Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis

Khadija Ali Vakeel, Saini Das, Godwin J. Udo & Kallol Bagchi

To cite this article: Khadija Ali Vakeel, Saini Das, Godwin J. Udo & Kallol Bagchi (2017) Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis, Behaviour & Information Technology, 36:4, 390-403, DOI: 10.1080/0144929X.2016.1236837

To link to this article: https://doi.org/10.1080/0144929X.2016.1236837

BEHAVIOUR & INFORMATION TECHNOLOGY, 2017
VOL. 36, NO. 4, 390–403
http://dx.doi.org/10.1080/0144929X.2016.1236837

Taylor & Francis
Taylor & Francis Group

Do security and privacy policies in B2B and B2C e-commerce differ? A comparative study using content analysis

Khadija Ali Vakeel[a], Saini Das[a], Godwin J. Udo[b] and Kallol Bagchi[b]

[a]Department of Information Systems, Indian Institute of Management Indore, Indore, India; [b]Department of Accounting & Information Systems, University of Texas at El Paso, El Paso, TX, USA

ABSTRACT

Security and privacy policies address consumer concerns related to security and privacy in e-commerce websites. As these policies represent only the vendor's perspective, often there exists a mismatch between the stated and desired policy. Based on transaction cost theory, we speculate that business-to-business (B2B) and business-to-consumer (B2C) e-commerce customers use their transaction cost savings in order to obtain varying levels of security and privacy. These differences are bound to be reflected in the security and privacy policies of e-commerce companies. Therefore, in this paper, we perform a comparative content analysis of the security and privacy policies in B2C and B2B e-commerce. Results show that B2B vendors are more concerned about security than their B2C counterparts, while B2C vendors are anxious about intimacy and restriction privacy. Our findings have important implications for e-commerce consumers and vendors as individual and corporate consumers have varying concerns while transacting online. Individual consumers are concerned about maintaining security and intimacy privacy, whereas corporate users are anxious about regulatory issues. Therefore, B2C vendors should incorporate stringent measures dedicated to confidentiality and protection of consumer data as well as enhance intimacy privacy in their security policies, while their B2B counterparts should focus on enhancing restriction privacy.

ARTICLE HISTORY
Received 12 March 2016
Accepted 12 September 2016

KEYWORDS
Security policy; privacy policy; content analysis; intimacy; restriction

1. Introduction

Over the years, a substantial bulk of trade has shifted from the traditional marketplace to the online space (Fearon, McLaughlin, and Jackson 2014). Due to the growth of electronic commerce (e-commerce) and the convenience associated with it, more and more customers are adopting e-commerce as a medium for transactions (Guo and Salvendy 2009; Hwang, Jung, and Salvendy 2006). However, this has also resulted in security and privacy issues. Pure-play e-commerce firms experience higher adverse market reactions in response to information security breaches compared to traditional brick-and-mortar firms (Bose and Leung 2013; Yayla and Hu 2011; Zwass 2003). Breaches involving theft of credit cards have seen a considerable rise from 3.8% in 2009 to 14.7% in 2013, whereas random brute force attacks have gone down considerably from 14.5% in 2009 to a meagre 3.7% in 2013. Around 54% of the attacks that took place in 2013 targeted e-commerce companies (Trustwave 2014). In a recent incident of fraud, the e-commerce mammoth Amazon suffered data loss in the form of customer username, passwords, and credit card information (Torossian 2015). In another incident, in early 2014, eBay suffered a data breach attack that compromised its primary database containing user passwords (Kelly 2014). The tour booking portal Viator suffered a massive data breach in 2014 when the payment card and personal information of approximately 1.4 million customers were compromised (Kovacs 2014). Similar is the landscape for privacy; big e-commerce companies are facing increasing number of cases related to the violation of consumer privacy (Sullivan 2015).

Exchange in an online environment takes place predominantly between either business-to-business (B2B) or business-to-consumer (B2C) segments. B2C transactions have gained popularity in the recent past due to online deals at high discounts. According to the 2014 Market Report, e-commerce in B2C market is increasing at a double-digit rate (Wu et al. 2012). But as the number of customers who share their personal and transactional data online increases, their concerns about security and privacy also increase (Zwass 2003). The B2B segment, on the other hand, is growing even faster, at approximately four times the rate of its B2C counterpart (Demery 2015). However, B2B e-commerce

CONTACT Khadija Ali Vakeel f13khadijav@iimidr.ac.in

is a less researched area and it significantly differs from B2C in transaction volume, average transaction amount, customer segments, logistics, fulfilment issues, and advertisement objectives (Chakraborty, Lala, and Warren 2003; Usunier, Roulin, and Ivens 2009). Other differences include the following: (1) B2C customers are concerned about personal financial data and privacy of personal information, while B2B customers want network security and corporate privacy (Guo and Salvendy 2009). (2) In B2C, transactions are discrete and small as compared to corporate deals in B2B (Hasan, Morris, and Probets 2012). (3) The impact of security and privacy breaches can be more harmful to businesses than to the individual consumers as B2B products and processes are more complex (Fearon, McLaughlin, and Jackson 2014). Finally, the legal norms for B2B and B2C e-commerce are different in many countries (Hesselink 2010). Moreover, based on transaction cost theory (TCT), we speculate that B2B and B2C e-commerce customers use the cost savings resulting from their online transactions in order to obtain different levels of security and privacy for themselves on the websites. Hence, these differences should reflect in the security and privacy policies of B2C and B2B e-commerce websites.

Despite these differences, it is observed that vendors of e-commerce follow similar security and privacy strategies in both B2B and B2C segments (Hong and Kim 2004; Hwang, Jung, and Salvendy 2006; Petre, Minocha, and Roberts 2006). They are often ignorant of the different customer requirements in the B2B and B2C spaces due to non-stringent legal norms, ease of management, blind consumer trust, and financial benefits. With fair information practices (FIPs), which are a global set of principles for fair balance of personal information collected online, a regulatory framework has come into existence, but this set of principles serve merely as guidelines (Schwaig, Kane, and Storey 2006). In several instances, it is observed that these policies represent only the vendor's perspective and there exists a mismatch between what is stated by the vendor and what is actually desired by the client (Wu et al. 2012). Hence, the incongruence between the client's security and privacy demand and vendor's services leads to dissatisfaction, which ultimately leads to loss of business as the customer would switch to other trustworthy e-commerce brands (McKnight and Chervany 2001; Yenisey, Ozok, and Salvendy 2005).

Moreover, the literature does not differentiate between varying requirements of B2B and B2C security and privacy policies. This study attempts to fulfil this gap by analysing the security and privacy policies of e-commerce companies belonging to B2B and B2C segments. In short, in this study, we perform a comparative analysis of privacy and security policies of B2C and B2B e-commerce websites from the vendor's perspective. We use the content analysis approach to arrive at security and privacy scores of security and privacy policies of B2C and B2B e-commerce websites. We also find the scores of privacy policies of B2B and B2C e-commerce websites on the eight categories of privacy stated by Gill et al. (2011). Finally, we apply regression analysis using ANOVA to find answers to our research questions. The results show that B2B vendors are more concerned about the security of data and processes on their websites than their B2C counterparts. On the other hand, privacy on the whole is equally important for both. However, B2C customers are more concerned about the intimacy and restriction aspects of privacy as compared to their B2B counterparts. The remaining aspects of privacy as described in this paper are considered equally important by both the B2B and B2C segments of e-commerce.

