.g., through cross-validation mechanisms. Similar information from various sources will additionally trigger the consistency heuristic [104] and potentially further improve the effectiveness of feedback, e.g., if reviews on a company's website and independent forums coincide with online and offline ratings.

To build trust and improve the purchasing intention of potential customers, companies should pay more attention to the way they present information about their reputation, including the company background, customer feedback and reviews, privacy- and security-related practices, and means of protection. Moreover, they need to ensure the quality of this information is satisfactory, together with the content of the website and its visual appeal. Firms should grant users more control over their information, including traditional forms of consent or permission management and the ability to modify/delete private data or deny access to personal information. They should also provide a choice of alternative ways to access the website content (e.g., not only in exchange for personal information but also on a freemium or subscription basis for a small fee that allows avoiding private data collection).

5.3 Limitations and Future Work

This study has some limitations. First, it was based on self-reported answers to questions about hypothetical companies. However, the results of goodness of fit and validity tests demonstrate that the survey successfully captured the difference between participants' opinions necessary for model validation. Therefore, our study provides useful empirical insight into the factors influencing perceived trustworthiness and purchasing intentions. Future laboratory or field experiments that observe user behavior on actual e-commerce websites will allow testing the external validity and the interaction effects among various factors. Second, we used the willingness to buy as a measurement of behavioral intention. Future studies should analyze the effect of our proposed factors on behavioral metrics, such as actual website visits, purchasing behavior, and repeat purchases. Third, replications of the study need to be performed in other countries to account for potential cross-cultural differences. Fourth, the structured equation modeling technique was susceptible to a number of limitations, such as multicollinearity and the assumption of multivariate normality. However, our dataset did not have univariate or multivariate outliers, the determinant of the covariance matrix did not indicate multicollinearity, and the residuals of the covariance did not deviate substantially from zero. Finally, because we used self-reported data, our study may be affected by common method variance. As a procedural remedy, we randomized the order of items across respondents and included positively and negatively worded statements. We also attempted to avoid any social desirability bias in our wording, and applied statistical techniques to control for it ex-post. The use of the marker variable method revealed between 0 and 2% shared variance with the main model constructs, while less than 50% of the variance was explained by a common latent factor. The indicators were close to, but did not exceed, the critical level. The study could be replicated in the future using a larger sample of respondents, introducing variability in anchor description of the scales, or running a longitudinal survey to reduce the common method bias.

6 Conclusion

Based on previous research and the results of two focus groups we created a list of website attributes and tested their impact on users' purchasing intentions and perceptions of trustworthiness with respect to privacy via a survey of 117 adults.

First, we found that privacy, security, and reputation strongly affected the perception of trustworthiness and purchasing intention, while website quality played a smaller role in building trust and has no effect on the willingness to buy. On average, websites with enhanced security, transparency regarding consumer privacy, and with a positive company background and feedback received a positive perception of trustworthiness and purchasing intention scores.

Second, we found a positive relationship between trust and purchasing intention. Generally participants were more likely to purchase from a trustworthy website and less likely to purchase from an untrustworthy website. However, in some cases participants that rated a company as untrustworthy were still likely to purchase from their website. This misalignment may be related to the tendency for the expected benefits to outweigh the potential privacy costs. When the website offered a functionality that improved or facilitated the online shopping process, but at the same time raised privacy concerns, a user's decision to trust and make a purchase from the website was dependent on the eventual tradeoff between benefits and costs. Because individuals tend to discount future outcomes and prefer short-term returns, the immediate and evident benefits of an improved shopping experience (which is also the main goal of engaging in e-commerce) may outweigh the uncertainty of potential future privacy costs (which is a by-product of online interactions rather than a primary component). Moreover, privacy-related aspects may be presented on the website in a less salient way than the shopping-related features, further enhancing an underestimation of the weighting of privacy components in the decision-making process. Finally, the asymmetric structure of the relationship between online seller and buyer put the customer in the position where they are required to engage in a degree of initial trust and accept some risks to conduct a transaction. Such situations may force consumers to accept take-it-or-leave-it offers, despite the concerns over such decisions.

Our findings suggest that leveraging the factors that positively influence the perception of trustworthiness would help companies to build trust, which would in turn affect a customer's purchasing intention. First, companies should ensure the security of their websites and communicate the level of security to the customers, for example by introducing strong password-composition requirements, safe payment options, and demonstrating compliance with security standards. Second, companies should pay great attention to privacy-related issues; limit the collection of user data to within the scope of well-defined and user-friendly activities; be transparent about the collection, storage, use, and sharing of this data; and give users control over their personal data. The form of this control should also evolve and improve over time together with the development of related technology and legislation. Companies should make an effort to create a positive reputation, including a presentation of information about the company's background and the actual people behind the website, and also respond to customers' concerns and questions. Firms, especially not well-known businesses, should invest time, money, and effort to create a good-quality website that contains accurate and up-to-date information, because in situations of uncertainty visual appeal plays an important role, whereas the quality of the content signals the quality of the company itself and its products.

Third, we found that participants trust and are more likely to purchase from the websites of companies that receive only positive feedback rather than mixed (both positive and negative) reviews, regardless of whether they were published on the company's own website or on independent forums. Therefore, companies should pay attention to any negative feedback from customers and respond to them publicly to maintain their reputation. Participants trusted online and offline sources of company rankings; however, the traditional sources appeared to have a greater impact on willingness to purchase. Therefore, companies should not forget to maintain their reputation in the traditional media, even though online sources of information have now gained a wider popularity. Our results suggest that first-party and especially third-party tracking of customers should be limited or avoided. Moving away from take-it-or-leave-it offers and granting consumers more control and choice will benefit trust relationships and increase purchasing intention.

Finally, we found that people, who use their real name on Facebook instead of a pseudonym and are experienced at using the Internet generally tended to trust websites more than the average user, while females, older subjects, people with less independent sources of income (i.e. without full-time employment), higher levels of privacy concerns, and a larger number of connections (friends) on Facebook were less inclined to trust. Similarly, less independent sources of income, privacy concerns, and a lower number of Facebook connections negatively affected purchasing intention, while Internet experience had a positive effect. Therefore, to establish trust-building strategies companies should be especially attentive to the above-mentioned target groups that currently do not have a disposition to trust. We also observed a relatively low level of privacy literacy among our respondents. About one third of participants demonstrated a misunderstanding of the basic privacy and security concepts. Such misconceptions may distort a user's expectations, lead to inefficient communication of the information, and cause economic or psychological harm. For example, a website that saliently presented a notification about the use of cookies may be perceived as less trustworthy than a website that hid such details or covertly collected information. Users that think cookies are essential for faster access to the Internet, as one of our subjects claimed, may enable cookie storage without a full understanding of the consequences that it will have on their privacy. The improvement of the communication of privacy- and security-related information to the consumers is important not only for policy makers and privacy advocates but is also beneficial for the business because enhanced levels of trust will increase purchasing intention.

Acknowledgments

The authors are grateful to the colleagues and reviewers for their insights and useful comments. Funding for this study was supported by a fellowship from Telecom Italia (TIM).

References

- [1] A. Acquisti, R. Taylor, and L. Wagman, The economics of privacy, *Journal of Economic Literature*, vol. 54, no. 2, pp. 442-492, 2016.
- [2] A. Acquisti, Privacy in electronic commerce and the economics of immediate gratification, in *Proceedings 5th ACM conference on Electronic commerce*. ACM, New York, 2004, pp. 21-29.
- [3] E. Aguirre, D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels, Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness, *Journal of Retailing*, vol. 91, no. 1, pp. 34-49, 2015.
- [4] R. Ahluwalia, Examination of psychological processes underlying resistance to persuasion, *Journal of Consumer Research*, vol. 27, no. 2, pp. 217-232, 2000.
- [5] I. Ajzen, *From Intentions to Actions: A Theory of Planned Behavior*. Berlin: Springer, 1985.
- [6] I. Ajzen, The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991.
- [7] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behaviour*. Michigan: Prentice-Hall, 1980.
- [8] M. Anderson, *Family Structure in Nineteenth Century Lancashire*. Cambridge, UK: Cambridge University Press, vol. 5, 1971.
- [9] M. Arcand, J. Nantel, M. Arles-Dufour, and A. Vincent, The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust, *Online Information Review*, vol. 31, no. 5, pp. 661-681, 2007.
- [10] G. Bansal and D. Gefen, The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, *European Journal of Information Systems*, vol. 24, no. 6, pp. 624-644, 2015.
- [11] Y. Bart, V. Shankar, F. Sultan, and G. L. Urban, Are the drivers and role of online trust the same for all web sites and consumers? a large-scale exploratory empirical study, *Journal of Marketing*, vol. 69, no. 4, pp. 133-152, 2005.
- [12] F. Bélanger, J. S. Hiller and W. J. Smith, Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 245-270, 2002.
- [13] A. Bhattacharjee, Individual trust in online firms: Scale development and initial test, *Journal of Management Information Systems*, vol. 19, no. 1, pp. 211-241, 2002.

