Electron Commer Res (2014) 14:459–496
DOI 10.1007/s10660-014-9148-1

An examination of trust assurances adopted by top internet retailers: unveiling some critical determinants

Farhod P. Karimov · Malaika Brengman

Published online: 23 September 2014

Abstract This paper investigates the different trust assurances adopted by internet retailers and tries to identify a link between the characteristics of an online vendor (i.e., cost of merchandise sold, reputation, offline presence, etc…) and the specific types of trust assurances applied. The findings demonstrate that e-retailers with a relatively stronger reputation rely more on internally provided e-assurance mechanisms, such as a privacy policy or a money back guarantee, and that they make less use of third party trust endorsements. Internally-provided e-assurances also appear to be utilized more by e-retailers putting more expensive products on the market and less by those selling cheaper products. The findings regarding externally-provided e-assurances also show that third party trust endorsements such as *privacy seals*, *security seals* and *award seals* are adopted almost exclusively by e-retailers who sell more expensive products as compared to those selling products lower in monetary value. The results demonstrate that these findings regarding the impact of the '*monetary value of goods traded*' on the adoption of externally-provided e-assurances remain valid when controlling for '*reputation*' and '*offline presence*'. The results also reveal that total seal investments are higher among e-commerce companies with a weaker '*reputation*', among those '*without offline presence*', and among e-tailers selling relatively '*more expensive merchandise*'.

Keywords Trust assurances · Trust seals · B2C e-commerce · Content analysis

F. P. Karimov (✉)
Department of Business, Westminster International University in Tashkent, 12 Istiqbol St., Tashkent, Uzbekistan, 100047
e-mail: Farhod.Karimov@gmail.com; FKarimov@wiut.uz

M. Brengman
Department of Business (BUSI) – Marketing and Consumer Behavior Research Unit, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium
e-mail: Malaika.Brengman@vub.ac.be

1 Introduction

Modern high-tech crime no longer requires guns, masks and cars for escape. To commit an online robbery, it is sufficient to make several creative clicks over the Internet, while being thousands of miles away from the crime scene. The characteristics of online transactions such as anonymity, low transaction costs, and the difficulties in fraud detection, may intensify the problem of '*information asymmetry*' and stimulate cybercrime [93]. Today, hacker attacks, identity theft, credit card fraud, fishing for sensitive information and non-delivered merchandise are important issues of concern, growing in number as well as in geographical reach [8,14,20,21,83]. For both online shops and their customers the economic costs of cybercrime are becoming enormous [3,24,72]. The official online retailer fraud statistics are really frightening and growing at a fast pace. The *Federal Bureau of Investigation*'s (FBI) *Internet Crime Complaint Center* (IC3) received 3.4 % more complaint submissions in 2011 as compared to 2010, which accounts for a total financial loss of $485.3 million [35]. Credit card fraud, identity theft, auction fraud, non-delivered merchandise, and computer fraud were among the top five IC3 complaint categories during 2011 [35].

Such online fraud statistics concerning the risks of cybercrime may result in a lack of consumers' trust which in turn negatively affects their decisions to shop online [11,23,49]. Since fraud can be a major stumbling block for the growth of e-commerce transactions on the web, online retailers need to invest in trust building activities that oppose such fraudulent activities on the Internet. In order to secure their businesses as well as consumers' online transactions and privacy, many e-retailers follow secure coding practices by installing expensive Web applications or filtering devices against malicious attacks, such as cross site scripting (XSS), SQL injection flaws or session hijacking. However, as online consumers are unable to assess this, they will base their trust in a specific e-retailer mainly on 'cognitive' or 'institutional' '*cues*' regarding its trustworthiness [94,106]. In order to ease consumers' concerns about online security and privacy and to stimulate their trust, e-retailers are therefore taking part in several '*seal*' programs, such as *VeriSign*, *eTrust* and *BBBOnline* and also clearly disclose their privacy and security policies.

The influence of trust assurance structures on online trust has been extensively studied. Although a majority of studies confirm the effectiveness of trust assurance structures in e-commerce settings, some empirical evidence seems to contradict these findings. While some scholars find a positive influence of Web seals (i.e., *TRUSTe*) on consumers' trust (e.g., [43]), others do not support this claim (e.g., [18]). Empirical evidence on the adoption of e-assurances by e-retailers on the other hand remains scarce and findings regarding the determinants of e-assurance adoption appear inconsistent. For example, while Kim and Benbasat [42] found that e-retailers selling expensive products adopt more e-assurances, Muylle and Basu [74] found that e-retailers selling low-cost products are more inclined to utilize more seller authentications. One problem is that the few previous studies have analyzed the adoption of trust assurances in general, without referring to their specific types and not considering other firm-level variables.

In order to address these gaps, we will first provide a classification of e-assurance structures, distinguishing between internally and externally provided e-assurances.

Then, we will apply '*Cue Signaling Theories*', such as the '*Cue Utilization Theory*' [76] and the '*Cue Consistency Theory*' [64] to explain how e-assurance cues can provide a signal about the trustworthiness of the e-vendor. In order to develop some hypotheses regarding potential determinants of e-assurance adoption, we will explain the different impact of internally and externally provided e-assurances on consumer trust, looking more closely at potential moderating factors. Subsequently, we will try to identify a link between some characteristics of the online vendor (i.e., cost of merchandise sold, reputation, offline presence, etc…) and the specific types of trust assurances applied. As we assume that e-retailers' need for e-assurances differ depending on those characteristics, we expect that their adoption of specific trust assurances will differ accordingly. A discussion of our analyses and results will then be presented, followed by some conclusions. Finally, some limitations and suggestions for further research will be pointed out and some managerial implications of this study will be provided. This study will provide some important insights for the effective implementation of e-assurance mechanisms and will contribute to a better understanding of their diffusion among the variety of e-retailers. Moreover, our findings should allow start-up B2C e-commerce ventures to 'benchmark' the condition of their current web interface and learn from the best practices of top e-retailers.

2 Classification of e-assurance structures

In this section, we provide a classification of e-assurance structures and explain their importance in engendering e-shoppers' trust. Later, we will rely on this classification to generate our hypotheses and streamline our arguments. '*Structural e-assurances'* (e.g., encryption, legal protections and technology safeguards) assure safe online transactions and prevent consumers from losing their personal identity [66,69]. Bahmanziari et al. [5] classify them as '*internally provided'* and '*externally provided*' *e-assurance structures*.

2.1 Internally provided e-assurances

Internally provided e-assurances *(IPeAs)* are provided and managed by the online retailer but not verified by an independent source. These assurance structures may consist of company policies and disclosures such as a privacy policy, a security policy and a return policy, etc [5].

2.1.1 Privacy policy

A website's *privacy policy* is a legal promise made by an e-retailer that informs its end-consumers about how their private data is gathered and used [2]. While the presence of an online privacy policy will generate higher perceptions of consumer trust, a lack of privacy assurances can increase customer privacy concerns [53,76]. The stronger the privacy policy is, the higher the perceived trustworthiness (ability, benevolence, and integrity) towards the e-retailer [50]. Since privacy concerns have a significant negative impact on consumers' behavioural intentions [9,100], protecting individual privacy in e-commerce is important and beneficial to both consumers and e-businesses [97].

2.1.2 Security policy

A *security policy* is a legal document that is composed of the technical and personal measures an organization takes to protect and distribute its sensitive information. It ensures that private information is not compromised and that unauthorized persons will not gain access [30]. Security policies have a positive influence on consumers' satisfaction and trust in commercial websites [65]. In addition to security policies, e-retailers can also embed *security statements* that provoke a perception of security, which in turn influences consumer trust [45].

As a matter of fact, a privacy policy is inextricably connected to a security policy, because when security fails, privacy is lost [30]. Therefore, in practice, companies may not necessarily make a clear distinction between their privacy policy and their security policy. Amazon.com's "privacy notice", for example, includes aspects that can be classified as belonging to the security policy. However, other companies, such as HSN Inc., explicitly show a security policy separate from their privacy policy.

2.1.3 Return policy

A *return policy* is another type of IPeA that is particularly relevant for customer loyalty [37]. The ease of refunds/returns is a significant determinant of the willingness of customers to shop again from the same web-shop [81]. Thus, it is an important competitive weapon to boost sustained sales volume in the online marketplace [15]. Return policies may vary widely among e-retailers and can be in the form of a full return (e.g., 100 % money-back guarantee), a partial return (e.g., when restocking fees are charged), store credit only, or no refund [99]. Restrictions may include short time limits for returning the product, the fact that products should be unused or that they should be returned in their original packaging [73]. An easy *return policy* is a core trust element for e-commerce websites; it can be the main motivator for the online buying decision and consumers often choose one retailer over another based on the e-retailer's *return policy* [37,91]. The more liberal the e-retailer is with its *return policy*, the more the consumer will trust the quality of the retailer's products [96]. However, embracing more liberal warranty rebate policies may increase the costs of inventory management and the space required by the e-retailer [22,96]. For example, in 2007, the U.S. electronics industry spent about $13.8 billion to re-box, restock and resell returned products [52]. The primary reason for returning goods was because products didn't meet consumers' expectations or the devices were too confusing to use; in fact only about 5 % of returns were because a product was truly defective [52].

2.2 Externally provided e-assurances

Externally provided e-assurance structures *(EPeAs)* are based on the idea of "making the vulnerable party (the consumer) more comfortable with the transaction and ensuring that 'the other' (the e-retailer) follows through on its promises" [95]. They involve a certificate (e.g., privacy seal, security seal) and are provided by a third party organization only after an independent evaluation of the retailer's e-commerce related activities [5]. Many studies have reported that displaying '*externally provided'* e-assurances on their websites helps e-retailers to fuel consumer trust (e.g., [32,43,106]). Web seals are particularly relevant for online markets where consumers mainly transact with 'unfamiliar' e-retailers under the protection of third party organizations that provide an institutional context [75,79]. Hence, many e-retailers are paying annual fees to third party organizations in order to display *externally provided* trust promoting seals on their websites. Each of the *externally provided* trust-promoting structures specializes in a different function and may involve different cost structures. Table 1 provides more information concerning the diverse types of seal programs and we define each of these mechanisms below.

2.2.1 Privacy seals

Privacy programs such as *TRUSTe*, *eTrust* and *BBBOnline privacy* specify that an e-retailer's website meets stringent information privacy and data protection requirements set by these privacy service providers. If a website has a privacy seal, that website has agreed to disclose its information practices and has its privacy practices reviewed for compliance by the seal provider [31]. Specifically, having a privacy seal (e.g., *eTrust*) on a website signifies to consumers that any critical data collected, such as home addresses and phone numbers are not exchanged with third parties without their consent [88].

2.2.2 Security seals

There are diverse types of security assurance programs such as *VeriSign*, *CyberTrust, GeoTrust*, and *Entrust* that secure transactions over the Internet. These security seal programs are intended to assure consumers that the website they are interacting with is secured by Secure Socket Layer (SSL) encryption and that any sensitive information they share with that site will be encrypted during online transactions. SSL prevents the content it delivers from being cached [98]. This means that no exchange between the website and its visitors can be "overheard", accidentally or intentionally, by a third party, regardless of whether the visitor is placing an order or is just signing up for a newsletter [29]. SSL is trusted to secure transactions for sensitive applications ranging from web banking and stock trading, to e-commerce [102].