2. Related studies

2.1. TCT in e-commerce

TCT was developed by Williamson (1979) to be used to explain the economic activities in firms. TCT maintains that organisations like to conduct business transactions in the most economic ways since most organisations' goal is to maximise profit by minimising costs. The essence of TCT is that institutional structure matters and certain institutional structures affect governance better than others. Given the growth of e-commerce, it is generally believed that markets, as an institution, now play a significant role in economic activities because most firms are practising B2B and B2C e-commerce. Information systems researchers have used TCT to explain the popularity of e-commerce of all types. For example, Steinfield and Whitten (1999) use TCT to show how locally sensitive e-commerce websites can be developed at both the firm level (i.e. B2B) and the individual level (i.e. B2C) and used as competitive strategies. This study further confirms that savings from transaction costs can be enhanced by information technology (such as the Internet) within the entire industry (Benjamin and Wigand 1995; Singh 2008; Weber 2012).

Devaraj, Fan, and Kohli (2002) have used transaction cost analysis to explain consumers' behaviour in B2B e-commerce transactions and conclude that satisfaction in this channel can partly be explained with TCT. According to Dellaert et al. (1998), the consumer takes into account both the cost of the product/service and convenience or time constraints required of him/her. Since e-commerce makes shopping easy and less time

consuming by reducing information asymmetry and inaccuracy, it is expected that this channel will continue to be preferred by consumers. TCT is a suitable theory for explaining the attractiveness of e-commerce for both firms (B2B) and individuals (B2C) who buy or sell using this channel. As well documented in the literature, economic exchange has three phases, namely, pre-purchase (search and evaluation), purchase (ordering and delivery), and post-purchase (after sales services) phases (Kalakota and Whinston 1996; Steinfield and Whitten 1999). E-commerce supports each of these phases more efficiently and effectively than the traditional channels, thereby minimising transaction costs at each phase. Teo and Yu (2005) also used TCT to explain what factors motivate or discourage consumers from buying online, including experience with online transaction, uncertainty, and cost of transaction.

In the present study, we speculate that both business and individual (i.e. B2B and B2C) customers are attracted to the e-commerce market channel because of its ability to cut transaction costs, but that each group may be handling the savings differently. We believe that business customers may use the transaction cost savings in obtaining more system security for their transactions because systems security is more important to them than their business privacy. On the other hand, individual customers may be more willing to compromise some of their privacy for convenience and near perfect information they get from online shopping. For example, in a survey conducted in the year 2010, European citizens showed more leniencies in privacy concerns when doing online shopping (European Commission 2013). A large majority of Europeans think revealing personal data is a part of everyday life, but are also worried about how their online data are being used. This speculation influences the two research questions in the present study as discussed later.

2.2. Information security in e-commerce

Due to the phenomenal growth in e-commerce, security- and privacy-related research has received increased attention in the recent years. Security and privacy issues have kept many consumers away from shopping online (Nilashi et al. 2011; Udo 2001; Yenisey, Ozok, and Salvendy 2005). Awareness regarding online security has played a significant role in maximising the extent of participation from customers. Research has found that security and privacy issues in e-commerce affect trust and repeat purchase intention of consumers (Chiu et al. 2014; Sharma and Yetton 2003). For example, higher privacy dimensions are found to be significantly related to trust (Wu et al. 2012). High security and privacy will lower concerns for risk and fraud, which will lead to higher purchase intention (Miyazaki and Fernandez 2000).

Perceived information security refers to 'subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations' (Chellappa and Pavlou 2002, 359). The perceived level of information security is different from the objective level of information security. Information security is described as a multidimensional perspective conceptualised as comprising confidentiality, availability, integrity, and non-repudiation (Hartono et al. 2014). In this paper, security is described as, 'circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse' (Belanger, Hiller, and Smith 2002, 249). Researchers have developed frameworks to analyse the risk and security associated with e-commerce sites (Baird, Jamieson, and Cerpa 2002).

2.3. Privacy in e-commerce

Privacy refers to the rights of individuals and organisations to determine when, how, and to what extent information about them is transmitted to others (Grandinetti 1996; Martin 1973; Udo 2001). It is the ability to manage information about oneself (Belanger, Hiller, and Smith 2002). Privacy dictionary comprises eight different categories of privacy experiences, namely, NegativePrivacy, NormsRequisite, OutcomeState, PrivateSecret, Intimacy, Law, Restriction, and OpenVisible (Gill et al. 2011; Usunier, Roulin, and Ivens 2009). Definitions of the different categories of privacy are provided in Table 1 (Gill et al. 2011; Usunier, Roulin, and Ivens 2009).

Table 1. Definitions of different categories of privacy as adopted from Vasalou et al. (2011).

Construct	Definition
NegativePrivacy	It captures the antecedents and consequences of privacy violations
NormsRequisite	It encapsulates the norms, beliefs, and expectations in relation to achieving privacy
OutcomeState	It includes words that describe the static behavioural states and the outcomes that are served through privacy
PrivateSecret	It includes descriptors or words that express the 'content' of privacy
Intimacy	It comprises words that portray and measure different facets of small group privacy
Law	It includes words employed to describe legal definitions of privacy
Restriction	It expresses the closed, restrictive, and regulatory behaviours employed in maintaining privacy
OpenVisible	It includes words that represent the dialectic openness of privacy

2.4. Security and privacy in B2C and B2B e-commerce

Privacy and security are most important customer concerns while shopping online (Miyazaki and Fernandez 2000). Much of the research has focused on perceived security and privacy in the B2C context (Chellappa and Pavlou 2002; Hartono et al. 2014; Miyazaki and Fernandez 2001; Smith, Dinev, and Xu 2011; Toufaily, Souiden, and Ladhari 2013). B2C is defined as, 'marketing, buying, selling, delivering, servicing, paying for products, services, and information across (non-proprietary) networks linking an enterprise and its prospects including customers, agents, suppliers, competitors, allies, and complementors' (Jeyaraj et al. 2004, 2638). Previous researchers have analysed the antecedents and outcome of web security in the B2C consumer segment in e-commerce (Hartono et al. 2014). Increased security and privacy lead to trust in the online medium that increases adoption of e-commerce (Chellappa and Pavlou 2002; Furnell and Karweni 1999). It is observed that the studies related to security and privacy in B2C e-commerce have given little consideration to whether the same findings are applicable for B2B e-commerce as well (Chakraborty, Lala, and Warren 2003; Hande and Ghosh 2015; Liu et al. 2005). B2B e-commerce is 'the process of deploying information and communication technologies to support the entire value chain from suppliers through the firm to customers' (Thatcher, Foster, and Zhu 2006, 93). Customers of B2C e-commerce are more concerned with the ease and method of payment with active return policy, while B2B e-commerce customers are focused on bulk deliveries on-time (Hande and Ghosh 2015).

Table 2 shows the difference between B2B and B2C e-commerce from the consumer's and vendor's perspectives.