- [14] L. L. Bove, S. J. Pervan, S. E. Beatty, and E. Shiu, Service worker role in encouraging customer organizational citizenship behaviors, *Journal of Business Research*, vol. 62, no. 7, pp. 698-705, 2009.
- [15] M. W. Browne, R. Cudeck, K. A. Bollen, and J. S. Long, *Alternative Ways of Assessing Model Fit*. Beverly Hills: CA: Sage, 1993.
- [16] J. K. Burgoon, L. A. Stern and L. Dillman, *Interpersonal Adaptation: Dyadic Interaction Patterns*. Cambridge: University Press, 2007.
- [17] J. Carlos Roca, J. José García and J. José de la Vega, The importance of perceived trust, security and privacy in online trading systems, *Information Management & Computer Security*, vol. 17, no. 2, pp. 96-113, 2009.
- [18] E. M. Caudill and P. E. Murphy, Consumer online privacy: Legal and ethical issues, *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 7-19, 2000.
- [19] S. Chaiken, The Heuristic Model of Persuasion, in *Social Influence: The Ontario Symposium*, vol. 5. Hillsdale, NJ: Lawrence Erlbaum Associates, 1987.
- [20] Y.-H. Chen and S. Barnes, Initial trust and online buyer behaviour, *Industrial Management & Data Systems*, vol. 107, no. 1, pp. 21-36, 2007.
- [21] Y. Chen, X. Yan, W. Fan, and M. Gordon, The joint moderating role of trust propensity and gender on consumers' online shopping behavior, *Computers in Human Behavior*, vol. 43, pp. 272-283, 2015.
- [22] C. M.-Y. Cheung, C.-L. Sia, and K. K. Kuan, Is this review believable? a study of factors affecting the credibility of online consumer reviews from an ELM perspective, *Journal of the Association for Information Systems*, vol. 13, no. 8, pp. 618-635, 2012.
- [23] R. B. Cialdini, *Influence: The Psychology of Persuasion*. New York: Morrow, 1993.
- [24] W. Conhaim, E-commerce, *Link-Up*, vol. 15, no. 1, pp. 13-15, 1998.
- [25] B. J. Corbitt, T. Thanasankit and H. Yi, Trust and e-commerce: a study of consumer perceptions, *Electronic Commerce Research and Applications*, vol. 2, no. 3, pp. 203-215, 2003.
- [26] C. L. Corritore, B. Kracher and S. Wiedenbeck, Online trust: concepts, evolving themes, a model, *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737-758, 2003.
- [27] M. J. Culnan, The Culnan-Milne survey on consumers & online privacy notices: Summary of responses, in *Proceedings Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices*, Washington DC, 2001, pp. 47-54.
- [28] M. J. Culnan and P. K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation, *Organization Science*, vol. 10, no. 1, pp. 104-115, 1999.
- [29] D. Cyr, K. Hassanein, M. Head, and A. Ivanov, The role of social presence in establishing loyalty in e-service environments, *Interacting with Computers*, vol. 19, no. 1, pp. 43-56, 2007.
- [30] N. Delafrooz, L. H. Paim and A. Khatibi, Understanding consumer's Internet purchase intention in Malaysia, *African Journal of Business Management*, vol. 5, no. 7, pp. 2837-2846, 2011.
- [31] R. Dhamija, J. D. Tygar and M. Hearst, Why phishing works, in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, Montreal, Canada, 2006, pp. 581-590.
- [32] T. Dinev and P. Hart, An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, vol. 17, no. 1, pp. 61-80, 2006.
- [33] T. Duncan and S. E. Moriarty, A communication-based marketing model for managing relationships, *The Journal of Marketing*, pp. 1-13, 1998.
- [34] Statista. (2017) Digital market outlook in Europe. Statista. [Online]. Available: <https://www.statista.com/outlook/243/102/ecommerce/europe?currency=eur#>
- [35] B. Edelman, *Adverse Selection in Online Trust Certifications*, in WEIS. Boston: Harvard Business Schol, 2006.
- [36] F. N. Egger, Affective design of e-commerce user interfaces: How to maximise perceived trustworthiness, in *Proceedings of the International Conference on Affective Human Factors Design*, 2001, pp. 317-324.
- [37] EPIC. (2000) EPIC alert, electronic privacy information center (EPIC). EPIC. [Online]. Available: <http://www.epic.org/alert/EPICAlert7.16.html>
- [38] M. S. Featherman and P. A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective, *International Journal of Human-Computer Studies*, vol. 59, no. 4, 2003, pp. 451-474.
- [39] S. Feldman, Motivational aspects of attitudinal elements and their place in cognitive interaction, *Cognitive Consistency*, pp. 76-114, 1966.
- [40] H. Finberg, M. L. Stone and D. Lynch, Digital journalism credibility study, *Online News Association*, vol. 3, 2002, pp. 1145-1149.
- [41] A. J. Flanagin and M. J. Metzger, Perceptions of Internet information credibility, *Journalism and Mass Communication Quarterly*, vol. 77, no. 3, 2000, pp. 515-540, 2000.
- [42] A. J. Flanagin and M. J. Metzger, Digital media and youth: Unparalleled opportunity and unprecedented responsibility, *Digital Media, Youth, and Credibility*, pp. 5-27, 2008.
- [43] B. J. Fogg, Prominence-interpretation theory: Explaining how people assess credibility online, in *Proceedings, CHI'03 Extended Abstracts on Human Factors in Computing Systems*. ACM, Lauderdale, FL, 2003, pp. 722-723.
- [44] C. Fornell and D. F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981.
- [45] FTC, *Privacy online: Fair information practices in the electronic marketplace: A federal trade commission report to congress*, Washington DC: FTC, 2000.
- [46] D. Gefen, E. Karahanna and D. W. Straub, Trust and TAM in online shopping: an integrated model, *MIS Quarterly*, vol. 27, no. 1, pp. 51-90, 2003.

- [47] D. Gefen and D. W. Straub, Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-Products and e-Services, *Omega*, vol. 32, no. 6, pp. 407-424, 2004.
- [48] J. F. George, The theory of planned behavior and Internet purchasing, *Internet Research*, vol. 14, no. 3, pp. 198-212, 2004.
- [49] D. W. Gerbing and J. C. Anderson, An updated paradigm for scale development incorporating unidimensionality and its assessment, *Journal of Marketing Research*, pp. 186-192, 1988.
- [50] G. Gigerenzer and P. M. Todd, *Simple Heuristics that Make us Smart*. USA: Oxford University Press, 1999.
- [51] M. Gladwell, *Blink: The Power of Thinking Without Thinking*. USA: Back Bay Books, 2007.
- [52] S. Grazioli and S. L. Jarvenpaa, Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers, *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, vol. 30, no. 4, pp. 395-410, 2000.
- [53] R. Gulati, Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances, *Academy of Management Journal*, vol. 38, no. 1, pp. 85-112, 1995.
- [54] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, R. L. Tatham et al., *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson Prentice Hall, 2006.
- [55] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, R. L. Tatham et al., *Multivariate data analysis*, 7th ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2010.
- [56] P. M. Herr, F. R. Kardes and J. Kim, Effects of word-of-mouth and product-attribute information on persuasion: An accessibility-diagnosticity perspective, *Journal of Consumer Research*, vol. 17, no. 4, pp. 454-462, 1991.
- [57] T. Hess, M. Fuller, and D. Campbell, Designing interfaces with social presence: Using vividness and extraversion to create social recommendation agents, *Journal of the Association for Information Systems*, vol. 10, no. 12, pp. 889-919, 2009.
- [58] B. Hilligoss and S. Y. Rieh, Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context, *Information Processing & Management*, vol. 44, no. 4, pp. 1467-1484, 2008.
- [59] I. B. Hong, Understanding the consumer's online merchant selection process: The roles of product involvement, perceived risk, and trust expectation, *International Journal of Information Management*, vol. 35, no. 3, pp. 322-336, 2015.
- [60] L.-t. Hu and P. M. Bentler, Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling*, vol. 6, no. 1, pp. 1-55, 1999.
- [61] N. Hu, I. Bose, Y. Gao, and L. Liu, Manipulation in digital word-of-mouth: A reality check for book reviews, *Decision Support Systems*, vol. 50, no. 3, pp. 627-635, 2011.
- [62] N. Hu, L. Liu and V. Sambamurthy, Fraud detection in online consumer reviews, *Decision Support Systems*, vol. 50, no. 3, pp. 614-626, 2011.
- [63] K.-L. Hui, H. H. Teo and S.-Y. T. Lee, The value of privacy assurance: an exploratory field experiment, *MIS Quarterly*, pp. 19-33, 2007.
- [64] T.-M. C. Jai, L. D. Burns and N. J. King, The effect of behavioral tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers, *Computers in Human Behavior*, vol. 29, no. 3, pp. 901-909, 2013.
- [65] S. L. Jarvenpaa, N. Tractinsky and L. Saarinen, Consumer trust in an Internet store: a cross-cultural validation, *Journal of Computer-Mediated Communication*, vol. 5, no. 2, pp. 1-35, 1999.
- [66] P. Jehiel and A. Lilico, Smoking today and stopping tomorrow: a limited foresight perspective, *CESifo Economic Studies*, vol. 56, no. 2, pp. 141-164, 2010.
- [67] M. L. Jensen, J. M. Averbek, Z. Zhang, and K. B. Wright, Credibility of anonymous online product reviews: A language expectancy perspective, *Journal of Management Information Systems*, vol. 30, no. 1, pp. 293-324, 2013.
- [68] L. K. John, The consumer psychology of online privacy: insight and opportunities from behavioral decision theory, *The Cambridge Handbook of Consumer Psychology*, pp. 619-646, 2016.
- [69] L. K. John, A. Acquisti and G. Loewenstein, Strangers on a plane: Context-dependent willingness to divulge sensitive information, *Journal of Consumer Research*, vol. 37, no. 5, pp. 858-873, 2011.
- [70] T. J. Johnson and B. K. Kaye, Cruising is believing?: Comparing Internet and traditional sources on media credibility measures, *Journalism & Mass Communication Quarterly*, vol. 75, no. 2, pp. 325-340, 1998.
- [71] T. J. Johnson and B. K. Kaye, Using is believing: The influence of reliance on the credibility of online political information among politically interested Internet users, *Journalism & Mass Communication Quarterly*, vol. 77, no. 4, pp. 865-879, 2000.
- [72] M. A. Kamins and H. Assael, Two-sided versus one-sided appeals: A cognitive perspective on argumentation, source derogation, and the effect of disconfirming trial on belief change, *Journal of Marketing Research*, vol. 24, no. 1, pp. 29-39, 1987.
- [73] E. Keisidou, L. Sarigiannidis, and D. Maditinos, Consumer characteristics and their effect on accepting online shopping, in the context of different product types, *International Journal of Business Science & Applied Management*, vol. 6, no. 2, pp. 31-51, 2011.
- [74] D. J. Kim, D. L. Ferrin, and H. R. Rao, A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents, *Decision Support Systems*, vol. 44, no. 2, pp. 544-564, 2008.
- [75] D. J. Kim, Y. I. Song, S. B. Braynov, and H. R. Rao, A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives, *Decision Support Systems*, vol. 40, no. 2, pp. 143-165, 2005.