2.2.3 Rating and award seals

In addition to privacy and security assurance seals, thriving e-retailers also widely use different types of *rating and award seals* from other neutral sources such as *BizRate*, *ResellersRating*, *Top500* and many others (e.g., J&R Electronics). For example, member merchants can display the *ResellersRating* feature throughout their shopping portals providing reviews from actual customers. Merchants are allowed to post replies to respond to reviews, but not to post any reviews themselves. *ResellersRating* also

Table 1 Seal types, functions and prices

Security seal function	Security seals											
	Comodo	CyberTrust	Digicert	Entrust	GeoTrust	GoDaddy	McAfee	RSASecurity	SecurityMetrics	Thawte	TrustWave	Verisign
Price range *(in USD per 1-year)*	179–809	349–845	144	132–699	149–499	49–64	2,017	637	699–1399	149–699	111–300	399–1,499
Encryption strength: up to 256-bit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2048-bit root	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Trustmark	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Warranty	250	–	1,000 K	1,000 K	500 K	179 K	–	–	–	100 K	100 K	1,000 K
99.9 % browser recognition	✓	–	–	–	✓	✓	–	–	–	✓	✓	–
Daily scanning	–	–	–	–	–	–			–	–	–	–
Green address bar	✓	–	–	–	–	✓	–	–	–	✓	–	✓
Privacy seals												
Price range (in USD per 1-year)	BBBOnline 349–1499				eTRUST 450–495				TRUSTe 499–995			
Privacy seal function	BBBOnline offers 2 seal programs with regard to *privacy* and *reliability*. The *Privacy Program* specifically addresses company's privacy practices and how a website uses personaly identifiable information it collects from website visitors. The *Reliability Program* signifies that the company is a member of their local BBB, that their advertising is truthful and that they practice other high business standards and are committed to dispute a resolution				An eTrust Privacy Certification indicates that a website has been reviewed by eTrust and has met their stringent privacy and data protection requirements. Having an eTrust Privacy logo on a website signifies to customers that any critical data collected, such as home addresses and phone numbers are not exchanged with third parties without their consent				TRUSTe has two main privacy seals. The TRUSTe Verified Web Privacy Seal is for e-commerce sites that are reviewed and approved as compliant with TRUSTe web privacy standards. The TRUSTe Certified Web Privacy Seal is for any website that is similarly reviewed and approved			

Source Authors' own compilation based on the data provided on seal providers' websites
Price range = minimum and maximum price of Web seals for 1 year (data were obtained: August 2011)

enables online merchants to flag reviews for verification, in order to be able to detect and to prevent fake reviews from someone who didn't place an order. In general, rating features provide consumers the opportunity to write real reviews, incorporating their impressions and to rate their store experiences. In addition, they enable consumers to search for virtually any product by linking them with over a million brands and stores [12]. Award seals (such as *SSPA Excellence* or *Fortune 500 Company*) can also be provided by reputable neutral sources that are also designed to promote online trust [104]. In brief, rating seals can work as e-assurance mechanisms as they enable consumers to assess the quality of different online stores.

3 'Signaling' trustworthiness by means of e-assurance cues

In an online context, the perceived risk involving transactions is usually high. In order to reduce consumers' concerns about online security and privacy, e-retailers are taking part in several e-assurance programs to provide *'cues'* to *'signal'* their *'trustworthiness'*. *'Cue Signaling Theories'* such as the *'Cue Utilization Theory'* [76] and *'Cue Consistency Theory'* [64] may provide useful frameworks through which we can understand the adoption patterns of e-assurance *'cues'* across different e-retailers. Previous research has used such *'Cue Signaling Theories'* to examine consumers' perceptions of trustworthiness of online vendors based on the trust seals provided in their websites (e.g., [32]). We use these theories as a foundation to understand why thriving e-retailers differ in their adoption of such trust signaling cues.

According to the '*Cue Utilization Theory'*, a product sends out a series of cues signaling its quality to consumers [76]. These cues can be classified either as 'intrinsic' or 'extrinsic' to the product. *'Intrinsic cues'* refer to those inseparable physical attributes of the product (e.g., ingredients) that cannot be altered without changing the product, whereas *'extrinsic cues'* refer to product-related attributes which are not part of the physical product (such as price, brand name and packaging). Websites also consist of a multitude of individual cues that assist online shoppers to form an impression of the online merchant. In the absence of sales assistants, other shoppers, and the products themselves, online shoppers often rely on the only source of cues available to them to make decisions (i.e., the website interface) [13]. The internet is low in intrinsic cues and it is impossible for consumers to evaluate all product and service attributes with their senses, thus, they usually rely on extrinsic cues to assess the trustworthiness of the online vendor [32]. Extrinsic cues on the Web may consist of brand reputation, product prices, ratings, and *'various e-assurance structures'*.

The*'Cue Consistency Theory'* proposes furthermore that multiple sources of information that corroborate one another are more useful than if they provide incongruent messages [64]. That is, multiple and consistent extrinsic cues may have a stronger impact on perceived quality than single cues [16,71]. An online vendor can address the various risk concerns of online consumers by adopting multiple e-assurance mechanisms such as different trust promoting seals. When multiple consistent e-assurance cues are presented to a consumer, each cue tends to receive more attention and weight in the consumer's evaluation [32]. Thus we expect that online vendors will use multiple e-assurance cues in order to signal their trustworthiness and to ease consumers' risk concerns.

Table 2 Empirical e-assurance research: the effect of IPeAs on consumers' initial trust

Type of IPeA	Trust effect	Product category		Study
		Cheap	Expensive	
Privacy policy disclosures	+	Gift items		Pan and Zinkhan [77]
	n.s.	Flowers, food, college souvenirs		Wang et al. [104]
	+	Text book		Liu et al. [61]
	+		Computer	Aljukhadar et al. [1]
Privacy and security statement	+		Contemporary furniture	Schlosser et al. [89]
Security policy disclosures	+	Flowers, food, college souvenirs		Wang et al. [104]
Return policy disclosure	n.s.	Flowers, food, college souvenirs		Wang et al. [104]
Guarantees, free shipping, return policies	+		Jewelry	Bahmanziari et al. [5]
Money back guarantees	+		DVD player	Pennington et al. [80]
Claim plus data and backing arguments	+		Watch	Kim and Benbasat [41]

Source Authors' own compilation of research
Positive sign (+) positive effect has been found; n.s. no significant effect has been found

3.1 The impact of IPeAs on consumer trust

The majority of empirical research confirms the positive influence of *'internally provided e-assurances' (IPeAs)* on consumer trust. Table 2 provides an overview of some of the published empirical e-trust studies concerning IPeAs. Only Wang et al. [104] do not find any positive effect of detailed privacy disclosures and higher levels of leniency in return-policy on consumers' institutional cue-based trust in e-retailers. However, they do confirm that privacy disclosures directly enhance consumers' willingness to provide personal information. According to the majority of the experiment-based empirical studies presented in Table 2, different IPeAs such as privacy policy disclosures, security policy disclosures, assurance statements, and return policies (i.e., money-back guarantees) all enhance consumers' trust in an e-vendor, which, in turn, positively influences their behavioral responses such as purchase intentions, bookmarking intentions and willingness to provide personal information.

3.2 The impact of EPeAs on consumer trust

On the other hand, with regard to the value of *'externally provided e-assurances' (EPeAs)* to signal trustworthiness, the findings seem inconclusive as some of the empirical studies have reached contradictory results. Table 3 presents some of the published empirical e-assurance research concerning the impact of EPeAs on initial trust. While some scholars find a positive influence of EPeAs on consumer trust (e.g., [106]), others do not report any effect (e.g., [18]). Despite these contradictions, however, there seems to be a common agreement that the effect of EPeAs on consumer trust may differ depending on several factors, such as the type of assurance program, the product category and the degree of consumer involvement (eg., [31,43,58,105,110]).

Indeed, the contradictory findings regarding the effectiveness of EPeAs could be due to the diverse manipulations of Web assurance programs, along with the fact that different product categories are involved, differing amongst others in monetary value (cheap vs. expensive products). For example, while Fisher and Chu [18] find no effect of *TRUSTe privacy* seals on purchasing a cheap product (i.e., a textbook), Nöteberg et al. [75] provide support that *TRUSTe privacy* seals positively influence consumer trust and subsequent purchase decisions for a more expensive product category (i.e., a Web camera). Thus, we presume that the root for these discrepancies is based on the dissimilar product categories and Web seals manipulated in the experiment-based studies.

4 Research objectives and hypotheses

In the virtual environment, engendering consumer trust is important because it leads to outcomes vital to the success of an Internet store, such as reduced risk perceptions and increased willingness to buy from the store [4,19,45]. However, choosing the appropriate e-assurance mechanisms could be a challenging task for an e-retailer, due to the diversity of e-assurance programs available in the marketplace and the various cost structures associated with them [32]. Therefore, the goal of this paper is to depict the adoption of diverse e-assurance mechanisms among thriving e-retailers, in order to provide a snapshot of best practices, as well as to identify some determinants of e-assurance adoption.

There are several factors that may explain the adoption of e-assurances by B2C websites. As we assume that e-retailers' needs for e-assurances differ according to several factors (such as the type of products they sell, their reputation, etc.) due to consumers' varying risk perceptions, we also expect that their adoption of e-assurances will differ accordingly. Underneath we present our hypotheses regarding some determinants of e-assurance adoption (IPeAs and EPeAs). More particularly, we will elaborate on the anticipated impact of the e-tailer's reputation, whether the retailer has an offline presence or not, and of the monetary value of products traded by the online vendor.

4.1 e-Assurance adoption according to the e-tailer's reputation

Prior research confirms that the *'reputation'* of an online vendor is a vital factor that signals its trustworthiness [17,55,56]. The *'reputation'* of a firm may refer to a firm's success, its time in business, its size, its brand equity, etc. It is regarded as a valuable asset that requires a significant and long term monetary and time investment from the firm [38]. Reputation is considered to signal expertise, positive character (i.e. integrity, care for customers), credibility, and reliability of a firm [17]. Reputation is also universally interpreted as a strong 'signal' of security control and quality because

Table 3 Empirical e-assurance research: the effect of EPeAs on consumer initial trust

Type of EPeA seal	Trust effect	Product category		Study
		Cheap	Expensive	
Privacy seals				
TRUSTe privacy	n.s.	Textbook		Fisher and Chu [18]
	n.s.	Book		Nöteberg et al. [75]
	+	Compact discs		Rifon et al. [84]
	+	Running shorts		Kim and Kim [43]
	+	Clothing		Kaplan and Nieschwietz [39]
	n.s.	Retail website		Kimery and McCord [46]
	+		Video camera, travel tour, securities	Nöteberg et al. [75]
	n.s.		Legal advice	McKnight et al. [69]
	+		Camera equipment	Wakefield et al. [103]
BBBOnline privacy	+	Compact discs		Rifon et al. [84]
	+		Camera equipment	Wakefield et al. [103]
CyberTrust privacy	+	Books, PC, apparel, perfume		Hu et al. [32]
	+	Books, laptops, perfume, clothing		Wu et al. [106]
Security seals				
VeriSign security	n.s.	Retail website		Kimery and McCord [46]
	+		Used laptop	Lee and Lee [54]
HiTrust security	+		Web camera	Yang et al. [107]
CyberTrust security	+	Books, PC, apparel, perfume		Hu et al. [32]
	+	Books, laptops, perfume, clothing		Wu et al. [106]
Rating seals				
Awards from neutral sources	+	Flowers, food, college souvenirs		Wang et al. [104]

Table 3 continued

Type of EPeA seal	Trust effect	Product category		Study
		Cheap	Expensive	
BizRatings	n.s.		DVD player	Pennington et al. [80]
Other seals				
BBBOnline reliability	n.s.	Retail website		Kimery and McCord [46]
WebTrust consumer protection	n.s.		Jewelry	Bahmanziari et al. [5]

Source Authors' own compilation of research
Positive sign (+) positive effect has been found, *n.s.* no effect has been found

it captures information about the past performance of retailers (such as that they have not routinely engaged in deceptive behavior such as security breaches and abuses) [82].

Hence, we expect that a firm's adoption of externally provided e-assurances will be inversely related with its reputation. That is, highly reputable companies may have less need for third-party endorsements because they may feel that their reputation can be a sufficient warrant for their 'trustworthiness'. Accordingly, Sivasailam et al. [95] already demonstrated that firms with relatively lower reputation rankings are more prone to invest in security seals as compared to those with higher reputation rankings. In contrast, they may rely more on internally provided trust assurances (such as privacy, security and return policies). Therefore, based on this discussion, we hypothesize:

H1 e-retailers with a relatively stronger reputation are more likely to adopt IPeAs: (a) privacy policy, (b) security policy, (c) return policy as compared to those with a weaker reputation.

H2 e-retailers with a relatively weaker reputation are more likely to adopt EPeAs (third-party endorsements: (a) privacy seals, (b) security seals, (c) rating seals, (d) award seals) as compared to those with a stronger reputation.

4.2 e-Assurance adoption according to the e-tailer's offline presence

Brick and click retailers that have a commonly recognized brand are proving to be more successful in the electronic marketplace as compared to their pure online counterparts [28,44]. Prior research has found a positive relationship between consumers' trust in the offline store and their confidence in the retailer's online store (e.g., [26]). An offline presence appears to influence perceptions of competence, integrity and benevolence regarding an Internet vendor significantly [10,48]. E-commerce sites without physical presence will have to 'signal' their trustworthiness by applying externally provided e-assurances [108]. Thus, based on the cue signaling theory, we may presume that e-retailers without physical presence will be more inclined to signal their trustworthiness by participating in different third-party trust assurance programs. E-tailers with offline presence are expected to rely more on internally provided trust assurances (such as privacy, security and return policies). Therefore, we hypothesize:

H3 e-retailers with an offline presence (i.e., Brick and Clicks) are more likely to adopt IPeAs: (a) privacy policy, (b) security policy, (c) return policy as compared to those without offline presence.