Security and privacy issues in the e-commerce space can be analysed from two different perspectives, namely, consumer and vendor perspectives. There are significant differences between the two (Belanger, Hiller, and Smith 2002). Most of the studies related to e-commerce focus on the consumer's perspective and tend to ignore the vendor's perspective. Very few studies focus on security and privacy in e-commerce from a vendor's perspective (Desai, Richards, and Desai 2003; Desai, Desai, and Phelps 2012; Yayla and Hu 2011). Policy statements are descriptions of how a company operates with respect to different factors, that is, privacy, security, shipping returns, and warranty (Desai, Desai, and Phelps 2012). Security and privacy policies represent the vendor's perspective related to these two issues of prime importance in e-commerce. As direct face-to-face communication is not possible in e-commerce, policies serve as the medium of connection between the consumers and vendors in the e-commerce space (Gefen, Karahanna, and Straub 2003). Security policies provide the set of laws, rules, and measures that regulate how an organisation manages and protects customer information (Desai, Desai, and Phelps 2012). Privacy policies comprise a set of statements explaining how consumers' data are dealt with and protected by the dealers (Desai, Desai, and Phelps 2012). Assessment of Fortune 500 corporations' policy statements showed that quite a few times they deviated from what they had written in the statements (Zwass 2003). For example, even though the policy statement of an organisation explicitly acknowledged the implementation of a secure socket layer and a closed port, in reality, upon examination both were found to be absent (Zwass 2003). Other important privacy policy concerns are legal issues, backdated and inadequate coverage of all customer-related categories such as return, shipping, warranty, and security (Desai, Richards, and Desai 2003; Desai, Desai, and Phelps 2012).

The above literature review indicates that (i) there is limited research on security and privacy in e-commerce considering the vendors' perspective; (ii) priority has been given to security and privacy issues in the B2C segment of e-commerce, while the same problems in the B2B segment have been ignored to a large extent; and (iii) no attempt has been made to identify the similarities and differences in privacy and security policies in B2C and B2B segments of e-commerce. This study attempts to fulfil these research gaps by examining security and privacy in e-commerce from the vendor's perspective for both B2C and B2B consumer segments Specifically, it is attempted to identify the differences in approach to security and privacy as reflected in the security and privacy policies of B2C and B2B e-commerce vendors and their implications on consumers of e-commerce companies belonging to the two segments. The next section elucidates the research questions taken up in this study.

Table 2. Difference between B2B and B2C e-commerce from the consumer's and vendor's perspectives.

S. No.	Parameter	B2C e-commerce	B2B e-commerce
1.	Consumer concern	Ease of payment, product replacement policy, security of transactions, and on-time delivery (Hande and Ghosh 2015)	Promotional schemes and bulk purchase options, product prices, and on-time delivery (Hande and Ghosh 2015)
2.	Vendor concern	Customer identification, unsolicited contact, and information sharing (Miyazaki and Fernandez 2000; Moulinos, Iliadis, and Tsoumas 2004)	Data privacy and market transparency; B2B technical infrastructure and support (Hempel and Kwong 2001)

3. Research questions

Security and privacy problems lead to major legal and ethical issues that are faced by e-commerce companies (Bloom, Milne, and Adler 1994; Miyazaki and Fernandez 2001). A web designer should incorporate authentic security and privacy policies to communicate the trustworthiness of his website as the trust often converts into repeat purchase (Belanger, Hiller, and Smith 2002; Chiu et al. 2014). There are many classifications of security break-ins in the computer science literature, based on the type of attack, place, and origin of an incident (Chellappa and Pavlou 2002). No one can guarantee foolproof security in an online space, but the risk can be mitigated by technological and managerial means (Mukhopadhyay et al. 2013; Schneier 1997). There are several studies dedicated to information security risk quantification, prevention, and mitigation in e-commerce (Baird, Jamieson, and Cerpa 2002; Das, Mukhopadhyay, and Anand 2012; Das, Mukhopadhyay, and Shukla 2013; Mukhopadhyay et al. 2013; Stoneburner, Goguen, and Feringa 2001). From these studies, it can be inferred that it is difficult to quantify information security risk (Anderson and Moore 2006; Rhee, Ryu, and Kim 2005; Ryan and Ryan 2006). Therefore, security risk prevention and mitigation are also difficult. Mechanisms of encryption, protection, authentication, and verification are some of the technological measures adopted by organisations to prevent cybercrimes (Chellappa and Pavlou 2002). However, these alone are not sufficient to prevent or mitigate information security risks (Das, Mukhopadhyay, and Shukla 2013). Along with the technological measures, security policies and procedures also play an important role. Privacy and security statements are the commitments provided by web merchants on data-sharing policies, security features, encryption, and password protection (Belanger, Hiller, and Smith 2002; Gefen, Karahanna, and Straub 2003). It is mandatory to update them regularly as they tend to degrade and become obsolete over time (Baird, Jamieson, and Cerpa 2002). Security seals, digital certificates, and third-party verifications have made the transactions over the Internet more reliable (Belanger, Hiller, and Smith 2002; Moulinos, Iliadis, and Tsoumas 2004). However, customers in the B2C and B2B segments analyse these features differently and also weigh them against risks and benefits in a different manner based on TCT, to take the decision to transact online (Desai, Desai, and Phelps 2012). Different factors vary in their degree of relevance for customers in B2B and B2C e-commerce as shown in Table 2 (Hande and Ghosh 2015). Promotional schemes and bulk purchase options, product prices, and on-time delivery are the most important factors for customers in B2B e-commerce platforms, while ease of payment, product replacement policy, security of transactions, and on-time delivery are the most important parameters affecting customers in B2C e-commerce (Hande and Ghosh 2015). Demographic factors, economic and financial resources, information structure, and industry structure impact B2B and B2C alike. But, organisational factors such as corporate culture, personal relationships, local competition, and entrepreneurial business culture impact B2B e-commerce more than its B2C counterpart (Kraemer, Gibbs, and Dedrick 2002). On the other hand, B2C e-commerce is influenced more by consumer attitude and preferences. B2C customers have reservations purchasing online; the same might not be the case with the B2B segment due to corporate relations (Kraemer, Gibbs, and Dedrick 2002). Hence, the specific factors that shape the consumer interest to transact online in B2B and B2C e-commerce are different (Kraemer, Gibbs, and Dedrick 2002). Therefore, the policies addressing the concerns of security should also vary for the e-commerce vendors in the two segments. To account for this difference, in our first research question, we try to analyse whether the perception of security is different for vendors in B2B and B2C e-commerce segments.

3.1. RQ1: Does the perception of security vary between vendors in B2B and B2C e-commerce segments?

Privacy and security are almost used interchangeably in the literature (Belanger, Hiller, and Smith 2002). The close relationship between the concepts of privacy and security exists at three different levels: the consumer level (there is a close relationship between the two concepts in the minds of consumers); the company level (companies tend to handle both concepts jointly); and the public level (the public, including government and legislation, views both ideas as closely related) (Flavián and Guinalíu 2006). However, in this paper, privacy is treated distinctly from security as obtained from prior research (Belanger, Hiller, and Smith 2002). Privacy is a cognitive process involving privacy risk and privacy control that affects privacy concerns of a consumer (Smith, Dinev, and Xu 2011). Privacy is the second most cited concern of online shoppers after system security concerns (Miyazaki and Fernandez 2001). Protection from fraud and privacy violation is hence one of the most important concerns of online retailers. B2C vendors are concerned about customer identification, unsolicited contact, and information sharing as shown in Table 2 (Miyazaki and Fernandez 2001). On the other hand, in B2B e-commerce, vendors are concerned

about data privacy and market transparency (Hempel and Kwong 2001). Similar to security policy, as vendors have different parameters to address in the context of privacy, policies addressing privacy concerns of consumers should also be different in B2B and B2C e-commerce. Therefore, in our second research question, we try to analyse whether the perception of privacy is different for vendors in B2B and B2C e-commerce segments.