- [76] D. Kim and I. Benbasat, Trust-related arguments in Internet stores: A framework for evaluation, *Journal of Electronic Commerce Research*, vol. 4, no. 2, pp. 49-64, 2003.
- [77] H.-W. Kim, Y. Xu and S. Gupta, Which is more important in Internet shopping, perceived price or trust? *Electronic Commerce Research and Applications*, vol. 11, no. 3, pp. 241-252, 2012.
- [78] M.-J. Kim, N. Chung and C.-K. Lee, The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea, *Tourism Management*, vol. 32, no. 2, pp. 256-265, 2011.
- [79] D.-G. Ko, L. J. Kirsch and W. R. King, Antecedents of knowledge transfer from consultants to clients in enterprise system implementations, *MIS Quarterly*, vol. 29, pp. 59-85, 2005.
- [80] D. Koehn, The nature of and conditions for online trust, *Journal of Business Ethics*, vol. 43, no. 1-2, pp. 3-19, 2003.
- [81] A. Kost (2012) Woman paid to post five-star Google feedback. ABC7 News. [Online]. Available: <http://bit.ly/SnOzRi>
- [82] E. L. Krupka and R. A. Weber, Identifying social norms using coordination games: Why does dictator game sharing vary? *Journal of the European Economic Association*, vol. 11, no. 3, pp. 495-524, 2013.
- [83] H.-H. Kuan and G.-W. Bock, Trust transference in brick and click retailers: An investigation of the before-online-visit phase, *Information & Management*, vol. 44, no. 2, pp. 175-187, 2007.
- [84] A. Lang, The limited capacity model of mediated message processing, *Journal of Communication*, vol. 50, no. 1, pp. 46-70, 2000.
- [85] R. LaRose and N. J. Rifon, Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior, *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 127-149, 2007.
- [86] T. W. Lauer and X. Deng, Building online trust through privacy practices, *International Journal of Information Security*, vol. 6, no. 5, pp. 323-331, 2007.
- [87] R. S. Laufer and M. Wolfe, Privacy as a concept and a social issue: A multidimensional developmental theory, *Journal of Social Issues*, vol. 33, no. 3, pp. 22-42, 1977.
- [88] B. Liu, Sentiment analysis and opinion mining, *Synthesis Lectures on Human Language Technologies*, vol. 5, no. 1, pp. 1-167, 2012.
- [89] C. Liu, J. T. Marchewka and C. Ku, American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce, *Journal of Global Information Management (JGIM)*, vol. 12, no. 1, pp. 18-40, 2004.
- [90] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu, Beyond concern - a privacy-trust-behavioral intention model of electronic commerce, *Information and Management*, vol. 42, no. 2, pp. 289-304, 2005.
- [91] P. B. Lowry, G. Moody, A. Vance, M. Jensen, J. Jenkins, and T. Wells, Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers, *Journal of the American Society for Information Science and Technology*, vol. 63, no. 4, pp. 755-776, 2012.
- [92] P. B. Lowry, A. Vance, G. Moody, B. Beckman, and A. Read, Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites, *Journal of Management Information Systems*, vol. 24, no. 4, pp. 199-224, 2008.
- [93] P. B. Lowry, D. Zhang, L. Zhou, and X. Fu, Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups, *Information Systems Journal*, vol. 20, no. 3, pp. 297-315, 2010.
- [94] X. Luo, Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory, *Industrial Marketing Management*, vol. 31, no. 2, pp. 111-118, 2002.
- [95] N. K. Malhotra, S. S. Kim, and J. Agarwal, Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, *Information Systems Research*, vol. 15, no. 4, pp. 336-355, 2004.
- [96] R. N. Mayer, J. Huh and B. J. Cude, Cues of credibility and price performance of life insurance comparison web sites, *Journal of Consumer Affairs*, vol. 39, no. 1, pp. 71-94, 2005.
- [97] D. Mayzlin, Promotional chat on the internet, *Marketing Science*, vol. 25, no. 2, pp. 155-163, 2006.
- [98] D. H. McKnight, V. Choudhury and C. Kacmar, The impact of initial consumer trust on intentions to transact with a web site: a trust building model, *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 297-323, 2002.
- [99] D. B. Meinert, D. K. Peterson, J. R. Criswell, and M. D. Crossland, Privacy policy statements and consumer willingness to provide personal information, *Journal of Electronic Commerce in Organizations*, vol. 4, no. 1, pp. 1-17, 2006.
- [100] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon, (Do Not) Track me sometimes: Users' contextual preferences for Web tracking, *Privacy Enhancing Technologies*, vol. 2, pp. 135-154, 2015.
- [101] F. Meskaran, R. Abdullah and M. Ghazali, A conceptual framework of Iranian consumer trust in B2C electronic commerce, *Computer and Information Science*, vol. 3, no. 2, pp. 126-139, 2010.
- [102] F. Meskaran, Z. Ismail and B. Shanmugam, Online purchase intention: Effects of trust and security perception, *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 6, pp. 307-315, 2013.
- [103] M. J. Metzger, Effects of site, vendor, and consumer characteristics on web site trust and disclosure, *Communication Research*, vol. 33, no. 3, pp. 155-179, 2006.
- [104] M. J. Metzger, A. J. Flanagan and R. B. Medders, Social and heuristic approaches to credibility evaluation online, *Journal of Communication*, vol. 60, no. 3, pp. 413-439, 2010.
- [105] M. D. Odom, A. Kumar and L. Saunders, Web assurance seals: How and why they influence consumers' decisions, *Journal of Information Systems*, vol. 16, no. 2, pp. 231-250, 2002.
- [106] T. O'Donoghue and M. Rabin, The economics of immediate gratification, *Journal of Behavioral Decision Making*, vol. 13, no. 2, pp. 233-250, 2000.