H4 e-retailers without offline presence (i.e. Pure Players) are more likely to adopt EPeAs (third-party endorsements: (a) privacy seals, (b) security seals, (c) rating seals, (d) award seals) as compared to those with offline presence.

4.3 e-Assurance adoption according to the monetary value of products traded

'*Monetary value*' is probably the most commonly used indicator of perceived financial risk because consumers risk more when the price is high [51]. Purchasing expensive products on the internet is considered as more risky than purchasing cheap products [7]. Lowengart and Tractinsky [63] empirically confirm that consumers perceive more financial risk in purchasing computers compared to the purchase of books. The likelihood of purchasing relatively inexpensive products (e.g., books) over the internet is for this reason significantly higher than the chance of buying more expensive products [33]. Most online shoppers indicate that they will not buy expensive items through the Internet [59]. Only those consumers who perceive the Web interface as a secure environment are likely to purchase expensive products online [58]. Trust related e-assurance mechanisms would accordingly matter more to consumers when considering purchasing relatively expensive products than when shopping for cheaper products, because there is more at stake in the online transaction [42]. Consumer involvement (cf. Rossiter and Percy [87]) will be higher, and more consideration will be paid. Therefore, in risky online environments consumers are expected to look more for e-assurances such as IPeAs and EPeAs that 'signal' the potential e-retailer's trustworthiness and to seek for better protection when considering purchasing more expensive product categories [68]. Kim and Benbasat [42] demonstrated that e-retailers vending expensive products are more likely to provide e-assurances compared to those selling inexpensive goods. Therefore, we can expect that e-retailers vending relatively more expensive products will be more prone to 'signal' their trustworthiness by means of multiple cues (i.e., IPeAs as well as EPeAs).

4.3.1 Effectiveness of internally provided e-assurances and the monetary value of products

Internally provided e-assurances (IPeAs) offered by a website, such as return policies, guarantees and free shipping, have been demonstrated to have a significant effect on consumer trust in purchasing products that are relatively higher in monetary value, such as jewelry [5]. Aljukhadar et al. [1] and Schlosser et al. [89] also find a positive effect of IPeAs (i.e., privacy and security disclosure) when purchasing a computer and contemporary furniture, both product categories of relatively higher monetary value. In contrast, Wang et al. [104] do not find any effect of return policy disclosures on consumer trust in purchasing flowers, food and college souvenirs, which are relatively cheaper and less risky products. On the basis of the cue signaling theory, we presume that e-retailers vending expensive products would be more prone to adopt IPeAs in order to signal their trustworthiness and to reduce perceived risk and uncertainty. Therefore we put forward the following hypothesis:

H5 e-retailers selling products of relatively higher monetary value are expected to utilize more internally provided e-assurance structures (a: privacy policy; b: security policy; c: return policy) than those selling relatively inexpensive goods.

4.3.2 Effectiveness of externally provided e-assurances and the monetary value of products

With regard to EPeAs, Nöteberg et al. [75] examined the effect of *TRUSTe* privacy assurance seals on purchase likelihood taking into account the *monetary value (low vs. high)* of the product categories sold. Their findings show that the value of third-party assurance seals becomes paramount in purchasing more expensive or high risk products (i.e., video camera; international travel tour; securities). They do not find any effect of EPeAs for products low in monetary value (i.e., books). This might be because consumers' online risk perceptions are elevated when purchasing more expensive product categories as compared to inexpensive goods. Yang et al. [107] also provide support that EPeAs (i.e., HiTrust Seal) positively influence consumer trust and subsequent purchase decisions in purchasing product categories that are more expensive and relatively risky (i.e., a Web camera).

Thus, based on the cue signaling theory, we assume that e-retailers vending relatively expensive products will be more inclined to utilize multiple EPeAs that consistently 'signal' their trustworthiness in order to reduce consumers' perceptions of uncertainty. Therefore, based on the premise that more risk is involved during the purchase of products of a higher monetary value, we put forward the following hypothesis:

H6 e-retailers selling products of relatively higher monetary value are expected to utilize more externally provided e-assurance structures (a: privacy seals; b: security seals; c: rating seals; d: award seals) than those selling relatively inexpensive goods.

5 Methodology

5.1 Content analysis: method and procedure

In order to establish to what extent structural assurances are adopted by B2C e-retailers, we content analyzed their websites, identifying the different internal and external e-assurance structures utilized. Content analysis is a scientific, objective, systematic, quantitative and generalizable research technique, used to make replicable and valid inferences from textual, pictorial, or audible matter to the contexts of their use [47]. This method has been used by many scholars to investigate website content across different domains (e.g., [40,67,109]). The analysis of the website content to obtain information on the adoption of IPeAs and EPeAs was carried out by one of the authors during June-July 2010 and proceeded in 2 stages: (1) careful investigation of the website's front page, (2) choosing a product and clicking until the last checkout page, carefully examining the website interface during the entire shopping process for the presence or absence of the different Web assurance seals, using a pragmatic coding scheme (see Appendix: Table 11). Since the absence or presence of Web assurance seals is easy to detect and to code (absence = 0; presence = 1), no additional coders are deemed required to assure reliability (cf. [27]).

In order to indirectly assess and compare the total *'investments'* made by different e-vendors to integrate externally provided e-assurances in their websites, we multiply the presence of e-assurance seals with their 'average' costs. In this regard, we have to note that different types of externally provided trust promoting seals have different cost structures. In most cases, the cost of a seal to a company depends on the size of the company seeking certification: the larger the company, typically the more complex the evaluation and the higher the cost [95]. *BBBOnline*, for example, charges companies based on the number of employees and its pricing may vary from $349 (for a company with 1–5 employees) to $1499 (for a company with over 200 employees) [6]. Conversely, pricing for *VeriSign* may vary according to the number of Secure Socket Layer IDs a company requires and each ID starts at around $399 [101].

5.2 Sample

The sample consisted of 210 top revenue generating B2C e-commerce retailers, as identified by the *Internet Retailer's 'Top 500 Guide'*. This *'Top 500'* ranks B2C e-retailers in the U.S. and Canada based on their full-year online sales [36]. We expect that these top companies can be considered as the most apt to have adequate resources and competences to afford different types of third-party assurance certificates. A similar approach for identifying relevant websites has been followed by other scholars (e.g., [42,60]).

As online sales significantly differ according to the product category involved [62], we included various industries in our sample. According to the classification provided by the Internet Retailer's *'Top 500 Guide'*, we first selected 12 B2C product industries. Subsequently, we identified the top 20 e-tailers within each industry. Note that some industries contained less than 20 e-vendors in the *'Top 500'*, which resulted in some smaller subsamples for some industries. We followed Karimov and Brengman [40] in classifying the commercial websites into 2 categories according to the *'monetary value'* of products sold (i.e., *cheaper* versus relatively *more expensive*). A similar classification of e-retailers according to the monetary value of products vended has also been proposed by other scholars (e.g., [42,74]). A complete list of the sectors, together with their classification, can be found in Table 4.

The sample acquired by means of this procedure contained 57.6 % e-stores with '*offline presence'* (i.e., *'brick and click'* retailers) and 42.4 % *'pure players'* (without offline existence), which were evenly distributed over the main categories as far as the monetary value of products traded is concerned ($\chi^2 = .327$, $p = .568$; see Table 5).

Furthermore, as we also want to control for *'reputation'* in our analyses, we consider the e-retailer's 'ranking' in the *'Top 500 Guide'* as a proxy for the e-vendor's *'reputation'* (see Appendix: Table 12). *Internet Retailer's* rankings are based on full-

Table 4 Sample distribution over various industries, according to the monetary value of products traded

Monetary value: relatively low		Monetary value: relatively high	
Industry type	Sample size	Industry type	Sample size
Apparel/accessories	20	Jewelry	15
Health/beauty	20	Housewares/home furnishings	20
Sporting goods	20	Automotive parts/accessories	7
Flowers/gifts	11	Computers/electronics	20
Books/music/videos	20	Hardware/home improvement	20
Food/drug	20	Office supplies	17
Total	N = 111	Total	N = 99

Table 5 Sample distribution over pure-players and brick and click retailers, according to the monetary value of products traded

Offline presence	Monetary value		Total	Chi-square (*p* value)
	Low n (%)	High n (%)		
Pure plays	45 (40.5 %)	44 (44.4 %)	89 (42.4 %)	
Brick and clicks	66 (59.5 %)	55 (55.6 %)	121 (57.6 %)	
Total	111 (100 %)	99 (100 %)	210 (100 %)	.327 *(.568)*

year online sales, including past years' sales, growth rate, monthly visits, conversion rates, website performance, search marketing and e-mail marketing data, and more [36]. We performed a median split between the 210 retailers in our sample based on Internet Retailer's rankings and coded relatively higher ranked retailers as "1" (105 sites) and lower ranked retailers as "0" (105 sites). A similar classification has also been used by other scholars (e.g., [44,95]).

6 Analyses and results

The quantified data, gathered by means of content analysis, was entered into SPSS and descriptive statistics were carried out in order to disclose the extent to which structural assurances are adopted by top B2C e-retailers. Furthermore, cross-tabulations with chi-square analyses and independent samples t-tests were performed to examine how the adoption of e-assurances varies among e-retailer categories.

6.1 The adoption of IPeAs among different e-retailer categories

The results indicate that 98.1 % of the top e-retailers examined in this study feature a *'privacy policy'*, 40 % display a *'Security Policy'* and 73.3 % offer a *'Return Policy'*. The adoption of IPeAs appears to vary markedly between the websites investigated: while 2 (1 %) of the websites investigated contain no IPeAs, 45 out of the 210 websites (21.4 %) provide only one IPeA, which in most cases appears to be a Privacy Policy, 90 of them (42.9 %) comprise 2 EPeAs and only 73 (34.8 %) of the sites provide Privacy, Return as well as Security Policies.

Table 6 Adoption of IPeAs among e-retailer categories

IPeA	Reputation		Totaln (%)	χ^2	df	Sig. (2-sided)
	Weak n (%)	Strong n (%)				
PRIVACY	101 (96.2)	105 (100.0)	206 (98.1)	4.078	1	(.043)
SECURITY	37 (35.2)	47 (44.8)	84 (40.0)	1.984	1	(.159)
RETURN	73 (69.5)	81 (77.1)	154 (73.3)	1.558	1	(.212)
ANY_IPeA	103 (98.1)	105 (100.0)	208 (99.0)	2.019	1	(.155)
IPeA	Offline presence		Total n (%)	χ^2	df	Sig. (2-sided)
	Pure-plays n (%)	Brick and clicks n (%)				
PRIVACY	87 (97.8)	119 (98.3)	206 (98.1)	.097	1	(.756)
SECURITY	41 (46.1)	43 (35.5)	84 (40.0)	2.369	1	(.124)
RETURN	68 (76.4)	86 (71.1)	154 (73.3)	.745	1	(.388)
ANY_IPeA	87 (97.8)	121 (100.0)	208 (99.0)	2.745	1	(.098)
IPeA	Monetary value		Total n (%)	χ^2	df	Sig. (2-sided)
	Low n (%)	High n (%)				
PRIVACY	111 (100.0)	95 (96.0)	206 (98.1)	4.572	1	(.032)
SECURITY	37 (33.3)	47 (47.5)	84 (40.0)	4.360	1	(.037)
RETURN	65 (58.6)	89 (89.9)	154 (73.3)	26.283	1	(.000)
ANY_IPeA	111 (100.0)	97 (98.0)	208 (99.0)	2.264	1	(.132)

Contingency table computed for a 2 × 2 design
Pearson Chi-square (2 tailed)

The results of cross-tabulations, presented in Table 6, provide an overview of how the adoption of internally provided e-assurances varies among e-retailer categories. Some additional independent samples t-tests also illustrate how the average number of IPeAs adopted among e-tailers ($M = 2.114$, $SD = 0.768$) varies across retailer categories, as will be discussed in more detail further on.