3.2. RQ2: Does the perception of privacy vary between vendors in B2B and B2C e-commerce segments?

We further try to analyse whether the perception of the eight categories of privacy shown in Table 1 is different for vendors in B2B and B2C e-commerce segments. The research questions pertaining to the categories of privacy are listed in Table 3.

4. Methodology

A deductive, quantitative content analysis of 200 security policies of e-commerce websites was done to analyse how much security and privacy content was present within them (Lowe 2004). Content analysis has three major steps. First, preparing a dictionary that covers all the words related to the construct. Second, frequency count of the word that appears in the text being analysed, from the dictionary. Third, the normalisation of the frequency count by the total number of words appearing in the text. After normalisation, the score obtained by the construct shows us how much importance has been given to it in the text.

The process followed in our paper is described in detail below:

1) Preparing a dictionary: we used existing dictionaries for the constructs 'security' and 'privacy' to get their scores from the security and privacy policies, respectively (Gill et al. 2011; Usunier, Roulin, and Ivens 2009). For security dictionary, we used a comprehensive list of words that come under the construct 'security' taken from SANS Glossary of Security Terms (2000). For privacy dictionary, we used the content analysis dictionary for the construct 'privacy' created by Vasalou et al. (2011). A total of 513 and 616 words were present in the security and privacy dictionaries, respectively. There are eight sub-categories of privacy shown in Table 1 (Vasalou et al. 2011). The total number of words in the security, privacy, and privacy sub-categories dictionaries is shown in Table 4. Along with this, the important words in each dictionary are also shown.

2) Frequency count: we used DICTION software to calculate security and privacy scores in the respective policies for each e-commerce vendor (Hart and Carroll 2011; Short and Palmer 2007). The score calculation is based on the frequency of the words included in the security and privacy dictionary (Gill et al. 2011; Usunier, Roulin, and Ivens 2009). The DICTION software automatically generates a score for each document according to the dictionary.

3) Regression: we used the scores obtained from the DICTION software for each construct to apply regression analysis using ANOVA to test our research questions.

Table 3. Subparts to RQ2.

S. No.	Research questions
RQ2a	Does the perception of NegativePrivacy vary between vendors in B2B and B2C e-commerce segments?
RQ2b	Does the perception of NormsRequisite vary between vendors in B2B and B2C e-commerce segments?
RQ2c	Does the perception of OutcomeState vary between vendors in B2B and B2C e-commerce segments?
RQ2d	Does the perception of PrivateSecret vary between vendors in B2B and B2C e-commerce segments?
RQ2e	Does the perception of Intimacy vary between vendors in B2B and B2C e-commerce segments?
RQ2f	Does the perception of Law vary between vendors in B2B and B2C e-commerce segments?
RQ2g	Does the perception of Restriction vary between vendors in B2B and B2C e-commerce segments?
RQ2h	Does the perception of OpenVisible vary between vendors in B2B and B2C e-commerce segments?

Table 4. Details of security and privacy dictionaries.

Name of dictionaries	Important words in dictionary	Total words in dictionary
Security	Availability, backdoor, cache	513
Privacy	choices, sharing, database	616
NegativePrivacy	judgmental, troubled, interfere	120
NormsRequisite	consent, respect, discrete	33
OutcomeState	freedom, separation, alone	39
PrivateSecret	secret, intimate, data	22
Intimacy	trust, friendship, confide	22
Law	confidentiality, policy, offence	27
Restriction	conceal, lock, exclude	63
OpenVisible	post, display, accessible	46

4.1. Data

The data for this study were collected from 200 e-commerce websites. All the e-commerce vendors specify privacy policies and in some cases security policies on their website. In several scenarios, it is observed that the security policy is present as a separate subsection embedded within the privacy policy. The list of e-commerce companies was drawn from Thompson Reuters for the online services segment. E-commerce has evolved across different geographies. Therefore, as a

Table 5. Positioning of security and privacy policy links in e-commerce websites.

S. No.	Positioning strategies of security policies	Number of e-commerce companies			
		B2B		B2C	
		n	%	*n*	%
1.	No security and privacy policy link available on website	6	6.31	6	5.71
2.	Security policy embedded within privacy policy link	79	83.15	91	86.66
3.	Security and privacy policy links available separately	9	9.47	8	7.61
4.	Only security policy link available on website	1	1.05	0	0

representative sample, we take an optimum mix of countries from Asia Pacific and the USA. The distribution of e-commerce companies selected for our study based on their country of origin is shown in Figure 1(a). Out of the 200 e-commerce companies in our study, 95 belonged to the B2B and 105 to the B2C segment. The 200 companies were further subdivided into various categories depending on their product variety as shown in Figure 1(b).

For businesses that had both security and privacy policies, the two documents were clubbed into one before analysis. The policies taken from the websites were the latest policies available, few had updated them in the recent past, and others were as old as two years. Table 5 represents the number of e-commerce companies in the B2B and B2C segments of our sample set that adopt one of the four possible positioning strategies of the security policies on their website.

5. Results

For each e-commerce vendor in both the B2B and B2C segments, we calculated scores for security, privacy, and its sub-categories using DICTION. To check if there is a difference between the B2B and B2C segments, we applied regression analysis using ANOVA for security, privacy, as well as its sub-categories for the two segments, respectively, in SPSS 23.

Table 6. Descriptive statistics for security.

Descriptive statistics for security scores					
Security	*N*	Minimum	Maximum	Mean	Std. deviation
Overall	200	70.40	207.66	139.81	17.15
B2B	95	87.18	207.66	142.98	17.82
B2C	105	70.40	167.39	136.97	16.09

Table 7. Results of regression for security.

Coefficients					
	Unstandardised coefficients		Standardised coefficients		
Model	*B*	Std. error	Beta	*t*	Sig.
Security	–.335	.134	–.175	–2.498	.013

5.1. RQ1: Difference in the perception of security between vendors in B2B and B2C e-commerce segments

Descriptive statistics of the security scores of B2B and B2C e-commerce segments obtained from the DICTION software are shown in Table 6. Table 7 represents the results of the regression analysis to gauge the relative importance of security in the security policies of B2B as compared to B2C e-commerce vendors. Security scores between the B2B and B2C segments were significantly different at $p < .05$. In summary, B2B is significantly different from B2C with respect to security policy. The negative value of standardised coefficient ($b = –.335$, $p < .05$) shows that the security score in B2C is less than that in B2B. Therefore, vendors of B2B are

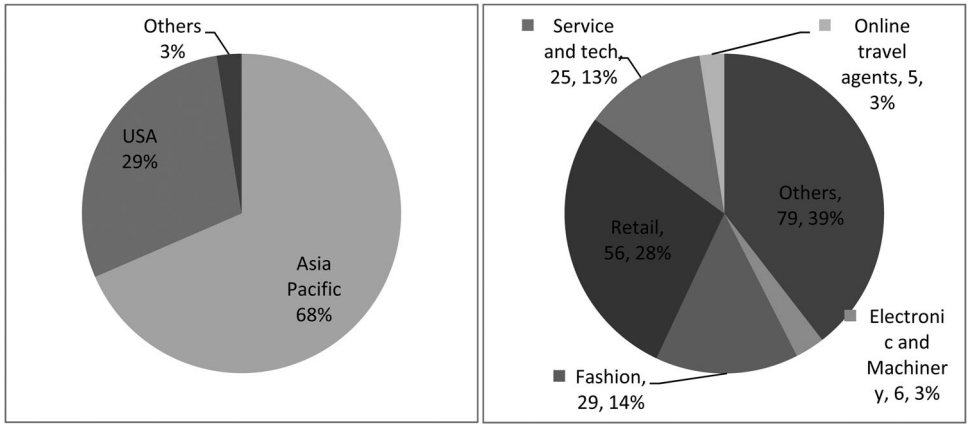

Figure 1. Distribution of e-commerce companies in this study: (a) country-wise and (b) product-wise.