- [107] T. O'Donoghue and M. Rabin, Choice and procrastination, *Quarterly Journal of Economics*, vol. 116, no. 1, pp. 121-160, 2001.
- [108] P&AB, New survey reports an increase in ID theft and decrease in consumer confidence, Privacy and American Business, conducted by Harris Interactive, Technical Report, 2005,
- [109] Y. Pan and G. M. Zinkhan, Exploring the impact of online privacy disclosures on consumer trust, *Journal of Retailing*, vol. 82, no. 4, pp. 331-338, 2006.
- [110] P. A. Pavlou, Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model, *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-134, 2003.
- [111] P. A. Pavlou and A. Dimoka, The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation, *Information Systems Research*, vol. 17, no. 4, pp. 392-414, 2006.
- [112] P. A. Pavlou, H. Liang and Y. Xue, Understanding and mitigating uncertainty in online environments: a principal-agent perspective, *MIS Quarterly*, vol. 31, no. 1, pp. 105-136, 2006.
- [113] D. Peterson, D. Meinert, J. Criswell, and M. Crossland, Consumer trust: privacy policies and third-party seals, *Journal of Small Business and Enterprise Development*, vol. 14, no. 4, pp. 654-669, 2007.
- [114] J. E. Phelps, G. D'Souza and G. J. Nowak, Antecedents and consequences of consumer privacy concerns: An empirical investigation, *Journal of Interactive Marketing*, vol. 15, no. 4, pp. 2-17, 2001.
- [115] P. Pirolli, Rational analyses of information foraging on the Web, *Cognitive Science*, vol. 29, no. 3, pp. 343-373, 2005.
- [116] E. B. Ponte, E. Carvajal-Trujillo and T. Escobar-Rodríguez, Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents, *Tourism Management*, vol. 47, pp. 286-302, 2015.
- [117] C. Pornpitakpan, The persuasiveness of source credibility: A critical review of five decades' evidence, *Journal of Applied Social Psychology*, vol. 34, no. 2, pp. 243-281, 2004.
- [118] S. Preibusch, Guide to measuring privacy concern: Review of survey and observational instruments, *International Journal of Human-Computer Studies*, vol. 71, no. 12, pp. 1133-1143, 2013.
- [119] A. R. Rao, L. Qu, and R. W. Ruekert, Signaling unobservable product quality through a brand ally, *Journal of Marketing Research*, vol. 36, no. 2, pp. 258-268, 1999.
- [120] M. Rao, How real is the Internet market in developing nations? OTI, 2002.
- [121] M. Rappa. (2003) Business models on the web. *Digital Enterprise*. [Online]. Available: <http://digitalenterprise.org/models/models.html>
- [122] S. Ray, T. Ow and S. S. Kim, Security assurance: How online service providers can influence security control perceptions and gain trust, *Decision Sciences*, vol. 42, no. 2, pp. 391-412, 2011.
- [123] P. Reinecke. (2015) E-commerce statistics for individuals. Eurostat. [Online]. Available: <http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commercestatisticsfrindividuals>
- [124] N. J. Rifon, R. LaRose, and S. Choi, Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures, *Journal of Consumer Affairs*, vol. 39, no. 2, pp. 339-362, 2005.
- [125] A. E. Schlosser, T. B. White and S. M. Lloyd, Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions, *Journal of Marketing*, vol. 70, no. 2, pp. 133-148, 2006.
- [126] J. Shim, C. Van Slyke, J. J. Jiang, and R. D. Johnson. (2004, January) Does trust reduce concern for information privacy in e-commerce?, Researchgate. [Online]. Available: https://www.researchgate.net/publication/228975626_Does_Trust_Reduce_Concern_for_Information_Privacy_in_E-Commerce
- [127] E. Silience, P. Briggs, L. Fishwick, and P. Harris, Trust and mistrust of online health sites, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, USA, 2004, pp. 663-670.
- [128] E. Silience, P. Briggs, P. Harris, and L. Fishwick, Health websites that people can trust—the case of hypertension, *Interacting with Computers*, vol. 19, no. 1, pp. 32-42, 2007.
- [129] H. A. Simon, A behavioral model of rational choice, *The Quarterly Journal of Economics*, vol. 69, no. 1, pp. 99-118, 1955.
- [130] Statista. (2016) Retail e-commerce sales in the U.S. from 2016 to 2022. Statista. [Online]. Available: <https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/>
- [131] K. J. Stewart, Trust transfer on the World Wide Web, *Organization Science*, vol. 14, no. 1, pp. 5-17, 2003.
- [132] S. S. Sundar, The MAIN model: A heuristic approach to understanding technology effects on credibility, *Digital Media, Youth, and Credibility*, vol. pp. 73-100, 2008.
- [133] P. Sztompka, *Trust: A Sociological Theory*. Cambridge: University Press, 1999.
- [134] Z. Tang, Y. Hu and M. D. Smith, Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor, *Journal of Management Information Systems*, vol. 24, no. 4, pp. 153-173, 2008.
- [135] A. N. Tariq and B. Eddaoudi, Assessing the effect of trust and security factors on consumers' willingness for online shopping among the urban Moroccans, *International Journal of Business and Management Science*, vol. 2, no. 1, pp. 17-32, 2009.
- [136] D. G. Taylor, D. F. Davis and R. Jillapalli, Privacy concern and online personalization: The moderating effects of information control and compensation, *Electronic Commerce Research*, vol. 9, no. 3, pp. 203-223, 2009.
- [137] T. S. Teo and J. Liu, Consumer trust in e-commerce in the United States, Singapore and China, *Omega*, vol. 35, no. 1, pp. 22-38, 2007.
- [138] E. G. Toms and A. R. Taves, Measuring user perceptions of web site reputation, *Information Processing & Management*, vol. 40, no. 2, pp. 291-317, 2004.

- [139] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, The effect of online privacy information on purchasing behavior: An experimental study, *Information Systems Research*, vol. 22, no. 2, pp. 254-268, 2011.
- [140] Y. C. Tsai and J. C. Yeh, Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products, *African Journal of Business Management*, vol. 4, no. 18, pp. 4057-4066, 2010.
- [141] J. Tullberg, Trust - the importance of trustfulness versus trustworthiness, *The Journal of Socio-Economics*, vol. 37, no. 5, pp. 2059-2071, 2008.
- [142] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy. (2009, September) Americans reject tailored advertising and three activities that enable it. Penn Libraries. [Online]. Available: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers
- [143] B. Tuttle. (2012) Why you shouldn't trust positive online reviews - or negative ones, for that matter. *Business Time*. [Online]. Available: <http://business.time.com/2012/08/28/why-you-shouldnt-trust-positive-online-reviews-or-negative-ones-for-that-matter>
- [144] A. Tversky and D. Kahneman. (1975) Judgment under uncertainty: Heuristics and biases, in *Utility, probability, and human decision making*. Springer. [Online]. Available: https://link.springer.com/chapter/10.1007/978-94-010-1834-0_8
- [145] H. van der Heijden and T. Verhagen, Measuring and assessing online store image: a study of two online bookshops in the Benelux, in *System Sciences*, 2002. HICSS, in *Proceedings of the 35th Annual Hawaii International Conference on*. IEEE, Hawaii, 2002, pp. 2639-2646.
- [146] R. L. Wakefield, M. H. Stocks and W. M. Wilder, The role of web site characteristics in initial trust formation, *Journal of Computer Information Systems*, vol. 45, no. 1, pp. 94-103, 2004.
- [147] H. Wang, M. K. Lee and C. Wang, Consumer privacy concerns about Internet marketing, *Communications of the ACM*, vol. 41, no. 3, pp. 63-70, 1998.
- [148] S. Wang, S. E. Beatty and W. Foxx, Signaling the trustworthiness of small online retailers, *Journal of Interactive Marketing*, vol. 18, no. 1, pp. 53-69, 2004.
- [149] J. M. Weber, D. Malhotra and J. K. Murnighan, Normal acts of irrational trust: Motivated attributions and the trust development process, *Research in Organizational Behavior*, vol. 26, pp. 75-101, 2004.
- [150] M. G. Weinberger, C. T. Allen and W. R. Dillon, Negative information: Perspectives and research directions, *Advances in Consumer Research*, vol. 8, pp. 398-404, 1981.
- [151] M. C. Weinburger and W. R. Dillon, The effects of unfavorable product information, *Advances in Consumer Research*, vol. 7, pp. 528-532, 1980.
- [152] J. D. Wells, J. S. Valacich and T. J. Hess, What signals are you sending? How website quality influences perceptions of product quality and purchase intentions, *MIS Quarterly*, vol. 35, no. 2, pp. 373-396, 2011.
- [153] A. F. Westin. *Privacy and Freedom*. New York: Atheneum, 1968.
- [154] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, The effect of online privacy policy on consumer privacy concern and trust, *Computers in Human Behavior*, vol. 28, no. 3, pp. 889-897, 2012.
- [155] L. G. Zucker, Production of trust: Institutional sources of economic structure, 1840-1920, *Research in Organizational Behavior*, vol. 8, pp. 53-111, 1986.

Appendix A: Questionnaire Items

Construct	Sub-construct	Variable		Item (translated from Italian)
		Perceived trustworthiness	Purchasing intention	
Security		ST	SP	
		ST1	SP1	The Company has published assurances from independent third parties and uses their icons on Website.
		ST2	SP2	The Company has a password-composition policy, <i>i.e.</i> , it imposes requirements for password creation on its website (<i>e.g.</i> , length, mandatory inclusion of numbers and letters, <i>etc.</i>).
		ST3	SP3	Green padlock icon is present in the location bar to the left of the web address verifying that the Company's Website uses an Extended Validation (EV) certificate.
		ST4	SP4	Several payment options are available on the website of the company (<i>e.g.</i> , credit cards, PayPal, web wallets, bank transfer, <i>etc.</i>).
Privacy		PT	PP	
	Collection	LT	LP	
		LT1	LP1	Notifications, banners and ads about products you searched for once on the company's website appear when you are visiting other websites.
		LT2	LP2	To recommend products/services that you may be interested in, the company's website asks about your tastes and preferences.
		LT3	LP3	To recommend products/services that you may be interested in, the company's website uses specific technologies to track your behavior and determine your preferences.
		LT4	LP4	The company allows access to the content of its website without registration but requires some personal information to be provided to place an order and purchase products and services from it.
		LT5	LP5	The company requires some personal information to be provided to gain access to its website and content.
		LT6	LP6	The details of a user's credit card are remembered by the company's website for future purchases.
		LT7	LP7	The user's address is remembered by the company's website for future deliveries.
	Control	NT	NP	
		NT1	NP1	The company's website (not browser) asks you to remember your login and password to quickly enter it next time you will visit it without needing to type it in again.
		NT2	NP2	The company's website asks your permission to use your current location.