Reputation

- Our results reveal that top e-tailers with a relatively stronger reputation make more use of IPeAs as compared to online vendors with a relatively weaker reputation (average number of IPeAs = $2.22_{StrongReputation}$ vs. $2.01_{WeakReputation}$; independent samples t-test, $p = .048$), *providing some general support for H1.*
- More specifically, retailers with a stronger reputation appear to feature *'Privacy Policies'* more often ($100\,\%_{StrongReputation}$ versus $96.2\,\%_{WeakReputation}$, χ^2 test p $= .043$), *in support of H1a.*
- While they also seem to display *'Security Policies'* ($44.8\,\%_{StrongReputation}$ versus $35.2\,\%_{WeakReputation}$, χ^2 test $p = .159$) and *'Return Policies'* ($77.1\%_{StrongReputation}$ versus $69.5\,\%_{WeakReputation}$, χ^2 test $p = .212$) more often, these differences appear to be insignificant. *Therefore H1b and H1c cannot be accepted.*

Offline presence

- Whether the e-tailer has an *'offline presence'* or not does not appear to affect the number of IPeAs displayed in the website (independent samples t-test, $p = .155$).
- While 'pure players' seem to display *'Security Policies'* somewhat more often ($46.1\,\%_{PurePlay}$ vs. $35.5\,\%_{BrickandClick}$), this difference appears to be insignificant (χ^2 test $p = .124$). *Thus no support could be found for H3.*

Monetary value of products traded

- As expected, e-tailers selling products of a higher *'monetary value'* feature more IPeAs on their website as compared to those selling relatively less expensive products (average number of IPeAs $= 2.33_{ExpensiveMerchandise}$ vs. $1.92_{CheaperMerchandise}$; independent samples t-test, $p < .001$), *providing some general support for H5.*
- In line with expectations, retailers selling more expensive products appear to display *'Security Policies'* more often ($47.5\,\%_{ExpensiveMerchandise}$ versus $33.3\,\%_{CheaperMerchandise}$, χ^2 test $p = .037$). However, controlling for *'reputation'* reveals that this is only the case for e-tailers with a stronger reputation and not for those with a weaker reputation. Controlling for *'offline presence'* discloses furthermore that this difference can only be discerned for 'brick and click' retailers and not for 'pure players'. See Table 7 for detailed results of these encompassing analyses. *This provides only some partial support for H5b.*
- As assumed, retailers selling more expensive products also appear to display *'Return Policies'* more often ($89.9\,\%_{ExpensiveMerchandise}$ versus $58.6\,\%_{CheaperMerchandise}$, χ^2 test $p < .001$), regardless of their reputation or whether they have offline presence or not, *supporting H5c.*
- In contrast to our expectations, retailers selling relatively cheaper merchandise appear to display *'Privacy Policies'* more often ($100\,\%_{CheaperMerchandise}$ versus $96.0\,\%_{ExpensiveMerchandise}$, χ^2 test $p = .032$). *Thus H5a has to be rejected.*

6.2 The adoption of EPeAs among different e-retailer categories

An overview of our findings regarding the overall adoption of different EPeAs is presented in Fig. 1. Accordingly, '*Security assurance Seals'* provided by McAfee (39.5 %) and VeriSign (34.3 %), as well as the *'Privacy assurance Seal'* provided by BBB*Online* (31 %) are the most common assurance mechanisms adopted by the top online retailers. The results indicate that 72.9 % of the top e-tailers in this study feature externally provided e-assurances: 65.7 % expose *'Security Seals'*, 33.8 % display *'Privacy Seals'*, 21.0 % exhibit *'Award Seals'* and 20.5 % present *'Rating Seals'*. The adoption of EPeAs appears to vary markedly along the websites investigated: while 57 out of 210 websites (27.1 %) did not display any EPeA, 23.8 % incorporated one, 20 % contained two, 14.8 % featured three and 14.3 % even included four or more different kinds of externally provided trust assurances and can be considered exemplary in this regard (e.g., 'Limoges Jewelry', 'HP Home and Home Office Store', 'National Business Furniture', etc.).

The results of cross-tabulations, presented in Table 8, provide an overview of how the adoption of externally provided e-assurances varies among e-retailer categories.

Table 7 Adoption of IPeAs among e-retailer categories—encompassing analyses

Offline presence	Reputation	IPeA type	Monetary value		Chi-square (p value)	Total n (%)
			Low n (%)	High n (%)		
Pure plays (n = 89)	Weak reputation (n = 50)	PRIVACY	22 (100.0)	26 (92.9)	1.637 (.201)	48 (96.0)
		SECURITY	10 (45.5)	10 (35.7)	.487 (.485)	20 (40.0)
		RETURN	13 (59.1)	25 (89.3)	6.158 (.013)	38 (76.0)
		ANY_IPeA	22 (100.0)	26 (92.9)	1.637 (.201)	48 (96.0)
			n = 22	n = 28		
	Strong reputation (n = 39)	PRIVACY	23 (100.0)	16 (100.0)	n.s.[a]	39 (100.0)
		SECURITY	9 (39.1)	12 (75.0)	4.885 (.027)	21 (53.8)
		RETURN	15 (65.2)	15 (93.8)	4.327 (.038)	30 (76.9)
		ANY_IPeA	23 (100.0)	16 (100.0)	n.s.[a]	39 (100.0)
			n = 23	n = 16		
	Total	PRIVACY	45 (100.0)	42 (95.5)	2.092 (.148)	87 (97.8)
		SECURITY	19 (42.2)	22 (50.0)	.542 (.462)	41 (46.1)
		RETURN	28 (62.2)	40 (90.9)	10.155 (.001)	68 (76.4)
		ANY_IPeA	45 (100.0)	42 (95.5)	2.092 (.148)	87 (97.8)
Brick and clicks (n = 121)	Weak reputation (n = 55)	PRIVACY	28 (100.0)	25 (92.6)	2.152 (.142)	53 (96.4)
		SECURITY	6 (21.4)	11 (40.7)	2.401 (.121)	17 (30.9)
		RETURN	14 (50.0)	21 (77.8)	4.583 (.032)	35 (63.6)
		ANY_IPeA	28 (100.0)	27 (100.0)	n.s.[a]	55 (100.0)
			n = 28	n = 28		

Table 7 continued

Offline presence	Reputation	IPeA type	Monetary value		Chi-square (p value)	Total n (%)
			Low n (%)	High n (%)		
	Strong reputation (n = 66)	PRIVACY	38 (100.0)	28 (100.0)	n.s.[a]	66 (100.0)
		SECURITY	12 (31.6)	14 (50.0)	2.291 (.130)	26 (39.4)
		RETURN	23 (60.5)	28 (100.0)	14.303 (.000)	51 (77.3)
		ANY_IPeA	38 (100.0)	28 (100.0)	n.s.[a]	66 (100.0)
			n = 38	n = 28		
	Total	PRIVACY	66 (100.0)	53 (96.4)	2.440 (.118)	119 (98.3)
		SECURITY	18 (27.3)	25 (45.5)	4.329 (.037)	43 (35.5)
		RETURN	37 (56.1)	49 (89.1)	15.920 (.000)	86 (71.1)
		ANY_IPeA	66 (100.0)	55 (100.0)	n.s.[a]	121 (100.0)
Total (n = 210)	Weak reputation (n = 105)	PRIVACY	50 (100.0)	51 (92.7)	3.780 (.052)	101 (96.2)
		SECURITY	16 (32.0)	21 (38.2)	.439 (.508)	37 (35.2)
		RETURN	27 (54.0)	46 (83.6)	10.857 (.001)	73 (69.5)
		ANY_IPeA	50 (100.0)	53 (96.4)	1.853 (.173)	103 (98.1)
			n = 50	n = 55		
	Strong reputation (n = 105)	PRIVACY	61 (100.0)	44 (100.0)	n.s.[a]	105 (100.0)
		SECURITY	21 (34.4)	26 (59.1)	6.289 (.012)	47 (44.8)
		RETURN	38 (62.3)	43 (97.7)	18.200 (.000)	81 (77.1)
		ANY_IPeA	61 (100.0)	44 (100.0)	n.s.[a]	105 (100.0)
			n = 61	n = 44		

Table 7 continued

Offline presence	Reputation	IPeA type	Monetary value		Chi-square (p value)	Total n (%)
			Low n (%)	High n (%)		
	Total	PRIVACY	111 (100.0)	95 (96.0)	4.572 (.032)[b]	206 (98.1)
		SECURITY	37 (33.3)	47 (47.5)	4.360 (.037)	84 (40.0)
		RETURN	65 (58.6)	89 (89.9)	26.283 (.000)	154 (73.3)
		ANY_IPeA	111 (100.0)	99 (100.0)	2.264 (.132)	208 (99.0)
			n = 111	n = 99		

Contingency table computed for a 2 × 2 × 2 design

Pearson Chi-square (2 tailed)

[a] No statistics has been computed because this variable is a constant

[b] 2 cells (50.0 %) have expected count less than 5

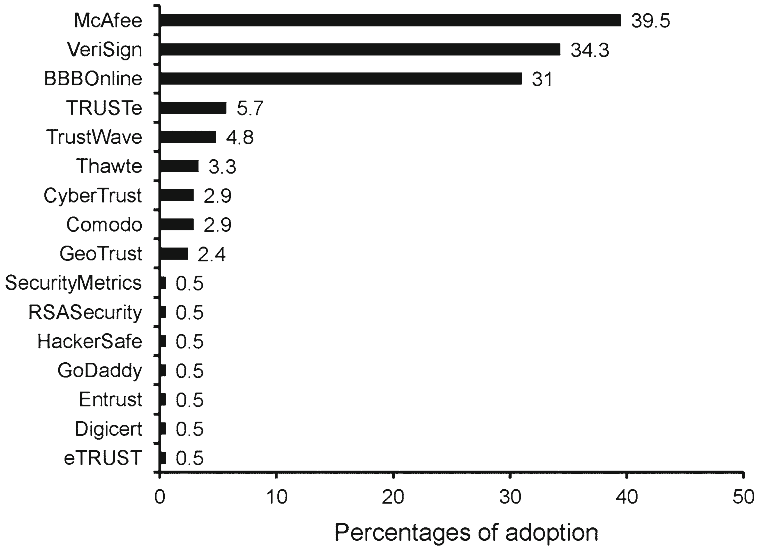

Fig. 1 Overall adoption of EPeAs

Some additional independent samples t-tests (exhibited in Table 9) also illustrate how the average number of EPeAs adopted among e-tailers ($M = 1.724$, $SD = 1.531$) and the amount of money invested in seals vary across retailer categories, as will be discussed in more detail next.

Reputation

- Our results reveal that top e-tailers with a relatively stronger reputation make less use of EPeAs as compared to online vendors with a relatively weaker reputation (average number of EPeAs $= 1.40_{StrongReputation}$ vs. $2.05_{WeakReputation}$; independent samples t-test, $p = .002$). While 82.9 % of the relatively lower ranked e-tailers display at least one EPeA, only 62.9 % of higher ranked e-commerce sites do apply EPeAs (χ^2 test $p = .001$). Moreover, the websites that do not display any seals appear to belong to famous reputable companies such as ‘Dell Inc.’, ‘Apple Inc.’, ‘SonyStyle’, etc. *This provides some general support for H2.*
- This is the case for the adoption of *‘Privacy Seals’*, which also appear to be adopted less by retailers with a stronger reputation ($27.6\,\%_{StrongReputation}$ vs. $40.0\,\%_{WeakReputation}$, χ^2 test $p = .058$; average number of PSs $= 0.29_{StrongReputation}$ versus $0.46_{WeakReputation}$; independent samples t-test, $p = .023$)*, in support of H2a.*
- Also less *‘Security Seals’* appear to be displayed in websites of e-vendors with a stronger reputation (average number of SSs $= 0.79_{StrongReputation}$ vs. $1.07_{WeakReputation}$; independent samples t-test, $p = .011$). ‘Security seals’ are featured in 76.2 % of the lower ranked websites as compared to in only 55.2 % of those with a stronger reputation (χ^2 test $p = .001$)*, supporting H2b.*
- While no significant difference according to the reputation of the e-tailer can be revealed for the adoption of *‘Rating Seals’ (no support for H2c)*, a marginally sig-