Table 8. Descriptive statistics for scores of privacy and its subparts.

	N			Minimum			Maximum			Mean			Std. deviation		
	T	B2B	B2C	*T*	B2B	B2C	*T*	B2B	B2C	*T*	B2B	B2C	*T*	B2B	B2C
Privacy	200	95	105	105.4	110.3	105.4	284.3	284.3	250.2	209.8	207.7	211.7	20.6	22	19.2
NegativePrivacy	200	95	105	32.9	35.8	32.9	111.3	111.3	91.8	67.7	66.2	69.2	11.8	13	10.4
NormsRequisite	200	95	105	53.8	57	53.8	141.8	141.8	132.4	107.9	106.7	108.9	14.1	14.6	13.6
OutcomeState	200	95	105	0	0.1	0	26.4	26.4	18.1	4.4	4.1	4.6	3.3	3.4	3.2
PrivateSecret	200	95	105	25.3	25.3	30.3	96.8	96.8	81.6	53.6	54	53.3	10.2	10.7	9.7
Intimacy	200	95	105	46.5	46.5	48.4	120.9	117	120.9	87.9	85.9	89.7	12	12	11.7
Law	200	95	105	8.8	11.5	8.8	70.6	70.6	58.8	39.7	40.5	39	9.7	10.2	9.3
Restriction	200	95	105	67.6	73.8	67.6	173.4	171.9	173.4	135.8	133.2	138.1	16.9	16.9	16.6
OpenVisible	200	95	105	7.3	7.3	10.1	53.9	53.9	42	24.8	23.8	25.6	7.3	7.9	6.6

more concerned about security while designing the security policies of their e-commerce websites compared to their B2C counterparts.

5.2. RQ2: Difference in the perception of privacy between vendors in B2B and B2C e-commerce segments

Descriptive statistics of the scores of privacy and its sub-categories for B2B and B2C e-commerce segments are shown in Table 8.

Table 9 shows the results of the regression analysis to gauge the relative importance of privacy and its various subparts in the privacy policies of B2B as compared to B2C e-commerce websites. The difference in privacy scores between the B2B and B2C segments was insignificant at $p < .05$. Therefore, privacy is considered equally important by vendors in both the segments. Out of the eight sub-categories of privacy, the difference between B2B and B2C e-commerce segments is significant only for sub-categories Intimacy and Restriction. For the remaining sub-categories, the difference is insignificant. The positive value of the standardised coefficients for Intimacy ($b = .303$, $p < .05$) and Restriction ($b = .288$, $p < .05$) shows that the scores for both these sub-categories of privacy in B2C are more than those in B2B e-commerce.

Table 9. Results of regression for scores of privacy and its sub-categories.

	Coefficients				
	Unstandardised coefficients		Standardised coefficients		
Model	*B*	Std. error	Beta	*t*	Sig.
Privacy	.188	.139	.096	1.35	.177
NegativePrivacy	.239	.131	.128	1.81	.071
NormsRequisite	.156	.141	.079	1.11	.270
OutcomeState	.131	.144	.065	0.91	.363
PrivateSecret	−.064	.135	−.034	−0.47	.638
Intimacy	.303	.134	.160	2.27	.024
Law	−.149	.140	−.075	−1.06	.290
Restriction	.288	.140	.145	2.06	.041
OpenVisible	.215	.122	.124	1.76	.080

6. Discussion

The summary of results of the various research questions is provided in Table 10.

The result of RQ1 reveals that the perception of security is different for vendors in the B2B and B2C e-commerce segments as reflected in their respective security policies. B2B e-commerce vendors are more concerned about security than their B2C counterparts. This finding reveals that there exists a mismatch between individual customers' expectations from B2C e-commerce vendors with respect to security and what the vendors deliver (Hande and Ghosh 2015). Table 5 reveals that 9.5% of B2B e-commerce companies in our sample set displayed both security and privacy policy links separately on their websites, whereas only 7.6% of B2C e-commerce companies in our sample set did the same. This reinforces the fact that B2B e-commerce vendors are more concerned about having a separate link dedicated to security on their website as compared to B2C vendors. Individual consumers are extremely concerned about the security and safety of their data while transacting online and there exists a significant negative relationship between security concerns and consumer's willingness to

Table 10. Summary of results.

S. No.	Research questions	Results
RQ1	Does the perception of security vary between vendors in B2B and B2C e-commerce segments?	Yes; B2B>B2C
RQ2	Does the perception of privacy vary between vendors in B2B and B2C e-commerce segments?	No
RQ2a	Does the perception of NegativePrivacy vary between vendors in B2B and B2C e-commerce segments?	No
RQ2b	Does the perception of NormsRequisite vary between vendors in B2B and B2C e-commerce segments?	No
RQ2c	Does the perception of OutcomeState vary between vendors in B2B and B2C e-commerce segments?	No
RQ2d	Does the perception of PrivateSecret vary between vendors in B2B and B2C e-commerce segments?	No
RQ2e	Does the perception of Intimacy vary between vendors in B2B and B2C e-commerce segments?	Yes; B2C>B2B
RQ2f	Does the perception of Law vary between vendors in B2B and B2C e-commerce segments?	No
RQ2g	Does the perception of Restriction vary between vendors in B2B and B2C e-commerce segments?	Yes; B2C>B2B
RQ2h	Does the perception of OpenVisible vary between vendors in B2B and B2C e-commerce segments?	No

purchase online (Miyazaki and Fernandez 2001). Individual consumers would prefer to see a dedicated security policy posted on the company's website that reveals the measures taken by the company to ensure security and protection of their sensitive information. For example, consumers prefer to see details such as how their sensitive information such as credit card number is handled, what type of encryption is used during storage and transmission, whether the company adheres to any international information security management standard such as ISO/IEC 27001, and what are the additional measures implemented by the company to safeguard their data from damage and theft. The study reveals that in many instances, the security policy is either absent altogether or embedded as an inconspicuous subsection within the privacy policy. This makes it almost impossible for a normal shopper to read it. Previous studies have shown that by discouraging shoppers from reading policies, companies often lose the opportunity to alleviate security concerns and build trust (Pollach 2007). This finding also serves as an immediate warning to B2C e-commerce vendors to improve the location of the security policies on their websites and to incorporate stringent measures dedicated to confidentiality, integrity, availability, non-repudiation, and protection of consumer data within them. Table 11 shows a list of the most frequently occurring words in the combined (privacy and security) policies of B2B and B2C e-commerce websites versus lists of the most frequently occurring words obtained from the security and privacy dictionaries which are also present in the combined policies. The comparison shows that there is hardly any commonality between the most frequent words that actually appear in the combined policies of B2C e-commerce websites and the most frequent words obtained from the security dictionary that are also present in the combined policies. On the other hand, there is some degree of commonality between the most frequent words (example, 'cookies') that actually appear in the combined policies of B2B e-commerce websites and the most frequent words obtained from the security dictionary that are also present in the combined policies. Therefore, while designing the security and privacy policies of e-commerce websites, emphasis should be given to words that are ranked high in the security and privacy dictionaries and also present in the combined policies as these refer to the words that the users prefer to see in the policies.