<i>continuation</i>				
		NT3	NP3	The company's website allows you to register via other websites (e.g., sign up using a Facebook or Google profile).
		NT4	NP4	The company's website's mobile application cannot be installed without permission to access some information (e.g., location, device model, profile, activity history, etc.).
		NT5	NP5	The company's website's mobile application cannot be installed without permission to access some information, but you are allowed to partially edit the list of permissions.
	Awareness	AT	AP	
		AT1	AP1	The company's website clearly explains how customer information is going to be used and how it will be shared with other companies and third parties.
		AT2	AP2	Informational text about the use of cookies is clearly present on the website as a fixed banner.
		AT3	AP3	The general privacy policy is clear and easy to understand.
Reputation		RT	RP	
	Background	BT	BP	
		BT1	BP1	Key names and photos of real people behind the company's website are shown.
		BT2	BP2	The company's website carries products/services with reputable brand names.
		BT3	BP3	The company runs a business and has had a website for many years.
		BT4	BP4	The background of the company (company history and key personnel) is described on its website.
	Feedback	FT	FP	
		FT1	FP1	The company has both good and bad feedback, and positive and negative reviews from other users and customers on independent websites and forums.
		FT2	FP2	The company has both good and bad feedback, and positive and negative reviews from other users and customers on its website.
		FT3	FP3	The company has a high ranking in traditional media (TV, radio, printed editions, etc.).
		FT4	FP4	The company has a high ranking in online sources (e.g., BizRate, Consumer reports Online eRatings, etc.).
		FT5	FP5	The company has good feedback and positive reviews from other users and customers on its website.
		FT6	FP6	There is a widget on the company's website that tells you which people with whom you are friends on Facebook like this company and its products/services.
Website quality		QT	QP	

<i>continuation</i>				
		QT1	QP1	The visual appearance and manner of the company's website is not professional (amateur looking).
		QT2	QP2	The company has broken links and typographical errors on its website.
		QT3	QP3	The company's website has suspicious banners, adverts, and links to third-party unrelated websites.

Appendix B: Final Questionnaire and Summary Statistics

1. What do you think was the purpose of the experiment? (Max 200 words)
2. How difficult was it for you to make a decision? (1= Not Difficult at All (7%), 2 = Not Very Difficult (49%), 3 = Somewhat Difficult (39%), 4 = Very Difficult (5%))
3. What is your gender (1 = Male (37%), 2 = Female (63%))
4. What is your age? (1 = Less than 18 years (0%), 2 = 18–25 years (0%), 3 = 26–30 years (1%), 4 = 31–35 years (10%), 5 = 36–40 years (44%), 6 = More than 41 years (45%))
5. What is your field of study? (1 = Social Sciences (Economics, Sociology, Law, *etc.*) (29%); 2 = Technical sciences (Informatics, Engineering, Architecture, *etc.*) (32%), 3 = Medical sciences (Medicine, Nursing, Pharmaceuticals, *etc.*) (2%), 4 = Humanities and Arts (Literature, Languages, Arts, *etc.*) (23%), 5 = Natural Sciences (Chemistry, Physics, Mathematics, *etc.*) (14%), 6 = Education science and pedagogics (0%), 7 = Agriculture (Agriculture, Veterinary, *etc.*) (0%), 8 = Other Applied Sciences (specify) (0%)).
6. What is the highest level of education you have completed? (1 = High school diploma or less (36%), 2 = Secondary school (17%), 3 = Bachelor's Degree (38%), 4 = Master's Degree (7%), 5 = Doctoral Degree (3%), 6 = Other (specify) (0%))
7. What is your nationality? (1= Italian (99%), 2 = Other (1%))
8. Did your parents complete their secondary education? (1 = Neither of my parents completed secondary education (26%), 2 = Only one of my parents completed secondary education (37%), 3 = Both parents completed secondary education (37%))
9. Where did you live for most of your life? (1 = Village with less than 1,000 inhabitants (7%), 2 = Town with 1,000–10,000 inhabitants (16%), 3 = City with 10,001–100,000 inhabitants (32%), 4 = City with 100,000–1,000,000 inhabitants (43%), 5 = Big city with more than 1 million inhabitants (2%)). ("Urban" index was coded as 1 if the subject lived in a city with >10,000 inhabitants (*i.e.*, if answered 3, 4, or 5 in Q9), 0 otherwise.)
10. What is your main source of income? (1 = Job (full-time) (67%), 2 = Job (part-time) (0%), 3 = Scholarship (27%), 4 = Parents (5%), 5 = Spouse (1%), 6 = Other relatives or members of family (0%), 7 = Bank loan (0%), 8 = Other (specify) (0%))
11. How much do you spend every month? (Including food, clothes, rent, utilities (heating, water), education, entertainment, *etc.*) (1 = Less than 500 Euro (2%), 2 = 501–800 Euro (21%), 3 = 801–1200 Euro (32%), 4 = 1201–2000 Euro (31%), 5 = More than 2000 Euro (15%), 6 = Prefer not to answer (0%))
12. Which programming languages are you able to use (more than one answer is allowed)? (1 = Java / Java Script, 2 = C / C++, 3 = Python, 4 = Ruby, 5 = Matlab, 6 = HTML, 7 = R, 8 = I do not know any programming languages, 9 = Other.) (Sixty three percent of respondents did not know any programming language. Respondents who knew at least one, on average, knew 2 programming languages. "Technical proficiency" index was coded as 1 if the subject knew at least one programming language (Q12), 0 otherwise.)
13. For how many years have you used the Internet? (1 = Less than 1 year (0%), 2 = 1–2 years (2%), 3 = 3–5 years (7%), 4 = 5–8 years (11%), 5 = More than 8 years (80%))
14. How many hours do you spend online per week? (Mean = 17.96; sd = 15.26; min = 0; max = 70)
15. How often do you use the Internet for each of the following purposes: (1 = Often; 2 = Sometimes; 3 = Never)
 - (a) Entertainment, (b) Educational, (c) Work-related research, (d) Personal finance (banking, stock trading), (e) Current events (news, sports, weather), (f) Travel-related (research, reservations), (g) Product information gathering, (h) Making purchases from online merchants, (i) Communicating with others (chat/email/social network), (j) Other (specify.) (Using a single-factor measurement model we calculated two indices: a) an index of using the Internet for utilitarian purposes (mean = -6.32e-09; sd = 0.15, min = -0.33; max = 0.28; Cronbach's alpha = 0.4625) based on the responses about the use of the Internet for educational, work-related, personal finance, and product-information gathering purposes; and b) an index of using the Internet for hedonic purposes (mean = 1.66e-09; sd = 0.19, min = -0.42; max = 0.30; Cronbach's alpha = 0.6110) based on the responses about the use of Internet for entertainment, current events, travel-related decisions, making purchases, and communication purposes.)

16. How often do you buy products/services online that cost: (a) < 50 Euro, (b) 50–100 Euro, (c) 101–300 Euro, (d) 301–500 Euro, (e) 501–1000 Euro, (f) More than 1000 Euro. (1 = Never, 2 = Once a year, 3 = Several times a year, 4 = Once a month, 5 = Several times a month, 6 = Once a week, 7 = Several times a week.) (Using a single-factor measurement model we calculated an “Online shopping frequency” index (mean = $-2.29e-09$; sd = 0.56, min = -0.37; max = 3.30; Cronbach’s alpha = 0.8854) based on the responses.)

17. I prefer to buy products and services from physical store rather than online. (1 = I totally disagree (10%), 2 = I somewhat disagree (47%), 3 = I somewhat agree (31%), 4 = I totally agree (12%))

18. What agencies that specialize in online privacy and security are you familiar with? More than one answer is allowed. (1 = VeriSign (44%), 2 = Entrust (15%), 3 = TRUSTe (35%), 4 = BBBOnline (Better Business Bureau Online) (1%), 5 = AIPC Webtrust (1%), 6 = WebAssured (8%), 7 = Pretty Good Privacy (6%), 8 = Thawte (8%), 9 = Other (specify) (29%).) (Sixty-nine percent of the respondents were familiar with one agency, 20% – with two agencies, 8% – with three agencies, 3% – with four agencies, and 1% – with five agencies.)

19. Do you recognize the label that represents the compliance of the website with the Extended Validation certificate? (1 = No (55%), 2 = Yes (45%))

20. Please explain what the Extended Validation certificate means? (55% provided the correct meaning)

21. Please explain what do cookies mean? (69% provided the correct meaning)

22. Are you concerned about your privacy online? (1 = Not concerned at all (6%), 2 = Somewhat unconcerned (28%), 3 = Somewhat concerned (56%), 4 = Very concerned (10%))

23. Rate your level of concern over the following Internet issues:

- (a) It’s too hard to use
- (a) It’s too hard to find what I want
- (b) Someone could be monitoring what I do online
- (c) It’s too expensive and pornography is too easily accessible
- (d) It’s too cluttered
- (e) It’s too slow
- (f) I get too much junk email
- (g) My personal information will be stolen
- (h) Someone will misuse the personal information I give them
- (i) Information will be censored
- (j) Other (specify)

(1 = Not at all concerned, 2 = Somewhat unconcerned, 3 = Somewhat concerned, 4 = Very concerned.)

(Using a single-factor measurement model we calculated an index of privacy being a motivation for concern related to the use of the Internet (mean = $-1.69e-09$; sd = 0.39, min = -1.1; max = 0.52; Cronbach’s alpha = 0.7820) based on the responses to statements 3, 9 and 10 of Q23.)