Table 8 Adoption of EPeAs among e-retailer categories

EPeA	Reputation		Total n (%)	χ^2	df	Sig. (2-sided)
	Weak n (%)	Strong n (%)				
PRIVACY	42 (40.0)	29 (27.6)	71 (33.8)	3.596	1	(.058)
SECURITY	80 (76.2)	58 (55.2)	138 (65.7)	10.229	1	(.001)
RATING	26.24.8)	17 (16.2)	43 (20.5)	2.369	1	(.124)
AWARD	28 (26.7)	16 (15.2)	44 (21.0)	4.140	1	(.042)
ANY_EPeA	87 (82.9)	66 (62.9)	153 (72.9)	10.619	1	(.001)
EPeA	Offline presence		Total n (%)	χ^2	df	Sig. (2-sided)
	Pure-plays n (%)	Brick and clicks n (%)				
PRIVACY	47 (52.8)	24 (19.8)	71 (33.8)	24.916	1	(.000)
SECURITY	65 (73.0)	73 (60.3)	138 (65.7)	3.673	1	(.055)
RATING	26 (29.2)	17 (14.0)	43 (20.5)	7.342	1	(.007)
AWARD	27 (30.3)	17 (14.0)	44 (21.0)	8.214	1	(.004)
ANY_EPeA	75 (84.3)	78 (64.5)	153 (72.9)	10.173	1	(.001)
EPeA	Monetary value		Total n (%)	χ^2	df	Sig. (2-sided)
	Low n (%)	High n (%)				
PRIVACY	24 (21.6)	47 (47.5)	71 (33.8)	15.629	1	(.000)
SECURITY	63 (56.8)	75 (75.8)	138 (65.7)	8.385	1	(.004)
RATING	18 (16.2)	25 (25.3)	43 (20.5)	2.624	1	(.105)
AWARD	7 (6.3)	37 (37.4)	44 (21.0)	30.495	1	(.000)
ANY_EPeA	69 (62.2)	84 (84.8)	153 (72.9)	13.619	1	(.000)

Contingency table computed for a 2 × 2 design
Pearson Chi-square (2 tailed)

nificant difference in line with expectations can be observed for the incorporation in the website of *'Award Seals'* (average number of ASs $= 1.16_{StrongReputation}$ vs. $0.28_{WeakReputation}$; independent samples t-test, $p = .058$). 'Award Seals' are featured in 26.7 % of the websites with a weaker reputation as compared to in 15.2 % of those with a stronger reputation (χ^2 test $p = .042$)*, supporting H2d.*

Offline presence

- Retailers with an *'offline presence'* also appear to adopt less EPeAs as compared to 'pure players' (average number of EPeAs $= 1.30_{BrickandClick}$ vs. $2.30_{PurePlay}$; independent samples t-test, $p < .001$). While 84.3 % of 'pure players' display at least one EPeA, only 64.5 % of 'brick and click' retailers do apply EPeAs (χ^2 test $p = .001$). This appears to be true for the adoption of each of the individual seals, *which not only provides general support for H4, but also specific support for H4a, H4b, H4c as well as H4d.*
- *'Privacy Seals'* are apparently featured less in e-stores with offline presence (19.8 %) as in commercial websites without offline existence (52.8 %; χ^2 test

Table 9 Total number of EPeAs adopted among e-retailer categories

Independent variables	Main effects independent samples t-tests								
	Reputation			Offline presence			Monetary value		
	Mean		Sig.	Mean		Sig.	Mean		Sig.
	Low	High		No	Yes		Low	High	
Dependent variables									
TOTAL EPeAs	2.05	1.40	(.002)	2.30	1.30	(.000)	1.23	2.27	(.000)
TOTAL NUMBER OF PRIVACY SEALS	.457	.285	(.023)	.595	.206	(.000)	.252	.505	(.001)
TOTAL NUMBER OF SECURITY SEALS	1.06	.790	(.011)	1.10	.801	(.007)	.747	1.13	(.000)
TOTAL NUMBER OF RATING SEALS	.247	.161	(.125)	.292	.140	(.010)	.162	.252	(.110)
TOTAL NUMBER OF AWARD SEALS	.276	161	(.058)	.314	.148	(.009)	.072	.383	(.000)
PRIVACY SEAL INVESTMENTS in $/y	493	308	(.022)	640	224	(.000)	267	550	(.000)
SECURITY SEAL INVESTMENTS in $/y	1,486	957	(.001)	1,406	1,087	(.047)	1,020	1,449	(.007)
TOTAL SEAL INVESTMENTS in $/y	1,979	1,265	(.000)	2,046	1,310	(.000)	1,287	1,998	(.000)

Sample (n = 210)
p values are reported in parentheses

$p < .001$; average number of PSs $= 0.21_{BrickandClick}$ versus $0.60_{PurePlay}$; independent samples t-test, $p < .001$).

- Also *'Security Seals'* turn out to be displayed somewhat less by 'brick and click' retailers than by 'pure plays' ($60.3\,\%_{BrickandClick}$ versus $73.0\,\%_{PurePlay}$, χ^2 test $p = .055$; average number of SSs $= 0.80_{BrickandClick}$ versus $1.10_{PurePlay}$; independent samples t-test, $p = .007$).
- This is also the case for *'Rating Seals'*, which are also featured less by 'brick and clicks' than by 'pure plays' ($14.0\,\%_{BrickandClick}$ vs. $29.2\,\%_{PurePlay}$, χ^2 test $p = .007$; average number of RSs $= 0.14_{BrickandClick}$ versus $0.29_{PurePlay}$; independent samples t-test, $p = .010$).
- Finally, also *'Award Seals'* are displayed less frequently among e-vendors with offline presence than among those without ($14.0\,\%_{BrickandClick}$ versus $30.3\,\%_{PurePlay}$, χ^2 test $p = .004$; average number of ASs $= 0.15_{BrickandClick}$ versus $0.31_{PurePlay}$; independent samples t-test, $p = .009$).

Monetary value of products traded

- As expected, e-tailers selling products of a higher *'monetary value'* feature more EPeAs on their websites as compared to those selling relatively cheaper merchandise (average number of EPeAs $= 2.27_{ExpensiveMerchandise}$ vs. $1.23_{CheaperMerchandise}$; independent samples t-test, $p < .001$). While 84.8 % of the merchants selling more expensive products exhibit at least one EPeA, only 62.2 % of those vending less expensive goods display any EPeA (χ^2 test $p < .001$). *This provides some general support for H6.*
- This is the case for the adoption of almost all of the individual seals: *'Privacy Seals'* amongst others, appear more adopted among e-commerce vendors selling more expensive wares ($47.5\,\%_{ExpensiveMerchandise}$ vs. $21.6\,\%_{CheaperMerchandise}$, χ^2

test $p < .001$; average number of PSs $= 0.51_{ExpensiveMerchandise}$ versus $0.25_{CheaperMerchandise}$; independent samples t-test, $p = .001$). *Supporting H6a.*
- Also more *'Security Seals'* appear to be displayed in websites of e-tailers selling more expensive goods (average number of SSs $= 1.13_{ExpensiveMerchandise}$ vs. $0.75_{CheaperMerchandise}$; independent samples t-test, $p < .001$). They are featured in 75.8 % of the websites of merchants selling expensive wares, as compared to in only 56.8 % of those selling cheaper products (χ^2 test $p = .004$). *This provides support for H6b.*
- For *'Rating Seals'* also a small difference in the expected direction seems to emerge, however this difference remains insignificant. *Thus H6c cannot be confirmed.*
- *'Award Seals',* in contrast, as expected, clearly featured significantly more often in websites of e-tailers selling relatively more expensive goods as compared to those selling less expensive goods (37.4 % vs. 6.3 %; χ^2 test $p < .001$; average number of ASs $= 0.38_{ExpensiveMerchandise}$ vs. $0.07_{CheaperMerchandise}$; independent samples t-test, $p < .001$). *H6d can therefore be accepted.*
- Some final encompassing analyses (reported in Table 10) demonstrate that these findings regarding the impact of the *'monetary value of goods traded'* on the adoption of EPeAs remain valid when controlling for *'reputation'* and *'offline presence'*. As far as the adoption of *'Security Seals'* is concerned, it should be pointed out that the difference established is only valid in case of online vendors with a strong reputation. For those with a weaker reputation no difference can be discerned with respect to the monetary value of merchandise traded. A considerable amount of online vendors with a weaker reputation (76.2 %) do appear to feature *'Security Seals'* regardless of the monetary value of their offerings.

6.3 Trust assurance seal investments among different e-retailer categories

As the costs related to the adoption of different kinds of seals appear to differ remarkably, we also aimed to indirectly assess and compare the total *'investments'* made by different e-vendors to integrate externally provided e-assurances in their websites. E-retailers may select trust promoting cues according to the assurances they want to provide and the kind of trustworthiness they want to 'signal'. A company may opt for only one "relatively expensive" *McAfee* security seal, or it may utilize a dozen of relatively "cheap" security seals such as *GoDaddy* or *Digicert*. According to our estimated results, e-assurance investments among top e-tailers vary from nothing at all to $5510 per year (*Total Seal Investments*: $M = 1622$ $ per year, $SD = 1442$). On average, more seems to be invested in externally provided *'Security Seals'* ($M = 1222$ $ per year, $SD = 1153$), than in externally provided *'Privacy Seals'* ($M = 400$ $ per year, $SD = 586$).

Some independent samples t-tests (reported in Table 8) illustrate how the amount of money invested in e-assurance seals varies across retailer categories. The results reveal that total seal investments are higher among e-commerce companies with a weaker *'reputation'* (Average Seal Investment $= 1979\$_{StrongReputation}$ vs. $1265\$_{WeakReputation}$; independent samples t-test, $p < .001$). As expected they also turn out to be higher for e-tailers without *'offline presence'* (Average Seal

Table 10 Adoption of EPeAs among e-retailer categories

Offline presence	Reputation	EPeA seal types	Monetary value		Chi-square (*p* value)	Total n (%)
			Low n (%)	High n (%)		
Pure plays (n = 89)	Weak reputation (n = 50)	PRIVACY	11 (50.0)	19 (67.9)	1.637 (.201)	30 (60.0)
		SECURITY	18 (81.8)	24 (85.7)	.139 (.709)	42 (84.0)
		RATING	7 (31.8)	9 (32.1)	.001 (.981)	16 (32.0)
		AWARD	3 (13.6)	15 (53.6)	8.528 (.003)	18 (36.0)
		ANY_EPeA	20 (90.9)	28 (100.0)	2.652 (.103)	48 (96.0)
			n = 22	n = 28		
	Strong reputation (n = 39)	PRIVACY	8 (34.8)	9 (56.2)	1.768 (.184)	17 (43.6)
		SECURITY	11 (47.8)	12 (75.0)	2.880 (.090)	23 (59.0)
		RATING	4 (17.4)	6 (37.5)	2.001 (.157)	10 (25.6)
		AWARD	2 (8.7)	7 (43.8)	6.532 (.011)	9 (23.1)
		ANY_EPeA	12 (52.2)	15 (93.8)	7.657 (.006)	27 (69.2)
			n = 23	n = 16		
	Total	PRIVACY	19 (42.2)	28 (63.6)	4.094 (.043)	47 (52.8)
		SECURITY	29 (64.4)	36 (81.8)	3.410 (.065)	65 (73.0)
		RATING	11 (24.4)	15 (34.1)	1.001 (.317)	26 (29.2)
		AWARD	5 (11.1)	22 (50.0)	15.920 (.000)	62 (69.7)
		ANY_EPeA	32 (71.1)	43 (97.7)	11.889 (.001)	75 (84.3)
Brick and clicks (n = 121)	Weak reputation (n = 55)	PRIVACY	1 (3.6)	11 (40.7)	11.133 (.001)	12 (21.8)
		SECURITY	19 (67.9)	19 (70.4)	.041 (.840)	38 (69.1)
		RATING	4 (14.3)	6 (22.2)	.582 (.446)	10 (18.2)
		AWARD	2 (7.1)	8 (29.6)	4.672 (.031)	10 (18.2)
		ANY_EPeA	19 (67.9)	20 (74.1)	.258 (.612)	39 (70.9)
			n = 28	n = 28		
	Strong reputation (n = 66)	PRIVACY	4 (10.5)	8 (28.6)	3.529 (.060)	12 (18.2)
		SECURITY	15 (39.5)	20 (71.4)	6.609 (.010)	35 (53.0)
		RATING	3 (7.9)	4 (14.3)	.694 (.405)	7 (10.6)
		AWARD	0 (.0)	7 (25.0)	10.627 (.001)	7 (10.6)
		ANY_EPeA	18 (47.4)	21 (75.0)	5.092 (.024)	39 (59.1)
			n = 38	n = 28		
	Total	PRIVACY	5 (7.6)	19 (34.5)	13.723 (.000)	24 (19.8)
		SECURITY	34 (51.5)	39 (70.9)	4.715 (.030)	73 (60.3)
		RATING	7 (10.6)	10 (18.2)	1.426 (.232)	17 (14.0)