Table 11. Frequently occurring words in combined polices, security and privacy dictionary.

Frequently occurring words	B2B	B2C
Combined (privacy + security) policies	Information, personal, service, privacy, cookies, data, access, users, email, contact	Information, personal, service, party, collect, data, email, address
Security dictionary	Browser, IP, Internet, Share, User, event, cookie	Browser, cookie, Internet, share, user,
Privacy dictionary	Personal, policy, privacy, data, disclose, consent, choose, protect, collected, security, law	Personal, privacy, policy, data, access, content, collected

The result of RQ2 reveals that both B2C and B2B vendors perceive privacy as equally important. This finding is in line with previous research (Belanger, Hiller, and Smith 2002; Miyazaki and Fernandez 2000). The relationship between privacy concerns and the desire to buy online is insignificant (Dai, Forsythe, and Kwon 2014; Islam and Daud 2011; Miyazaki and Fernandez 2000). Customers are less aware of privacy seals and cookies than about encryption. It is also possible that users understand security better than privacy because security is a more concrete concept (Belanger, Hiller, and Smith 2002).

Results of the subparts of RQ2 reveal that out of all the categories of privacy, there is a significant difference between B2B and B2C e-commerce vendors with respect to only two categories, namely, Restriction and Intimacy. B2C vendors are more concerned about Restriction and Intimacy in their privacy policies compared to their B2B counterparts. Prior studies reveal that in general online privacy policies simply adhere to FIP principles and are concerned about protecting organisations from litigations and potential lawsuits, instead of protecting user interests (Earp et al. 2005; Pollach 2007). For other categories, there is no significant difference between the privacy policies of B2B and B2C e-commerce websites. This finding again reveals that there exists a mismatch between individual customer's expectations from B2C e-commerce vendors with respect to privacy and what the vendors deliver (Hande and Ghosh 2015). Individual consumers are more concerned about Intimacy and PrivateSecret categories of privacy in the privacy policies of websites rather than restriction, law, and regulation. They would prefer to see words such as 'personal', 'access', and 'collect' (obtained from the privacy dictionary) in the privacy policies in order to demonstrate a higher concern for user Intimacy while interacting with their website. Table 11 shows that there exists a certain degree of commonality between the words (such as, 'personal' and 'data') that have higher frequency in the existing combined policies and the words that the users would prefer to see in the privacy policies (obtained from the privacy dictionary) in order to demonstrate a higher concern for user privacy while interacting with their website. On the other hand, corporate users of B2B websites prefer to see words (such

Table 12. Count of words from the privacy sub-categories dictionary per 500 words in a privacy policy.

Privacy category	B2B	B2C
NegativePrivacy	66.86167	69.24936
NormsRequisite	107.1032	108.8499
OutcomeState	4.106563	4.472182
PrivateSecret	54.15198	53.33718
Intimacy	86.48448	89.668
Law	40.4075	38.96245
Restriction	133.7992	138.0514
OpenVisible	24.59167	25.57345

as 'laws' and 'disclose') which have a legal or regulatory dimension to them. Therefore, the vendors of B2B websites should try to increase the frequency of such terms in their privacy policies in order to enhance the trust and confidence of corporate users.

Table 12 shows the count of words from the privacy sub-categories dictionary per 500 words in a privacy policy. It is observed that both B2B and B2C websites give least priority to OutcomeState (4.1 and 4.4) and maximum importance to Restriction (133.79 and 138.05) in their privacy policies. In case of B2C companies, more importance should be given to Intimacy and PrivateSecret aspects of privacy in the privacy policies. At the same time, there should also be reduction in the importance of the restriction aspect of privacy. Therefore, the privacy policies should avoid expressing the closed, restrictive, and regulatory behaviours employed in maintaining privacy (Vasalou et al. 2011).

6.1. Managerial implications

Individual and corporate consumers have varying levels of concern related to security and privacy while transacting online. Individual consumers are more concerned about maintaining security and intimacy privacy, whereas corporate users are anxious about regulatory issues and legal violations. Therefore, the implications of this study for founders and managers of B2B and B2C e-commerce websites are threefold. First, as shown by RQ1, B2B vendors are more concerned about security compared to their B2C counterparts as they deal with corporate data and bulk online orders. But this should not deter B2C vendors from actively addressing security concerns in their websites. Individual consumers are extremely concerned about the confidentiality, integrity, and availability of their personal data in the online space. They expect their personal information to be secure while transacting online. Therefore, managers of B2C e-commerce companies should implement more stringent security policies in their websites as individual customers in the B2C segment are becoming increasingly conscious of online threats. It is important for B2C e-commerce websites to alleviate their concerns about security issues in order to generate trust and loyalty. Second, higher Intimacy in B2C e-commerce websites is justified as individual consumers are more concerned about Intimacy privacy in the online environment. They expect the privacy policies to demonstrate a higher concern for user Intimacy while interacting with a website. Therefore, managers should focus on the Intimacy aspects of privacy in the privacy policies of their websites. Third, B2C e-commerce websites are more concerned about the Restriction and Law aspects of privacy than their B2B counterparts. However, corporate users of B2B websites are more concerned about Restriction and Law compared to B2C users while transacting online. Therefore, the vendors of B2B websites should try to increase the frequency of such terms in their privacy policies in order to enhance the trust and confidence of corporate users.

6.2. Research implications

This study contributes to the body of literature on the security and privacy aspects of e-commerce in three distinct ways. First, this research, to the best of our knowledge, is one of the first studies that quantitatively establish the differences between the B2C and B2B e-commerce vendors with respect to security and privacy. While previous studies have surveyed consumers to establish the differences in security and privacy policies between B2B and B2C e-commerce websites, we attempted to take a step forward by using content analysis of security and privacy policies of these two segments of e-commerce to quantitatively establish the differences existing between them. Second, this paper uses TCT to explain the differences in consumer attitude to security and privacy in B2C and B2B e-commerce. Based on the differences in individual and corporate consumers' attitudes and interests related to security and privacy in e-commerce, this paper also proposes how these policies in the respective e-commerce segments should differ. Third, this is one of the few papers that advanced research related to the eight sub-categories of privacy proposed by Vasalou et al. (2011).

6.3. Limitations and future work

Our study attempted to establish the differences in security and privacy policies between B2B and B2C e-commerce websites in general. However, the differences are expected to be more prominent in a category-wise study. For example, the B2C websites in the healthcare e-commerce category may be more concerned about consumer privacy compared to their B2B counterparts

as they deal with patients' confidential health information. Moreover, within the B2C segment, there may be a significant difference between websites based on product variety. For example, B2C healthcare e-commerce companies may also be more concerned about user privacy compared to B2C retail e-commerce companies. This aspect is not taken into consideration in this study due to the lack of data in a particular category of e-commerce and can be taken up as future work. Currently, our research uses secondary information available on the e-commerce vendors' website. Primary data including interviews of vendors would help us in arriving at more conclusive results. This also provides scope for future work in this direction.

7. Conclusion

The huge surge in the number of security breaches and privacy violations in the e-commerce space suggests that security and privacy are the two most important concerns in e-commerce today. As direct face-to-face communication is not possible between vendors and customers in e-commerce, security and privacy policies serve as the bridge between the two parties and represent the vendor's perspective on these two issues of prime importance. Vendors publish their security and privacy policies online to communicate measures that they adopt against such threats. It is observed that these policies represent only the vendor's perspective and in many instances, there exists a mismatch between the policy stated by the vendor and the one desired by the consumer. Moreover, based on TCT we speculate that in B2B and B2C segments, customers use their transaction cost savings resulting from e-commerce to obtain varying levels of security and privacy for themselves on the websites. Therefore, these differences should be reflected in the security and privacy policies of the websites.