24. If asked to provide personal information, how often (%) do you refuse to give the requested personal information / leave the website? (mean = 45.09%; sd = 31.18; min = 0%; max = 100%)

25. If you do provide personal information to websites, how often (%) do you provide false information (if at all)? (mean = 9.77%; sd = 16.26; min = 0%; max = 90%)

26. If you have refused to disclose personal information or given falsified information, how important to you were the following issues:

- (a) I am unfamiliar with how the technology works
- (b) I am unfamiliar with the company/individual running the site

- (c) The company/individual running the site does not have a good reputation
- (d) I don't trust the company/individual running the site
- (e) The site does not disclose how they plan to use my information
- (f) The value I will receive from the site is not worth the information I give
- (g) I generally prefer to be anonymous
- (h) They asked for particularly sensitive pieces of information
- (i) I am concerned that the information will be intercepted or stolen
- (j) It takes too much time to fill out the forms
- (k) I am concerned I will receive junk mail if I give my home address
- (l) I am concerned I will receive junk email if I give my email address
- (m) I am concerned I will receive junk SMS/calls if I give my (mobile) telephone number
- (n) Other (specify)

(1 = Not one of my reasons, 2 = Not very important, 3 = Somewhat important reason, 4 = Very important reason)

(Using a single-factor measurement model we calculated two indices: a) an index of privacy concern giving the reason for not providing or providing falsified information (mean = 0.008; sd = 0.47, min = -1.97; max = 0.49; Cronbach's alpha = 0.7980) based on the responses to statements 5-9; and b) an index of trust issues giving the reason for not providing or providing falsified information (mean = -0.003; sd = 0.41, min = -1.68; max = 0.28; Cronbach's alpha = 0.9015) based on the responses to statements 2-4 in Q26.)

27. How willing are you to provide personally identifiable information and demographics to websites? (1 = Not willing at all (3%), 2 = Not very willing (63%), 3 = I am indifferent (19%), 4 = I would not mind (11%), 5 = Very willing (3%))

28. Would you be more willing to provide personally identifiable information and demographics for online advertising purposes if the website compensated you for your information? (1 = No (62%), 2 = Yes (38%))

29. How willing are you to provide information about your tastes, interests and preferences without personal identification to websites? (1 = Not willing at all (5%), 2 = Not very willing (28%), 3 = I am indifferent (28%), 4 = I would not mind (30%), 5 = Very willing (9%))

30. Would you be more willing to provide personal information about your tastes, interests, and preferences for online advertising purposes if the website compensated you for your information? (1 = No (31%), 2 = Yes (69%))

31. Have you personally experienced incidents whereby your personal information was used by some company or e-commerce website without your authorization? (1 = No (66%), 2 = Yes (34%))

32. Have you personally been the victim of what you felt was an invasion of privacy? (1 = No (57%), 2 = Yes (43%))

33. Please indicate the extent to which you (dis)agree with the following statements:

- (a) Consumers have lost all control over how personal information is collected and used by companies (reverse coded)
- (b) Most businesses handle the personal information they collect about consumers in a proper and confidential way
- (c) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today

(1 = Strongly Agree, 2 = Somewhat agree, 3 = Somewhat disagree, 4 = Strongly disagree)

(We computed a Westin's Privacy index [153]: 1 = Unconcerned (0-1 privacy concerned answers); 2 = Pragmatists (2 privacy concerned answers); 3 = Fundamentalists (3 privacy concerned answers).)

34. If you are a member of an online social network, which do you use the most actively? (more than one answer is allowed) (1 = Facebook (56% use it), 2 = Google + (19%), 3 = Twitter (9%), 4 = My Space (0%), 5 = Instagram (10%), 6 = Other (specify) (9%), 7 = I am not a member of any online social network (29%))
35. How many connections do you have on Facebook? (1 = less than 50 (20%), 2 = 51–100 (15%), 3 = 101–200 (9%), 4 = 201–300 (4%), 5 = 301–500 (9%), 6 = 501–700 (1%), 7 = 701–1000 (1%), 8 = 1001–2000, 9 = More than 2000 (0%), 10 = I do not have a profile on Facebook (39%))
36. What do you use as your user name on Facebook? (1 = Real name (57%), 2 = Pseudonym, and nobody knows who I am in real life (3%), 3 = Pseudonym, but everybody knows who I am in real life (0%), 4 = I do not have a Facebook account (39%))
37. What do you use as your profile picture in your primary social network? (1 = Real photo of me (42%), 2 = Real photo of me with other person/people (6%), 3 = Photo of other person or celebrity (1%), 4 = Photo/image of non-human (5%), 5 = No photo at all (4%), 6 = I do not have a Facebook account (39%), 7 = Other (3%))
38. What are your privacy settings on Facebook? (1 = Public. Everybody can get access to my profile and read my entries (7%), 2 = Private. Only my friends can get access to my profile and read my entries (36%), 3 = My profile and entries are mostly public and partially private (3%), 4 = My profile and entries are mostly private and partially public (12%), 5 = I have different accounts for public and private entries (0%), 6 = I do not have a Facebook account (39%), 7 = Other (please describe in detail) (3%))
39. Do you ever change your privacy settings on Facebook? (1 = Never (20%), 2 = I changed privacy settings on Facebook immediately after registration (20%), 3 = I changed privacy settings on Facebook several times (20%), 4 = I changed privacy settings on Facebook after someone misused my personal information (1%), 5 = I do not have a Facebook account (39%), 6 = Other (please describe in detail) (0%))
40. What is your favorite movie? (1 = Specify (85%), 2 = I do not wish to say (15%))
41. What is your favorite book? (1 = Specify (82%), 2 = I do not wish to say (18%))
42. What is your favorite sport? (1 = Specify (89%), 2 = I do not wish to say (11%))
43. What is your hobby? (1 = Specify (91%), 2 = I do not wish to say (9%))
44. Imagine that two people do the same job in the same company. Both have the same qualification, but person A works more productively than person B. Is it fair that person A gets a larger remuneration? (1 = Yes, it's fair (94%), 2 = No, it's unfair (6%))
45. In general, one can trust people . . . (1 = I totally agree (4%), 2 = I somewhat agree (43%), 3 = I somewhat disagree (50%), 4 = I totally disagree (3%))
46. Nowadays one cannot rely on anyone . . . (1 = I totally agree (7%), 2 = I somewhat agree (67%), 3 = I somewhat disagree (23%), 4 = I totally disagree (3%))
47. When dealing with strangers it's better to be careful before trusting them. . . (1 = I totally agree (11%), 2 = I somewhat agree (52%), 3 = I somewhat disagree (37%), 4 = I totally disagree (0%))
48. Do you think that the majority of people. . . (1 = . . . would exploit you if they had an opportunity . . . " (45%), 2 = . . . would try to be fair to you . . . (55%))
49. Do you think that people most of the times. . . (1 = . . . try to be considerate of others (72%), 2 = . . . follow their own interests (28%).) (Using a single-factor measurement model we calculated a "trust disposition" index based on the responses to Q45-49 (mean = 2.13e-09; sd = 0.42; min = -0.91; max = 0.83; Cronbach's alpha = 0.7582).

Appendix C: Summary Statistics of Values

Summary Statistics of the Values of Perception of Trustworthiness						
Variable	Mean	Median	Std. Dev.	Variance	Min	Max
QT3	2.97	3	1.98	3.92	1	11
QT1	3.30	3	1.85	3.43	1	10
QT2	3.31	3	2.17	4.70	1	12
LT6	3.69	3	2.66	7.05	1	11
LT1	3.91	4	2.31	5.33	1	10
NT4	4.16	4	2.64	6.96	1	12
FT6	4.53	4	2.63	6.93	1	12
NT2	4.74	4	2.65	7.03	1	12
NT3	4.90	5	2.60	6.76	1	12
LT2	4.92	5	2.57	6.59	1	11
LT3	5.03	4	2.64	6.99	1	11
LT5	5.13	5	2.66	7.05	1	12
LT7	5.40	5	2.73	7.44	1	12
LT4	5.41	6	2.74	7.49	1	12
NT5	5.61	6	2.66	7.06	1	12
NT1	5.69	6	2.82	7.94	1	12
FT1	5.81	6	2.41	5.81	1	12
FT2	6.07	6	2.53	6.42	1	12
AT2	6.18	6	2.84	8.06	1	12
BT2	6.52	6	2.73	7.47	1	12
BT4	6.57	6	2.65	7.02	1	12
FT5	6.80	7	2.77	7.68	1	12
FT4	6.84	7	2.87	8.26	1	12
BT1	7.06	7	2.90	8.38	1	12
FT3	7.12	7	2.82	7.93	1	12
ST4	7.22	7	3.01	9.06	1	12
BT3	7.46	8	2.80	7.84	1	12
ST1	7.53	8.5	3.12	9.72	1	12
ST3	7.57	8	2.81	7.87	1	12
AT3	7.75	8	3.04	9.26	1	12
AT1	7.84	8	2.91	8.50	1	12
ST2	7.93	8.5	2.85	8.15	1	12
Summary Statistics of the Value of Purchasing Intention						
QP3	2.83	2	2.06	4.26	1	12
QP1	3.04	3	1.85	3.43	1	10
QP2	3.26	3	2.30	5.27	1	12
LP6	4.61	4	3.13	9.80	1	12
LP1	4.73	5	2.54	6.47	1	11
NP4	4.92	5	2.82	7.94	1	12
LP5	5.83	6	2.74	7.49	1	12
NP2	5.97	6	2.78	7.73	1	12
LP4	6.05	7	2.92	8.51	1	12
NP3	6.08	6	2.78	7.71	1	12
FP1	6.20	6	2.64	6.95	1	12
LP2	6.24	6	2.79	7.79	1	12
NP5	6.26	6	2.74	7.51	1	12
FP6	6.48	6.5	2.98	8.87	1	12
FP2	6.53	6	2.72	7.41	1	12
NP1	6.59	7	2.91	8.47	1	12
LP3	6.59	7	2.83	8.00	1	12
AP2	6.61	7	2.87	8.22	1	12
LP7	6.69	7	2.97	8.83	1	12
BP4	7.20	7	2.47	6.08	1	12
BP1	7.58	8	2.68	7.20	1	12
FP4	7.79	8	2.87	8.25	1	12
SP1	7.80	8	3.19	10.16	1	12