Table 10 continued

Ofline presence	Reputation	EPeA seal types	Monetary value		Chi-square (*p* value)	Total n (%)
			Low n (%)	High n (%)		
		AWARD	2 (3.0)	15 (27.3)	14.600 (.000)	17 (14.0)
		ANY_EPeA	37 (56.1)	41 (74.5)	4.475 (.034)	78 (64.5)
Total (n = 210)	Weak reputation (n = 105)	PRIVACY	12 (24.0)	30 (54.5)	10.182 (.001)	42(40.0)
		SECURITY	37 (74.0)	43 (78.2)	.252 (.615)	80 (76.2)
		RATING	11 (22.0)	15 (27.3)	.391 (.532)	26 (24.8)
		AWARD	5 (10.0)	23 (41.8)	13.559 (.000)	28 (26.7)
		ANY_EPeA	39 (78.0)	48 (87.3)	1.585 (.208)	87 (82.9)
			n = 50	n = 55		
	Strong reputation (n = 105)	PRIVACY	12 (19.7)	17 (38.6)	4.599 (.032)	29 (27.6)
		SECURITY	26 (42.6)	32 (72.7)	9.369 (.002)	58 (55.2)
		RATING	7 (11.5)	10 (22.7)	2.385 (.123)	17 (16.2)
		AWARD	2 (3.3)	14 (31.8)	16.120 (.000)	16 (15.2)
		ANY_EPeA	30 (49.2)	36 (81.8)	11.663 (.001)	66 (62.9)
			n = 61	n = 44		
	Total	PRIVACY	24 (21.6)	47 (47.5)	15.629 (.000)	71 (33.8)
		SECURITY	63 (56.8)	75 (75.8)	8.385 (.004)	138 (65.7)
		RATING	18 (16.2)	25 (25.3)	2.624 (.105)	43 (20.5)
		AWARD	7 (6.3)	37 (37.4)	30.495 (.000)	44 (21.0)
		ANY_EPeA	69 (62.2)	84 (84.8)	13.619 (.000)	153(72.9)
			n = 111	n = 99		

Contingency table computed for a 2 × 2 × 2 design. Pearson Chi-square (2 tailed)

Investment = 2046$_{PurePlays}$ vs. 1310$_{BrickandClick}$; independent samples t-test, $p < .001$). Finally, in line with expectations the investment in e-assurance seals apparently also depends on the *'monetary value of traded merchandise'* (Average Seal Investment = 1998$_{ExpensiveMerchandise}$ vs. 1287$_{CheapMerchandise}$; independent samples t-test, $p < .001$).

7 Discussion and conclusions

In this paper, a comprehensive discussion of trust assurance mechanisms is provided as well as a snapshot of their adoption among thriving e-retailers. Our findings show that almost all B2C e-commerce websites examined in this study feature *'internally provided e-assurances'* (IPeAs): 98.1 % display a *'Privacy Policy'*, 40 % exhibit a *'Security Policy'* and 73.3 % provide a *'Return Policy'*. It is obvious that these thriving e-retailers put much effort in taking technical and personal measures to protect consumers' private data from unauthorized use. There have been many cases where consumers have suffered from illegal online business practices. Recently, 22 online businesses have been accused of linking their consumers with discount promotions that ended up charging them illegal fees [70]. Among them, there are big names such as 'Staples', 'Barnes and Nobles', 'Orbitz', 'Avon Products' and'1–800-Flowers.com'. Software company 'Echometrix' has been fined $100,000 for selling its clients' data to external marketing companies without its customers' knowledge [34]. 'Real Networks Inc.' has used its downloadable Real Jukebox CD player to secretly collect all sorts of data on its customers' listening habits and to automatically send this data back to Web servers at Real Networks' corporate offices [86]. In August 2000, a famous toy retailer 'Toys "R" Us' and its baby sites 'Babies "R" Us', 'Lucy.com', and 'Fusion.com' forwarded their customer information to the marketing company 'Coremetrics', which used the data to build demographic information for vendor websites [60]. Our findings show that thriving e-retailers are doing everything they can to prevent such illegal practices and to communicate their trustworthiness through IPeAs.

Since the boom of the internet, online shoppers have been severely targeted by cyber criminals. According to Consumer Reports, one in five online consumers have been victims in the last two years and consumers have lost around $8 billion due to viruses, spyware and phishing [25]. In January 2011, for example, customers of cosmetics company 'Lush' have experienced unauthorized use of their credit cards as the company's main e-commerce website in the United Kingdom has been attacked by an anonymous hacker who broke into its database and stole thousands of credit card numbers [85]. A similar incident has happened in May of 2011; a group of hackers breached Sony's PSN, Qriocity music service, and Sony Online network and stole data from more than 100 million users, including encrypted credit card numbers [92]. A recent study by LexisNexis Risk Solutions [57] reveals that e-retailers in the U.S. lost more than $139 billion due to identify theft and charge-backs where they incurred $310 in total losses for every $100 in fraudulent transactions during 2010. According to the study, there were 6.5 million consumer victims of credit card fraud and 3.5 million shoppers experienced debit card fraud, which caused $5.5 billion in costs [57].

As these kinds of frightening online fraud statistics are widely covered by the media, Web users are becoming smart about online security and many of them look for the padlock icon, the "https" prefix, a green address bar or trust promoting seals before making a purchase, creating an account or submitting personal information to any website [29]. Since many traditional cues for assessing trust in the physical world are not available online [78,90], the presence of encryption or e-assurance seals increases the likelihood that participants make an online purchase [66]. Our findings reveal that thriving e-retailers are well aware of the importance of institution-based trust as a crucial antecedent of online purchase behavior, as quite a lot of them do feature *'externally provided e-assurances'* (EPeAs). According to our findings 72.9 % of the investigated web-shops also feature *'externally provided e-assurances'* (EPeAs): 65.7 % expose *'Security Seals'*, 33.8 % display *'Privacy Seals'*, 21.0 % exhibit *'Award Seals'* and 20.5 % present *'Rating Seals'*. These additional assurances are provided in order to ensure rigorous protection and to (re)establish consumer trust in online vendors.

Aiming to identify a link between the characteristics of an online vendor and the specific types of trust assurances applied, we identified some important factors determining the need for assurances and their subsequent adoption. The e-vendor's *'reputation'*, whether there is an *'offline presence'* or not and the *'monetary value of goods traded'*, all appear to be important determining factors.

Our results reveal that top e-tailers with a relatively stronger *'reputation'* make more use of IPeAs as compared to online vendors with a relatively weaker reputation. More specifically they appear to feature 'Privacy Policies' more often. In contrast, e-commerce merchants with a stronger reputation appear to display less EPeAs in comparison with their relatively less reputable counterparts. They appear to feature 'Privacy Seals', 'Security Seals' and 'Rating Seals' less often. Thus, our results demonstrate that e-retailers with a relatively higher reputation rely more on internally provided e-assurance mechanisms such as privacy policy and money back guarantee, and that they make less use of third-party trust endorsements. This finding is consistent with prior research which confirms that third-party assurances have a significant positive effect when the vendor is unknown and that their use is unnecessary for highly reputable vendors (e.g., [106]).

Whether the e-tailer has an *'offline presence'* or not does not appear to affect the number of IPeAs displayed in its website. E-vendors with an 'offline presence', however, do appear to feature less EPeAs in comparison to 'pure players'. This is true for 'Privacy Seals', 'Security Seals', 'Rating Seals' as well as 'Award Seals'.

As expected, e-tailers selling products of a higher *'monetary value'* feature more IPeAs on their website as compared to those selling relatively less expensive products. They appear to display Security and Return Policies more often. In contrast, they do not always seem to display a Privacy Policy. They are also found to offer more EPeAs on their website: they display 'Privacy Seals', 'Security Seals' and 'Award Seals' more often in comparison with those selling relatively cheaper wares.

Finally, we established indirectly that top e-tailers invest a considerable amount of money on trust assuring seals. These investments also seem to vary across retailer categories. The results reveal that total seal investments are higher among e-commerce companies with a weaker *'reputation'*, among those *'without offline presence'*, and among e-tailers selling relatively *'more expensive merchandise'*. This is in line with expectations as these companies have a stronger need to 'signal' their trustworthiness.

8 Limitations and suggestions for further research

While this study provides some interesting insights regarding the adoption of e-assurances by B2C commercial websites, it has some limitations that should be considered. First, the nature of this empirical work is a *'natural observation'*. While it allows us to provide a description of the current situation, we can only attempt to provide logical explanations for our observations. Based on the findings acquired by means of this research technique we cannot definitely answer the "why" questions, which provides some room for further investigation. A survey among e-vendors may provide a better picture of their reasons for adopting certain seals.

Questioning the online merchants may also provide a solution to another limitation of this study, which relates to the *'indirect assessment of the investments'* involved. In order to indirectly assess and compare the total investments made by different e-vendors to integrate externally provided e-assurances in their websites, we multiplied the presence of e-assurance seals with their 'average' costs. Still, as these costs for the same seal can vary considerably, depending on several different factors, it may be more appropriate to have the e-tailer provide more detailed information concerning his exact costs.

Another limitation involves the *'coding process'* used to register the availability of different e-assurance cues in the websites. As this coding is performed by only one of the authors, some bias in the coding is conceivable. Still, according to Hayes and Krippendorff [27] there is no real need to perform an additional recording of the nominal data by different observers to ensure reliability, as the pragmatic coding scheme only involved two clear possibilities (absence = 0; presence = 1).

Furthermore, the *'sample'* for this study included only a limited group of *'thriving' e-retailers*, because we aimed to provide a snapshot of their best practices. However, while these top-ranked e-tailers may have the necessary resources to invest in the most appropriate externally provided e-assurances, they also appear to have a less stringent need for EPeAs as they can rely more on internally provided e-assurances (IPeAs) to provide the desired 'signal' of trustworthiness. Based on this limited sample we could already establish the vital role of 'reputation' as an important determining factor in the adoption of trust assurances. Future research should therefore also include lower ranked, less familiar e-vendors and start-ups.

'*Categorizing online merchants'* according to the monetary value of the merchandise they sell is not a straightforward task, because within one single product category often cheaper as well as more expensive products are provided. We relied on the categorization of industries proposed by Karimov and Brengman [40] that represents a continuum from 'less' to 'more expensive' product categories and recognize that this is not a clear-cut categorization. We also acknowledge that Rossiter and Percy's [87] conceptualization of involvement (low vs. high) may provide a more theoretical and encompassing base for categorizing online vendors, but we feel it is less straightforward to use for the objective classification of the entire product category, as consumer involvement may be brand and target specific, depending amongst others on brand preference, experience and expertise.

Further research should also investigate *'how consumers experience the need for trust assurance mechanisms'* among different kinds of online retailers. Next to the monetary value of products, the degree of consumer involvement, as well as risk perceptions in a particular shopping context should be taken into account. Moreover, it should be examined whether and how customers actually distinguish between different IPeAs and EPeAs.

Based on our observations and review of available empirical studies, we recommend that future experimental research considers the *'monetary value'* of products sold, as well as control for *'reputation'* and *'offline presence'* when testing the effectiveness of e-assurance structures in generating online trust. Finally, our results regarding the adoption of e-assurance mechanisms by top online retailers are limited to a certain time period. It would be interesting to perform a longitudinal study to see how the adoption of trust assurance mechanisms will evolve over time.

9 Managerial implications

According to the findings in this study, e-commerce vendors with a *'relatively weaker reputation'*, *'without offline presence'* and *'selling more expensive merchandise'* are in need of more cues 'signaling' their trustworthiness to potential consumers. They need to recognize this larger need when they consider the adoption of externally provided assurances. Since online shoppers are more reluctant to give their credit card number to unfamiliar e-retailers [59,66], reducing vendor-related perceived risk is also specifically crucial for this category. Thus, *'unfamiliar e-retailers'* and *'start-up businesses'* in particular also need to consider providing more third-party e-assurance structures in order to reduce consumers' risk perceptions and generate trust. E-tailers first need to have acquired a well established reputation in order to be able to rely on internally provided e-assurances only (i.e. privacy, security and return policies).

In this study, we noted that 29 % of e-retailers adopted externally provided privacy assurance mechanisms as well as externally provided security assurance mechanisms, both at the same time. According to Hu et al. [32], however, combining a privacy assurance seal with a security assurance seal weakens the effects of both assurance mechanisms in enhancing consumers' trust. In fact, Hu et al. [32] confirm that each of these two assurance mechanisms have a significant positive impact in enhancing consumers' trust, as long as the other one is absent. The effect of either function on enhancing consumers' trust is weakened by the presence of the other. For this reason, e-retailers must be careful in choosing the appropriate seals, because the extra money paid for more assurance mechanisms could be wasted and even counterproductive.