In this paper, we performed a comparative analysis of the security and privacy policies in B2C vis-à-vis B2B e-commerce to identify the differences in the vendors' perspective in these two segments. We used deductive content analysis to compare security and privacy policies of e-commerce vendors in the B2C and B2B segments. We further made an attempt to find the relative importance of the sub-categories of privacy in the two segments of e-commerce. Our results show that B2B vendors are more concerned about security than their B2C counterparts, but privacy is considered equally important by both. Only two of the eight sub-categories of privacy, namely, Restriction and Intimacy, are different in B2B and B2C e-commerce. Hence, we identify that there exists a mismatch between individual customers' expectations from B2C e-commerce vendors with respect to security and what the vendors actually deliver. This finding also serves as an immediate warning to B2C e-commerce vendors to incorporate stringent measures in their security policy dedicated to the security and protection of consumer data. Our results also demonstrate that B2C e-commerce vendors should focus on aspects of Intimacy in their privacy statements because they cater to individual customers who are more concerned about Intimacy and private or secret aspects of privacy compared to corporate customers. On the other hand, B2B e-commerce vendors should be more concerned about restriction and legal aspects, in order to enhance the trust of corporate customers.

Disclosure statement

No potential conflict of interest was report by the authors.

References

Anderson, R., and T. Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–613.

Baird, A., R. Jamieson, and N. Cerpa. 2002. "Development of a Framework for Risks and Security in B2C e-Business." In *Towards the Knowledge Society: eCommerce, eBusiness and eGovernment*, edited by J. L. Monteiro, P. M. C. Swatman, and L. V. Tavares, 399–413. Boston: Kluwer Academic Publishers.

Belanger, F., J. S. Hiller, and W. J. Smith. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security and Site Attributes." *The Journal of Strategic Information Systems* 11 (3): 245–270.

Benjamin, R., and R. Wigand. 1995. "Electronic Markets and Virtual Value Chains on the Information Superhighway." *Sloan Management Review* 36 (2): 62–72.

Bloom, P. N., G. R. Milne, and R. Adler. 1994. "Avoiding Misuse of New Information Technologies: Legal and Societal Considerations." *The Journal of Marketing* 58 (1): 98–110.

Bose, I., and A. C. M. Leung. 2013. "The Impact of Adoption of Identity Theft Counter Measures on Firm Value." *Decision Support Systems* 55 (3): 753–763.

Chakraborty, G., V. Lala, and D. Warren. 2003. "What Do Customers Consider Important in B2B Websites?" *Journal of Advertising Research* 43 (1): 50–61.

Chellappa, R. K., and P. A. Pavlou. 2002. "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions." *Logistics Information Management* 15 (5/6): 358–368.

Chiu, C. M., E. T. Wang, Y. H. Fang, and H. Y. Huang. 2014. "Understanding Customers' Repeat Purchase Intentions in B2C e-Commerce: The Roles of Utilitarian Value, Hedonic Value and Perceived Risk." *Information Systems Journal* 24 (1): 85–114.

Dai, B., S. Forsythe, and W. S. Kwon. 2014. "The Impact of Online Shopping Experience on Risk Perceptions and Online Purchase Intentions: Does Product Category Matter?" *Journal of Electronic Commerce Research* 15 (1): 13–24.

Das, S., A. Mukhopadhyay, and M. Anand. 2012. "Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics." *Journal of Information Privacy and Security* 8 (4): 27–55.

Das, S., A. Mukhopadhyay, and G. K. Shukla. 2013. "i-HOPE Framework for Predicting Cyber Breaches: A Logit Approach." In *Proceedings of 46th Hawaii International Conference on System Sciences (HICSS): IEEE*, Hawaii, USA, 3008–3017.

Dellaert, B. G. C., T. A. Arentze, M. Bierlaire, A. W. J. Borgers, and H. J. P. Timmermans. 1998. "Investigating Consumers' Tendency to Combine Multiple Shopping Purposes and Destinations." *Journal of Marketing Research* 35 (2): 177–188.

Demery, P. 2015. *Internet Retailer*. Accessed October 11. http://www.internetretailer.com/2014/10/27/first-its-kind-look-b2b-e-commerce.

Desai, M. S., K. J. Desai, and L. D. Phelps. 2012. "E-commerce Policies and Customer Privacy: A Longitudinal Study (2000–2010)." *Information Management and Computer Security* 20 (3): 222–244.

Desai, M. S., T. C. Richards, and K. J. Desai. 2003. "E-commerce Policies and Customer Privacy." *Information Management and Computer Security* 11 (1): 19–27.

Devaraj, S., M. Fan, and R. Kohli. 2002. "Antecedents of B2C Channel Satisfaction and Preference: Validating E-commerce Metrics." *Information System Research* 13 (3): 316–333.

Earp, J. B., A. Anton, L. Aiman-Smith, and W. H. Stufflebeam. 2005. "Examining Internet Privacy Policies Within the Context of User Privacy Values." *IEEE Transactions on Engineering Management* 52 (2): 227–237.

European Commission. 2013. "Eurobarometer 74.3: The European Parliament, Energy Supply, Data Protection and Electronic Identity, Chemical Labeling and Rare Diseases." MI: Inter-university Consortium for Political and Social Research (ICPSR34264-v3) [distributors], Cologne, Germany: GESIS/Ann Arbor. http://doi.org/10.3886/ICPSR34264.v3.

Fearon, C., H. McLaughlin, and S. Jackson. 2014. "Measuring and Evaluating IS Expectations and Benefit Success from B2B Electronic Trading: A New Survey Approach." *Behaviour & Information Technology* 33 (4): 308–317.

Flavián, C., and M. Guinalíu. 2006. "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site." *Industrial Management and Data Systems* 106 (5): 601–620.

Furnell, S. M., and T. Karweni. 1999. "Security Implications of Electronic Commerce: A Survey of Consumers and Businesses." *Internet Research* 9 (5): 372–382.

Gefen, D., E. Karahanna, and D. W. Straub. 2003. "Trust and TAM in Online Shopping: An Integrated Model." *Management Information Systems Quarterly* 27 (1): 51–90.

Gill, A. J., A. Vasalou, C. Papoutsi, and A. N. Joinson. 2011. "Privacy Dictionary: A Linguistic Taxonomy of Privacy for Content Analysis." In *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, 3227–3236. ACM.

Glossary of Security Terms. 2000. *SANS Glossary*. Accessed October 11, 2015. www.sans.org/security-resources/glossary-of-terms/.

Grandinetti, M. 1996. "Establishing and Maintaining Security on the Internet." *Sacramento Business Journal* 13 (25): 22–35.

Guo, Y., and G. Salvendy. 2009. "Factor Structure of Content Preparation for e-Business Web Sites: Results of a Survey of 428 Industrial Employees in the People's Republic of China." *Behaviour & Information Technology* 28 (1): 73–86.

Hande, P. V., and D. Ghosh. 2015. "A Comparative Study on Factors Shaping Buying Behaviour on B2B and B2C e-Commerce Platforms in India." *Excel International Journal of Multidisciplinary Management Studies* 5 (3): 1–10.

Hart, R. P., and C. Carroll. 2011. *DICTION: The Text-Analysis Program*. Thousand Oaks, CA: Sage.