Appendix D: Confirmatory Factor Analysis of the Measurement Model

Confirmatory Factor Analysis (CFA) of the Measurement Model of Perceived Trustworthiness

Construct	Sub- construct	Variable	Factor loading	Uniqueness	Cronbach's α
Security		ST			0.8952
		ST1	0.7607	0.4213	
		ST2	0.8676	0.2473	
		ST3	0.7988	0.3619	
		ST4	0.8263	0.3172	
Privacy		PT			0.8688
	Collection	LT	0.8808	0.2243	0.8569
		LT1	0.5403	0.7081	
		LT2	0.6878	0.5269	
		LT3	0.7007	0.5091	
		LT4	0.6884	0.5261	
		LT5	0.7830	0.3869	
		LT6	0.6496	0.5780	
		LT7	0.6924	0.5206	
	Control	NT	0.8562	0.2669	0.8415
		NT1	0.8548	0.2693	
		NT2	0.6850	0.5308	
		NT3	0.7157	0.4878	
		NT4	0.6448	0.5842	
		NT5	0.8113	0.3417	
		NT6	0.7032	0.5055	
	Awareness	AT	0.6990	0.5114	0.8615
		AT1	0.6876	0.5271	
		AT2	0.8604	0.2597	
		AT3	0.7949	0.3681	
		AT4	0.7417	0.4498	
Reputation		RT			0.9094
	Background	BT	0.8744	0.2354	0.9030
		BT1	0.8743	0.2357	
		BT2	0.8268	0.3164	
		BT3	0.8518	0.2745	
		BT4	0.7742	0.4007	
		BT5	0.8525	0.2733	
	Feedback	FT	0.8744	0.2354	0.8990
		FT1	0.8743	0.2357	
		FT2	0.7830	0.3869	
		FT3	0.7273	0.4711	
		FT4	0.8488	0.2795	
		FT5	0.6288	0.6047	
		FT6	0.7950	0.3679	
		FT7	0.8447	0.2864	
Website quality		QT			0.6458
		QT1	0.4868	0.7805	
		QT2	0.6943	0.5180	
		QT3	0.5821	0.6611	
Security		ST			0.8952
		ST1	0.7607	0.4213	

<i>continuation</i>					
		ST3	0.7988	0.3619	
		ST4	0.8263	0.3172	
Privacy		PT			0.8688
	Collection	LT	0.8808	0.2243	0.8569
		LT1	0.5403	0.7081	
		LT2	0.6878	0.5269	
		LT3	0.7007	0.5091	
		LT4	0.6884	0.5261	
		LT5	0.7830	0.3869	
		LT6	0.6496	0.5780	
		LT7	0.6924	0.5206	
	Control	NT	0.8562	0.2669	0.8415
		NT1	0.8548	0.2693	
		NT2	0.6850	0.5308	
		NT3	0.7157	0.4878	
		NT4	0.6448	0.5842	
		NT5	0.8113	0.3417	
		NT6	0.7032	0.5055	
	Awareness	AT	0.6990	0.5114	0.8615
		AT1	0.6876	0.5271	
		AT2	0.8604	0.2597	
		AT3	0.7949	0.3681	
		AT4	0.7417	0.4498	
Reputation		RT			0.9094
	Background	BT	0.8744	0.2354	0.9030
		BT1	0.8743	0.2357	
		BT2	0.8268	0.3164	
		BT3	0.8518	0.2745	
		BT4	0.7742	0.4007	
		BT5	0.8525	0.2733	
	Feedback	FT	0.8744	0.2354	0.8990
		FT1	0.8743	0.2357	
		FT2	0.7830	0.3869	
		FT3	0.7273	0.4711	
		FT4	0.8488	0.2795	
		FT5	0.6288	0.6047	
		FT6	0.7950	0.3679	
		FT7	0.8447	0.2864	
Website quality		QT			0.6458
		QT1	0.4868	0.7805	
		QT2	0.6943	0.5180	
		QT3	0.5821	0.6611	

Confirmatory Factor Analysis (CFA) of the Measurement Model of Purchasing Intention

Construct	Sub-construct	Variable	Factor loading	Uniqueness	Cronbach's α
Security		SP			0.9030
		SP1	0.7419	0.4497	
		SP2	0.8297	0.3116	
		SP3	0.8263	0.3173	
		SP4	0.8642	0.2531	
Privacy		PP			0.8659
	Collection	LP	0.8671	0.2481	0.8748
		LP1	0.6758	0.5432	
		LP2	0.7736	0.4015	
		LP3	0.7250	0.4744	
		LP4	0.7247	0.4748	
		LP5	0.7093	0.4969	
		LP6	0.6419	0.5880	
		LP7	0.6875	0.5273	
	Control	NP	0.8048	0.3523	0.8437
		NP1	0.8027	0.3557	
		NP2	0.6973	0.5137	
		NP3	0.7415	0.4502	
		NP4	0.6251	0.6093	
		NP5	0.7797	0.3921	
	Awareness	AP	0.7428	0.4482	0.8598
		AP1	0.7377	0.4558	
		AP2	0.8675	0.2474	
		AP3	0.7884	0.3784	
Reputation		AP4	0.7343	0.4608	0.9334
		RP			
	Background	BP	0.9058	0.1796	
		BP1	0.9059	0.1794	
		BP2	0.8440	0.2877	
		BP3	0.8236	0.3216	
		BP4	0.8471	0.2824	
	Feedback	BP5	0.8418	0.2913	
		FP	0.9058	0.1796	
		FP1	0.9059	0.1794	
		FP2	0.7214	0.4796	
		FP3	0.6891	0.5252	
		FP4	0.7841	0.3852	
		FP5	0.6604	0.5639	
		FP6	0.7635	0.4170	
Website		FP7	0.8069	0.3489	
		QP			0.6895
		QP1	0.5677	0.6777	
		QP2	0.7473	0.4416	
		QP3	0.5594	0.6871	

Appendix E: Structural Equation Model Estimation Results

Structural Equation Model (SEM) Estimation Results

Latent variable	Item variable	Stand. path coefficient	p-value	AVE	CR	R-sq
Security ST	ST1	0.757	0.000	0.681	0.895	0.573
	ST2	0.892	0.000			0.795
	ST3	0.816	0.000			0.666
	ST4	0.830	0.000			0.689
SP	SP1	0.740	0.000	0.680	0.894	0.548
	SP2	0.841	0.000			0.708
	SP3	0.831	0.000			0.690
	SP4	0.880	0.000			0.774
Privacy Collection						
LT	LT1	0.579	0.000	0.448	0.849	0.335
	LT2	0.739	0.000			0.547
	LT3	0.705	0.000			0.498
	LT4	0.609	0.000			0.371
	LT5	0.753	0.000			0.566
	LT6	0.553	0.000			0.306
	LT7	0.719	0.000			0.516
LP	LP1	0.709	0.000	0.488	0.869	0.503
	LP2	0.806	0.000			0.650
	LP3	0.733	0.000			0.537
	LP4	0.616	0.000			0.379
	LP5	0.708	0.000			0.502
	LP6	0.583	0.000			0.340
Control	LP7	0.713	0.000			0.509
NT	NT1	0.592	0.000	0.523	0.844	0.351
	NT2	0.722	0.000			0.522
	NT3	0.671	0.000			0.451
	NT4	0.877	0.000			0.769
	NT5	0.722	0.000			0.522
NP	NP1	0.596	0.000	0.511	0.838	0.355
	NP2	0.761	0.000			0.579
	NP3	0.667	0.000			0.445
	NP4	0.813	0.000			0.661
	NP5	0.717	0.000			0.514
Awareness AT	AT1	0.976	0.000	0.707	0.887	0.952
	AT2	0.709	0.000			0.503
	AT3	0.817	0.000			0.667
AP	AP1	0.955	0.000	0.688	0.867	0.913
	AP2	0.707	0.000			
Reputation	AP3	0.808	0.000			0.652
Background						
BT	BT1	0.856	0.000	0.702	0.904	0.732
	BT2	0.850	0.000			0.723
	BT3	0.765	0.000			0.585
	BT4	0.876	0.000			0.767
BP	BP1	0.850	0.000	0.722	0.912	0.722
	BP2	0.839	0.000			0.704
	BP3	0.856	0.000			0.732
Feedback	BP4	0.855	0.000			0.731
FT	FT1	0.771	0.000	0.610	0.903	0.595
	FT2	0.722	0.000			0.522
	FT3	0.789	0.000			0.623

<i>continuation</i>						
	FT4	0.863	0.000			0.745
	FT5	0.859	0.000			0.739
	FT6	0.660	0.000			0.435
FP	FP1	0.700	0.000	0.554	0.880	0.489
	FP2	0.615	0.000			0.378
	FP3	0.755	0.000			0.569
	FP4	0.854	0.000			0.730
	FP5	0.814	0.000			0.662
Website quality	FP6	0.704	0.000			0.495
QT	QT1	0.504	0.000	0.452	0.696	0.254
	QT2	0.903	0.000			0.815
	QT3	0.535	0.000			0.287
QP	QP1	0.556	0.000	0.517	0.743	0.309
	QP2	1.000	0.000			1.000
	QP3	0.492	0.000			0.242

Note: R-squared is equal to Bentler-Raykov squared multiple correlation coefficient.