Acknowledgments We would like to thank the anonymous reviewers and the editor for their helpful and constructive suggestions. Special thanks for Prof. dr. Jaafar El-Murad (Head of Department of Business Strategy and Marketing at University of Westminster, London) for proofreading and correcting the English.

10 Appendix

See Tables 11, 12.

Table 11 Coding Scheme of e-assurance mechanisms (IPeA and EPeA variables)

Category	Code	Subcategory
Internally and externally provided e-assurances		
IPeA	PRIVACY_POLICY	Privacy policy (0/1)
	SECURITY_POLICY	Security policy (0/1)
	RETURN_POLICY	Return policy (0/1)
	ANY_IPeA	= ANY_PRIVACY_POLICY or SECURITY_POLICY … or RETURN_POLICY; binary (0/1)
	TOTAL_IPeA	PRIVACY_POLICY + SECURITY_POLICY + RETURN_POLICY; ranges between 0–3
EPeA	Privacy Seal	
	PPRIVACY_SEAL1	BBBOnline Privacy (0/1)
	PPRIVACY_SEAL2	eTRUST (0/1)
	PPRIVACY_SEAL3	TRUSTe (0/1)
	ANY_PRIVACY_SEAL	= PPRIVACY_SEAL1 or PPRIVACY_SEAL2 … or PPRIVACY_SEAL3; binary (0/1)
	TOTAL_ PRIVACY_SEAL	= PPRIVACY_SEAL1 + PPRIVACY_SEAL2 + PPRIVACY_SEAL3; integer, ranges between 0-3
	Security seal	
	SECURITY_SEAL1	Comodo (0/1)
	SECURITY_SEAL2	CyberTrust (0/1)
	SECURITY_SEAL3	Digicert (0/1)
	SECURITY_SEAL4	Entrust (0/1)
	SECURITY_SEAL5	GeoTrust (0/1)
	SECURITY_SEAL6	GoDaddy (0/1)
	SECURITY_SEAL7	HackerSafe (0/1)
	SECURITY_SEAL8	McAfee (0/1)
	SECURITY_SEAL9	RSA Security (0/1)
	SECURITY_SEAL10	SecurityMetrics (0/1)
	SECURITY_SEAL11	Thawte (0/1)
	SECURITY_SEAL12	TrustWave (0/1)
	SECURITY_SEAL13	Verisign (0/1)
	ANY_SECURITY_SEAL	= SECURITY_SEAL1 or SECURITY_SEAL2 … or SECURITY_SEAL6; binary (0/1)
	TOTAL_SECURITY_SEAL	= SECURITY_SEAL1 + SECURITY_SEAL2 … + SECURITY_SEAL6; integer, ranges between 0–13

Table 11 continued

Category	Code	Subcategory
	Rating seal	
	RATING_SEAL1	BizRate (Shopzilla) (0/1)
	RATING _SEAL2	ResellerRating (0/1)
	RATING _SEAL3	Shopping.com (0/1)
	ANY_RATING_SEAL	= RATING_SEAL1 or RATING _SEAL2 … or RATING _SEAL3; binary (0/1)
	TOTAL_RATING_SEAL	= RATING_SEAL1 + RATING _SEAL2 … + RATING _SEAL3; integer, ranges between 0–3
	Award seal	
	AWARD_SEAL1	Inc500 (0/1)
	AWARD_SEAL2	5 StarGuarantee (0/1)
	AWARD_SEAL3	SSPAExcellence (0/1)
	AWARD_SEAL4	Systemax Fortune 1000 (0/1)
	AWARD_SEAL5	Top500 (0/1)
	AWARD_SEAL6	YahooTopService (0/1)
	ANY_AWARD_SEAL	=AWARD_SEAL1 or AWARD_SEAL2 … or AWARD_SEAL6; binary (0/1)
	TOTAL_AWARD_SEAL	=AWARD_SEAL1 + AWARD_SEAL2 … + AWARD_SEAL6; integer, ranges between 0–6
	ANY_EPeA	=ANY_RIVACY or ANY_SECURITY … RS or ANY_AWARD; binary (0/1)
	TOTAL_EPeA	= TOTAL_PRIVACY+TOTAL_SECURITY+TOTAL_ RATING+ TOTAL_AWARD; ranges between 0–30

Source Authors' own research

Table 12 Definitions of explanatory variables

Variable codes	Description	Source
Site-specific variables		
MONETARY_VALUE	= E-commerce sectors have been categorized according to the average value of the products sold: Low (value = 0) *versus* High (1)	Karimov and Brengman [40]
SITE_REPUTATION	We did a median split between 210 retailers based on the InternetRetailer's rankings. Relatively higher ranked retailers are coded = 1; Lower ranked retailers are coded = 0	InternetRetailer's rankings
OFFLINE_PRESENCE	Dummy variable: bricks and clicks= 1, pure-plays = 0	Own survey
PRIVACY_SEAL_COST	Total sum of the privacy seal costs	Own survey
SECURITY_SEAL_COST	Total sum of the security seal costs	Own survey
TOTAL_SEAL_COST	Total sum of the privacy seal and the security seal cost: (= PRIVACY_SEAL_COST + SECURITY_SEAL_COST)	Own survey

References

1. Aljukhadar, M., Senecal, S., & Ouellette, D. (2010). Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments. *International Journal of Electronic Commerce*, *14*(4), 103–126.
2. Antón, A. I., Bertino, E., Li, N., & Yu, T. (2007). A roadmap for comprehensive online privacy policy management. *Communications of the ACM*, *50*(7), 109–116.
3. Arthur, C., & Halliday, J. (2010). Amazon UK goes offline amid threats of cyber attacks. Guardian.co.uk (December 12, 2010). http://www.guardian.co.uk/technology/2010/dec/12/amazon-uk-offline-christmas. Accessed 20 December 2010.
4. Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behaviour. *MIS Quarterly*, *26*(3), 243–268.
5. Bahmanziari, T., Odom, M. D., & Ugrin, J. C. (2009). An experimental evaluation of the effects of internal and external e-Assurance on initial trust formation in B2C e-commerce. *International Journal of Accounting Information Systems*, *10*(3), 152–170.
6. BBBOnline.com. (2011). Accredited membership fees for retail & service industry. http://manitoba.bbb.org/WWWRoot/SitePage.aspx?site=159&id=85f5430f-5705-41e2-8720-c1196a33acf9. Accessed 31 August 2011.
7. Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, *43*(11), 98–105.
8. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613.
9. Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, *7*(2), 117–141.

10. Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management*, *4*(2), 303–318.
11. Chen, J., & Dibb, S. (2010). Consumer trust in the online retail context: Exploring the antecedents and consequences. *Psychology and Marketing*, *27*(4), 323–346.
12. Clemons, E. K. (2007). An empirical investigation of third-party seller rating systems in e-commerce: The case of buySAFE. *Journal of Management Information Systems*, *24*(2), 43–71.
13. Demangeot, C., & Broderick, A. J. (2010). Consumer perceptions of online shopping environments: A gestalt approach. *Psychology & Marketing*, *27*(2), 117–140.
14. Demery, P. (2010a). Hackers attack e-retailers on peak shopping days. InternetRetailer.com (December 16, 2010). http://www.internetretailer.com/2010/12/16/hackers-attack-e-retailers-peak-shopping-days. Accessed 20 December 2010.
15. Demery, P. (2010b). Return policies can win over customers, and there's more than one path to success. InternetRetailer.com (March 31, 2010). http://www.internetretailer.com/2010/03/31/get-back. Accessed 20 January 2011.
16. Dodds, W. B., Monroe, K. B., & Grewal, D. (1991). Effects of price, brand, and store information on buyers' product evaluations. *Journal of Marketing Reseearch*, *28*(3), 307–319.
17. Eastlick, M. A., & Lotz, S. (2011). Cognitive and institutional predictors of initial trust toward an online retailer. *International Journal of Retail & Distribution Management*, *39*(4), 234–255.
18. Fisher, R., & Chu, S. Z. (2009). Initial online trust formation: The role of company location and web assurance. *Managerial Auditing Journal*, *24*(6), 542–563.
19. Ganguly, B., Dash, B. S., Cyr, D., & Head, M. (2010). The effects of website design on purchase intention in online shopping: The mediating role of trust and the moderating role of culture. *International Journal of Electronic Business*, *8*(4/5), 302–330.
20. Gavish, B., & Tucci, C. L. (2006). Fraudulent auctions on the Internet. *Electronic Commerce Research*, *6*(2), 127–140.
21. Gavish, B., & Tucci, C. L. (2008). Reducing internet action fraud. *Communications of the ACM*, *51*(5), 89–97.
22. Gavish, B., & Sobol, M. (2010). Warranty policy impact on net revenues as a function of part replacements and optional purchases. *International Journal of Information Technology & Decision Making*, *9*(4), 507–523.
23. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90.
24. Griffith, E. (2008). Amazon.com web site down. AppScout.com (June 6, 2008). http://www.appscout.com/2008/06/amazoncom_web_site_down.php. Accessed 20 December 2010.
25. Hackett, L. (2009). Consumer Reports survey: One in five online consumers has been victims of cybercrime. Consumer Reports (May 4, 2009). http://www.consumersunion.org/pub/core_financial_services/011331.html. Accessed 01 February 2011.
26. Hahn, K. H., & Kim, J. (2009). The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context. *International Journal of Retail & Distribution Management*, *37*(2), 126–141.
27. Hayes, A. F., & Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data. *Communication Methods and Measures*, *1*(1), 77–89.
28. Head, M. M., & Hassanein, K. (2002). Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly Journal of Electronic Commerce*, *3*(3), 307–325.
29. Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology*, *8*(4), 1–35.
30. Hiller, J. S. (2010). The regulatory framework for privacy and security. In J. Hunsinger, L. Klastrup, & A. Matthew (Eds.), *International Handbook of Internet Research* (pp. 251–266). Virginia, USA: Springer.
31. Hu, Z., Lin, Z., & Zhang, H. (2002). Trust-promoting seals in electronic markets: An exploratory study of their effectiveness for online sales promotion. *Journal of Promotion Management*, *9*(1–2), 163–180.
32. Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, *48*(2), 407–418.

33. Huang, P., Lurie, N. H., & Mitra, S. (2009). Searching for experience on the Web: An empirical examination of consumer behavior for search and experience goods. *Journal of Marketing*, *73*(2), 55–69.
34. Huffman, M. (2010). Software company sold children's chats to marketers. ConsumerAffairs.com (September 15, 2010). http://www.consumeraffairs.com/news04/2010/09/software_company_sold_childrens_chats_to_marketers.html. Accessed 04 February 2011.
35. Internet Crime Complaint Center. (IC3) Internet crime report. FBI IC3 (2009). http://www.ic3.gov/media/annualreports.aspx. Accessed 20 December 2010.
36. InternetRetailer. (2010). Top 500 Guide. http://www.internetretailer.com/top500/list/. Accessed 23 August 2010.
37. Jack, E. P., Powers, T. L., & Skinner, L. (2009). Reverse logistics capabilities: Antecedents and cost savings. *International Journal of Physical Distribution and Logistics Management*, *40*(3), 228–246.
38. Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, *1*(1/2), 45–71.
39. Kaplan, S. E., & Nieschwietz, R. J. (2003). A Web assurance model of trust for B2C e-commerce. *International Journal of Accounting Information Systems*, *4*(2), 95–114.
40. Karimov, F. P., & Brengman, M. (2011). Adoption of social media by online retailers: Assessment of current practices and future directions. *International Journal of E-Entrepreneurship and Innovation*, *2*(1), 26–45.
41. Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's Model of Argumentation. *Information Systems Research*, *17*(3), 286–300.
42. Kim, D., & Benbasat, I. (2010). Designs for effective implementation of trust assurances in Internet stores. *Communications of the ACM*, *53*(2), 121–126.
43. Kim, K., & Kim, J. (2010). Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust. *Journal of Interactive Marketing*, *25*(3), 145–158.
44. Kim, D. J., Sivasailam, N., & Rao, H. R. (2004). Information assurance in B2C websites for information goods/services. *Electronic Markets*, *14*(4), 344–359.
45. Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, *9*(1), 84–95.
46. Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application*, *4*(2), 63–82.
47. Krippendorff, K. (2004). *Content analysis: Introduction to its methodology* (2nd ed., p. 18). Beverley Hills, CA: Sage Publications Inc.
48. Kuan, H.-H., & Bock, G.-W. (2007). Trust transference in brick and click retailers: An investigation of the before-online-visit phase. *Information & Management*, *44*(2), 175–187.
49. Kukar-Kinney, M., & Close, A. G. (2010). The determinants of consumers′online shopping cart abandonment. *Journal of the Academy of Marketing Science*, *38*(2), 240–250.
50. Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*(5), 323–331.
51. Laurent, G., & Kapferer, J.-N. (1985). Measuring consumer involvement profiles. *Journal of Marketing Research*, *22*(1), 41–53.
52. Lawton, C. (2008). The war on returns. The Wall Street Journal (May 8, 2008). http://online.wsj.com/article/SB121020824820975641.html. Accessed 25 December 2010.
53. Lee, C. H., & Cranage, D. A. (2010). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, *32*(5), 987–994.
54. Lee, S. M., & Lee, S. (2005-2006). Consumers' initial trust toward second-hand products in the electronic market. *Journal of Computer Information Systems*, *46*(2), 85–98.
55. Lee, C. H., Eze, U. C., & Ndubisi, N. O. (2011a). Analyzing key determinants of online repurchase intentions. *Asia Pacific Journal of Marketing and Logistics*, *23*(2), 200–221.
56. Lee, J., Park, D.-H., & Han, I. (2011b). The different effects of online consumer reviews on consumers' purchase intentions depending on trust in online shopping malls: An advertising perspective. *Internet Research*, *21*(2), 187–206.

57. LexisNexis. (2010). True cost of fraud study. LexisNexis (2010). http://img.en25.com/Web/LexisNexis/2010%20True%20Cost%20of%20Retail%20Fraud%20Study.pdf. Accessed 25 December 2010.
58. Lian, J.-W., & Lin, T.-Z. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior*, *24*(1), 48–65.
59. Lim, N. (2003). Consumers' perceived risk: Sources versus consequences. *Electronic Commerce Research and Applications*, *2*(3), 216–228.
60. Liu, L., & Arnett, P. (2002). An examination of privacy policies in Fortune 500 Web Sites. *Mid-American Journal of Business*, *17*(1), 13–21.
61. Liu, C., Marchewka, J. T., Lu, J., & Yu, Ch-Sh. (2004). Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 127–142.
62. López-Bonilla, J. N., & López-Bonilla, L. M. (2008). Sensation seeking and e-shoppers. *Electronic Commerce Research*, *8*(3), 143–154.
63. Lowengart, O., & Tractinsky, N. (2001). Differential effects of product category on shoppers' selection of web-based stores: A probabilistic modeling approach. *Journal of Electronic Commerce Research*, *2*(4), 142–156.
64. Maheswaran, D., & Chaiken, S. (1991). Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. *Journal of Personality and Social Psychology*, *61*(1), 13–25.
65. Martín, S. S., & Camarero, C. (2008). Consumer trust to a Web site: Moderating effect of attitudes toward online shopping. *Cyberpsychology and Behavior*, *11*(5), 549–554.
66. Mascha, M. F., Miller, C. L., & Janvrin, D. J. (2011). The effect of encryption on Internet purchase intent in multiple vendor and product risk settings. *Electronic Commerce Research*, *11*(4), 401–419.
67. Maynard, M., & Tian, Y. (2004). Between global and global: Content analysis of the Chinese Web Sites of the 100 top global brands. *Public Relations Review*, *30*(3), 285–291.
68. McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, *23*(3), 473–490.
69. McKnight, D. H., Kachmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a Web business. *Electronic Markets*, *14*(3), 252–266.
70. McMullen, T. (2010). New York Attorney General alleges online retail fraud. abcNEWS (January 29, 2010). http://abcnews.go.com/Business/ny-attorney-general-alleges-online-retail-fraud/story?id=9697913. Accessed 05 February 2011.
71. Miyazaki, A. D., Grewal, D., & Goodstein, R. C. (2005). The effect of multiple extrinsic cues on quality perceptions: A matter of consistency. *Journal of Consumer Research*, *32*(1), 146–153.
72. Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3–20.
73. Mukhopadhyay, S. K., & Setoputro, R. (2005). Optimal return policy and modular design for build-to-order products. *Journal of Operations Management*, *23*(5), 496–506.
74. Muylle, S., & Basu, A. (2004). Online support for commerce processes and survivability of Web retailers. *Decision Support Systems*, *38*(1), 101–113.
75. Nöteberg, A., Christiaanse, E., & Wallage, P. (2003). Consumer trust in electronic channels: The impact of electronic commerce assurance on consumers' purchasing likelihood and risk perceptions. *E-Service Journal*, *2*(2), 46–67.
76. Olson, J. C., & Jacoby, J. (1972). Cue utilization in the quality perception process. In M. Venkatesan (Ed.), *Proceedings of the third annual conference of the association for consumer research* (pp. 167–79). Association for Consumer Research: Iowa City.
77. Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331–338.
78. Patton, M. A., & Josang, A. (2004). Technologies for trust in electronic commerce. *Electronic Commerce Research*, *4*(1–2), 9–21.
79. Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37–59.
80. Pennington, R., Wilcox, H. D., & Grover, V. (2003-2004). The role of system trust in business-to-consumer transactions. *Journal of Management Informaiion Systems*, *20*(3), 197–226.

81. Ramanathan, R. (2010). E-commerce success criteria: Determining which criteria count most. *Electronic Commerce Research*, *10*(2), 191–208.
82. Ray, S., Ow, T., & Kim, S. S. (2011). Security assurance: How online service providers can influence security control perceptions and gain trust. *Decision Sciences*, *42*(2), 391–412.
83. Ries, B. (2010). Hackers' most destructive attacks. TheDailyBeast.com (December 13, 2010). http://www.thedailybeast.com/blogs-and-stories/2010-12-11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns/. Accessed 20 December 2010.
84. Rifon, N. J., La Rose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of Web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339–62.
85. Rigoli, E. (2011). Credit fraud: Cosmetics Company Lush shuts down UK website, speaks directly to hacker. PrivateWifi.com (January 25, 2011). http://www.privatewifi.com/credit-fraud-cosmetics-company-lush-shuts-down-uk-website-speaks-directly-to-hacker/. Accessed 02 February 2011.
86. Robinson, S. (1999). CD software said to gather data on users. New York Times (November 01, 1999). http://www.nytimes.com/1999/11/01/business/cd-software-said-to-gather-data-on-users.html. Accessed 02 February 2011.
87. Rossiter, J. R., & Percy, L. (1985). Advertising communication models. *Advances in Consumer Research*, *12*, 510–524.
88. Runyan, B., Smith, K. T., & Smith, L. M. (2008). Implications of Web assurance services on e-commerce. *Accounting Forum*, *32*(1), 46–61.
89. Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting Web site visitors into buyers: How Web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing*, *70*(2), 133–48.
90. Serban, C., Chen, Y., Zhang, W., & Minsky, N. (2008). The concept of decentralized and secure electronic marketplace. *Electronic Commerce Research*, *8*(1–2), 79–101.
91. Shahibi, M. S., & Bakar, Z. A. (2010). E-commerce interaction and the elements of trust. *The Business and Management Quarterly Review*, *1*(4), 1–7.
92. Sherr, I. & Schatz, A. (2011). Sony Details Hacker Attack. The Wall Street Journal (May 5, 2011). http://online.wsj.com/article/SB10001424052748703849204576302970153688918.html. Accessed 22 June 2011.
93. Shim, S., & Lee, B. (2010). An economic model of optimal fraud control and the aftermarket for security services in online marketplaces. *Electronic Commerce Research and Applications*, *9*(5), 435–445.
94. Sinclaire, J. K., Simon, J. C., & Wilkes, R. B. (2010). A prediction model for initial trust formation in electronic commerce. *International Business Research*, *3*(4), 17–27.
95. Sivasailam, N., Kim, D. J., & Rao, H. R. (2002). What companies are(n't) doing about Web site assurance. *IEEE IT Professional*, *4*(3), 33–40.
96. Skinner, L. R., Bryant, P. T., & Richey, G. (2008). Examining the impact of reverse logistics disposition strategies. *International Journal of Physical Distribution and Logistics Management*, *38*(7), 518–539.
97. Smith, R., & Shao, J. (2007). Privacy and e-commerce: A consumer-centric perspective. *Electronic Commerce Research*, *7*(2), 89–116.
98. Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2005). Managing the performance impact of Web security. *Electronic Commerce Research*, *5*(1), 99–116.
99. Su, X. (2009). Consumer returns policies and supply chain performance. *Manufacturing and Service Operations Management*, *11*(4), 595–612.
100. Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203–223.
101. VeriSign.com. (2011). Cpmpare SSL Certificates. http://www.verisign.com/ssl/buy-ssl-certificates/compare-ssl-certificates/index.html. Accessed 31 August 2011.
102. Vincent, O. R., Folorunso, O., & Akinde, A. D. (2010). Improving e-payment security using Elliptic Curve Cryptosystem. *Electronic Commerce Research*, *10*(1), 27–41.
103. Wakefield, R. L., Stocks, M. H., & Wilder, W. M. (2004). The role of Web site characteristics in initial trust formation. *Journal of Computer Information Systems*, *45*(1), 94–103.
104. Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing*, *18*(1), 53–69.

105. Weathers, D., Sharma, S., & Wood, S. L. (2007). Effects of online communication practices on consumer perceptions of performance uncertainty for search and experience goods. *Journal of Retailing*, *83*(4), 393–401.
106. Wu, G., Hu, X., & Wu, Y. (2010). Effects of perceived interactivity, perceived Web assurance and disposition to trust on initial online trust. *Journal of Computer-Mediated Communication*, *16*(1), 1–26.
107. Yang, Sh-Ch., Hung, W-Ch., Sung, K., & Farn, Ch-K. (2006). Investigating initial trust toward e-tailers from the elaboration likelihood model perspective. *Psychology and Marketing*, *23*(5), 429–445.
108. Yoon, S.-J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47–63.
109. Zhao, J. J., & Zhao, S. Y. (2004). Internet technologies used by INC. 500 corporate websites. *Issues in Information Systems*, *5*(1), 366–372.
110. Zhang, H. (2005). Trust-promoting seals in electronic markets: Impact on online shopping decisions. *Journal of Information Technology Theory and Application*, *6*(4), 29–40.

Farhod P. Karimov (PhD in Applied Economics, Vrije Universiteit Brussel) is a principal lecturer in Business discipline and a Deputy Rector on pre-university studies at Westminster International University in Tashkent (WIUT). He teaches in postgraduate and undergraduate programs in the areas of marketing and management. Most recently he was a Head of the Department of Contemporary Management at the Academy of State Governance under the President of the Republic of Uzbekistan. He also has industry experience in production, business consulting, and government sectors. Dr. Karimov's research interests are broadly in the domain of website atmospherics, web security, online trust, social-media in e-commerce and entrepreneurial marketing. He has published in a range of leading international journals including: Journal of Electronic Commerce Research; Management Research Review; International Journal of E-Entrepreneurship and Innovation; International Journal of E-Adoption; and Marketing Cahier. He has presented his findings at numerous international conferences.

Malaika Brengman (PhD in Applied Economics, University of Ghent), is Associate Professor at the Vrije Universiteit Brussel (VUB), where she teaches Marketing, Consumer Behaviour and Market Research. She started her academic career as Assistant Professor at Hasselt University, where she has also been lecturing in Marketing Communications, e-Business, Services Management and Customer Relationship Management. She has also been guest lecturing at other academic institutions, such as Solvay Business School at the Université Libre de Bruxelles and the International School of Management at the Leti-Lovanian University in St. Petersburg, Russia. Guided by her strong interests in Retailing, Marketing Communications and Consumer Behaviour, her scientific research generally focuses on the impact of store atmospherics and consumers' shopping motivations and behaviour, specifically also with regard to alternative distribution channels such as e-commerce and Virtual Worlds. She also studies marketing communications' effectiveness, especially with regard to new media. She has published her work in well-established journals, such as the 'Journal of Electronic Commerce Research', the 'Journal of Business Research', 'Psychology and Marketing', the 'Journal of Retailing and Consumer Services', 'Contemporary Management Research', the 'Journal of Marketing Communications', the 'Journal of Brand Management', the 'Journal of Product and Brand Management', the 'Journal of Customer Behaviour' and 'Advances in Consumer Research'. She has presented her findings at numerous international conferences.