Structural Model Structural Equation Model (SEM) Estimation Results

Latent variable	Item variable	Stand. path coefficient	p-value	AVE	CR	R-sq
Trust (T)	ST	0.899	0.000	0.618	0.912	0.808
	QT	0.224	0.039			0.050
	BT	0.905	0.000			0.819
	FT	0.863	0.000			0.745
	AT	0.869	0.000			0.755
	NT	0.744	0.000			0.553
	LT Control variables:	0.771	0.000			0.59
	Q3: Female	-0.054	0.000			
	Q4: Age	-0.214	0.019			
	Q9: Urban	0.021	0.828			
	Q10: Income source	-0.230	0.019			
	Q11: Spending	-0.065	0.498			
	Q12: Programming languages	0.070	0.489			
	Q13: Internet experience	0.233	0.022			
	Q16: Online shopping frequency	0.040	0.698			
	Q17: Online shopping preference	-0.073	0.480			
	Q18: Familiarity with	0.014	0.889			
	privacy agencies					
	Q20: Correct explanation for EVC	-0.136	0.157			
	Q21: Correct explanation for cookies	0.038	0.703			
	Q22: General privacy concern	-0.170	0.053			
	Q27: Willingness to reveal PII	0.059	0.553			
	Q32: Privacy invasion	-0.041	0.690			
	Q33: Westin's privacy index	-0.174	0.065			
	Q35: Number of	-0.599	0.000			
	Facebook connections					
	Q36: Name in Facebook	0.376	0.006			
	Q49: Index of trust disposition	-0.027	0.789			
Purchase intention (P)	SP	0.942	0.000	0.664	0.925	0.887
	QP	0.126	0.296			0.016
	BP	0.929	0.000			0.863
	FP	0.910	0.000			0.829
	AP	0.902	0.000			0.814
	NP	0.761	0.000			0.580
	LP Control variables:	0.810	0.000			0.65
	Q3: Female	0.011	0.819			
	Q4: Age	-0.136	0.129			
	Q9: Urban	-0.075	0.422			
	Q10: Income source	-0.191	0.052			
	Q11: Spending	-0.042	0.651			
	Q12: Programming languages	0.090	0.358			
	Q13: Internet experience	0.289	0.002			
	Q16: Online shopping frequency	0.031	0.751			
	Q17: Online shopping preference	-0.132	0.183			
	Q18: Familiarity with	0.012	0.904			
	privacy agencies					
	Q20: Correct explanation for EVC	-0.091	0.357			
	Q21: Correct explanation for	-0.008	0.936			
	cookies					
	Q22: General privacy concern	-0.187	0.028			
	Q27: Willingness to reveal PII	0.112	0.237			
	Q32: Privacy invasion	0.044	0.660			
	Q33: Westin's privacy index	-0.152	0.094			
	Q35: Number of	-0.459	0.002			
	Facebook connections					
	Q36: Name in Facebook	0.174	0.196			
	Q49: Index of trust disposition	-0.039	0.696			

Appendix F: Goodness of Fit Test Results

	Absolute fit indices		Incremental fit indices	
	RMSEA	SRMR	CFI	TLI
Acceptable values	≤ 0.08	≤ 0.08	≥ 0.90	≥ 0.90
Source	Browne	Hu and	Hair	Hu and
	et al.	Bentler	et al.	Bentler
	[15]	[60]	[55]	[60]
Measurement model				
Security	0.057	0.029	0.994	0.989
Collection	0.084	0.082	0.958	0.941
Control	0.108	0.073	0.955	0.924
Awareness	0.080	0.016	0.996	0.982
Background	0.076	0.028	0.989	0.979
Feedback	0.105	0.055	0.953	0.928
Website quality	0.026	0.031	0.999	0.997
Structural model	0.082	0.092	0.922	0.893

Appendix G: Correlation and Covariance Matrices

Covariance Matrix

	ST	QT	BT	FT	AT	NT	LT	SP	QP	BP	FP	AP	NP	P
ST														
QT	-0.052													
BT	0.067	-0.054												
FT	0.197	-0.058	0.307											
AT	0.125	-0.005	-0.025	0.177										
NT	0.089	0.070	0.141	0.328***	0.098									
LT	0.200		0.348**	0.426***	0.459	0.459***								
SP	1.023***													
QP		0.909***					0.072							
BP			0.707***				-0.193	0.049						
FP				0.402***			-0.168	0.080	0.203					
AP					0.801***		-0.153	0.030	0.143	0.063				
NP						0.529***	-0.136	0.035	0.241	0.323**	0.082			
LP							-0.172	-0.007	0.147	0.319*		0.093		0.456***
T														0.931***

Correlation Matrix

	ST	QT	AT	NT	LT	FT	BT	SP	QP	AP	NP	LP	FP	BP
ST	1.000													
QT	0.122	1.000												
AT	0.835***	0.105	1.000											
NT	0.630***	0.256***	0.578***	1.000										
LT	0.640***	0.365***	0.620***	0.790***	1.000									
FT	0.796***	0.286***	0.768***	0.685***	0.786***	1.000								
BT	0.830***	0.155*	0.753***	0.664***	0.727***	0.852***	1.000							
SP	0.949***	0.124	0.777***	0.551***	0.539***	0.717***	0.760***	1.000						
QP	0.057	0.922***	0.110	0.155*	0.290***	0.256***	0.103	0.077	1.000					
AP	0.844***	0.137	0.194***	0.512***	0.539***	0.716***	0.734***	0.876***	0.105	1.000				
NP	0.675***	0.200**	0.551***	0.747***	0.622***	0.6013***	0.604***	0.697***	0.154*	0.643***	1.000			
LP	0.655***	0.308***	0.564***	0.525***	0.712***	0.649***	0.610***	0.683***	0.262***	0.660***	0.805***	1.000		
FP	0.800***	0.251***	0.7208***	0.513***	0.607***	0.808***	0.712***	0.847***	0.235**	0.818***	0.736***	0.803***	1.000	
bp	0.861***	0.166*	0.7457***	0.562***	0.587***	0.776***	0.880***	0.890***	0.125	0.851***	0.727***	0.728***	0.866***	1.000

Appendix H: Summary of the Hypotheses Test Results

Hypothesis	Description	Result
H1a	Privacy → Trust:	
	AT → T	Supported (p< 0.001)
	NT → T	Supported (p< 0.001)
	LT → T	Supported (p< 0.001)
H1b	Privacy → Purchasing intentions:	
	AP → P	Supported (p< 0.001)
	NP → P	Supported (p< 0.001)
	LP → P	Supported (p< 0.001)
H2a	Security → Trust:	
	ST → T	Supported (p< 0.001)
H2b	Security → Purchasing intentions:	
	SP → P	Supported (p< 0.001)
H3a	Website quality → Trust:	
	QT → T	Supported (p< 0.05)
H3b	Website quality → Purchasing intentions:	
	QP → P	Not supported
H4a	Reputation → Trust:	
	BT → T	Supported (p< 0.001)
	FT → T	Supported (p< 0.001)
H4b	Reputation → Purchasing intentions:	
	BP → P	Supported (p< 0.001)
	FP → P	Supported (p< 0.001)
H5a	FT1 > FT2	Not supported
	FP1 > FP2	Not supported
H5b	FT1 < FT5	Supported (p< 0.001)
	FT2 < FT5	Supported (p< 0.001)
	FP1 < FP5	Supported (p< 0.001)
	FP2 < FP5	Supported (p< 0.001)
H5c	FT3 > FT4	Not supported
	FP3 > FP4	Supported (p< 0.05)
H5d	LT4 > LT5	Not supported
	LP4 > LP5	Not supported
H5e	LT2 > LT3	Not supported
	LP2 > LP3	Not supported
H5f	LT1 < LT3	Supported (p< 0.001)
	LP1 < LP3	Supported (p< 0.001)
H5g	NT4 < NT5	Supported (p< 0.001)
	NP4 < NP5	Supported (p< 0.001)
H6	Trust ~ Purchasing intentions:	
	T ~ P	Supported (p< 0.001)
	AT ~ AP	Supported (p< 0.001)
	NT ~ NP	Supported (p< 0.001)
	LT ~ LP	Supported (p< 0.001)
	ST ~ SP	Supported (p< 0.001)
	QT ~ QP	Supported (p< 0.001)
	BT ~ BP	Supported (p< 0.001)
	FT ~ FP	Supported (p< 0.001)