Hartono, E., C. W. Holsapple, K. Y. Kim, K. S. Na, and J. T. Simpson. 2014. "Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Re-specification and Validation." *Decision Support Systems* 62 (2014): 11–21.

Hasan, L., A. Morris, and S. A. Probets. 2012. "Comparison of Usability Evaluation Methods for Evaluating e-Commerce Websites." *Behaviour & Information Technology* 31 (7): 707–737.

Hempel, P. S., and Y. K. Kwong. 2001. "B2B e-Commerce in Emerging Economies: i-metal.com's Non-ferrous Metals Exchange in China." *The Journal of Strategic Information Systems* 10 (4): 335–355.

Hesselink, M. W. 2010. "Towards a Sharp Distinction Between B2B and B2C? On Consumer, Commercial and General Contract Law after the Consumer Rights Directive." *European Review of Private Law* 18 (18): 57–102.

Hong, S., and J. Kim. 2004. "Architectural Criteria for Website Evaluation – Conceptual Framework and Empirical Validation." *Behaviour & Information Technology* 23 (5): 337–357.

Hwang, W., H. S. Jung, and G. Salvendy. 2006. "Internationalisation of e-Commerce: A Comparison of Online Shopping Preferences among Korean, Turkish and US Populations." *Behaviour & Information Technology* 25 (1): 3–18.

Islam, M. A., and K. A. K. Daud. 2011. "Factors that Influence Customers' Buying Intention on Shopping Online." *International Journal of Marketing Studies* 3 (1): 128–139.

Jeyaraj, A., D. Balser, C. Chowa, and G. Griggs. 2004. "Institutional Factors Influencing e-Business Adoption." In *Proceedings of Americas Conference on Information Systems (AMCIS)*, New York, USA, 2638–2642.

Kalakota, R., and A. B. Whinston. 1996. *Frontiers of Electronic Commerce*. Reading, MA: Addison Wesley Longman.

Kelly, G. 2014. "eBay Suffers Massive Security Breach, All Users Must Change Their Passwords." *Forbes*. Accessed October 11, 2015. http://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/.

Kovacs, E. 2014. "TripAdvisor's Viator Suffers Payment Card Data Breach, 1.4 Million Affected." *SecurityWeek*. Accessed October 11, 2015. http://www.securityweek.com/tripadvisors-viator-suffers-payment-card-data-breach-14-million-affected.

Kraemer, K., J. Gibbs, and J. Dedrick. 2002. "Environment and Policy Factors Shaping e-Commerce Diffusion: A Cross-country Comparison." In *Proceedings of International*

Conference on Information Systems (ICIS), Barcelona, Spain, 30, 325–335.

Liu, C., J. T. Marchewka, J. Lu, and C. S. Yu. 2005. "Beyond Concern – A Privacy-Trust-Behavioral Intention Model of Electronic Commerce." *Information and Management* 42 (2): 289–304.

Lowe, W. 2004. "Content Analysis and Its Place in the Methodological Scheme of Things." *Qualitative Methods: Newsletter of the American Political Science Association Organized Section on Qualitative Methods* 2 (1): 25–27.

Martin, J. 1973. *Security, Accuracy and Privacy in Computer Systems*. Vol. 71. Prentice-Hall, NJ: Englewood Cliffs.

McKnight, D. H., and N. L. Chervany. 2001. "What Trust Means in e-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology." *International Journal of Electronic Commerce* 6 (2): 35–59.

Miyazaki, A. D., and A. Fernandez. 2000. "Internet Privacy and Security: An Examination of Online Retailer Disclosures." *Journal of Public Policy and Marketing* 19 (1): 54–61.

Miyazaki, A. D., and A. Fernandez. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping." *Journal of Consumer Affairs* 35 (1): 27–44.

Moulinos, K., J. Iliadis, and V. Tsoumas. 2004. "Towards Secure Sealing of Privacy Policies." *Information Management and Computer Security* 12 (4): 350–361.

Mukhopadhyay, A., S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan. 2013. "Cyber-risk Decision Models: To Insure IT or Not?" *Decision Support Systems* 56 (2013): 11–26.

Nilashi, M., K. Bagherifard, O. Ibrahim, N. Janahmadi, and M. Barisami. 2011. "An Application Expert System for Evaluating Effective Factors on Trust in B2C Websites Trust, Security, ANFIS, Fuzzy Logic, Rule Based Systems, Electronic Commerce." *Engineering* 3 (11): 1063–1071.

Petre, M., S. Minocha, and D. Roberts. 2006. "Usability Beyond the Website: An Empirically-Grounded e-Commerce Evaluation Instrument for the Total Customer Experience." *Behaviour & Information Technology* 25 (2): 189–203.

Pollach, I. 2007. "What's Wrong with Online Privacy Policies?" *Communications of the ACM* 50 (9): 103–108.

Rhee, H. S., Y. Ryu, and C. T. Kim. 2005. "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security." In *Proceedings of International Conference on Information Systems (ICIS)*, Las Vegas, Nevada, USA, 31, 381–394.

Ryan, J. J., and D. J. Ryan. 2006. "Expected Benefits of Information Security Investments." *Computers & Security* 25 (8): 579–588.

Schneier, B. 1997. "Why Cryptography Is Harder than It Looks." *Information Security Bulletin* 2 (2): 31–36.

Schwaig, K. S., G. C. Kane, and V. C. Storey. 2006. "Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures?" *Information & Management* 43 (7): 805–820.

Sharma, R., and P. Yetton. 2003. "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation." *Management Information Systems Quarterly* 27 (4): 533–556.

Short, J. C., and T. B. Palmer. 2007. "The Application of DICTION to Content Analysis Research in Strategic Management." *Organizational Research Methods* 11 (4): 727–757.

Singh, N. 2008. "Transaction Costs, Information Technology and Development." *Indian Growth and Development Review* 1 (2): 212–236.

Smith, H. J., T. Dinev, and H. Xu. 2011. "Information Privacy Research: An Interdisciplinary Review." *Management Information Systems Quarterly* 35 (4): 989–1016.

Steinfield, C., and P. Whitten. 1999. "Community Level Socio-economic Impacts of Electronic Commerce." *Journal of Computer-Mediated Communication* 5 (2). http://www.ascusc.org/jcmc/.

Stoneburner, G., A. Y. Goguen, and A. Feringa. 2001. "Risk Management Guide for Information Technology Systems." In Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, NIST Special Publication, October, 800–830.

Sullivan, B. 2015. "Online Privacy Fears Are Real." *NBC News*. Accessed October 11. http://www.nbcnews.com/id/3078835/t/online-privacy-fears-are-real/#.VQUqcNKUciE.

Teo, S. H., and Y. Yu. 2005. "Online Buying Behavior: A Transaction Cost Economics Perspective." *Omega* 33 (5): 451–465.

Thatcher, S. M., W. Foster, and L. Zhu. 2006. "B2B e-Commerce Adoption Decisions in Taiwan: The Interaction of Cultural and Other Institutional Factors." *Electronic Commerce Research and Applications* 5 (2): 92–104.

Torossian, R. 2015. "Amazon Data Breach and the Public Relations Crisis That Follows." *Businesss2Community*. Accessed March 10. http://www.business2community.com/crisis-management/amazon-data-breach-public-relations-crisis-follows-01110994.

Toufaily, E., N. Souiden, and R. Ladhari. 2013. "Consumer Trust Toward Retail Websites: Comparison Between Pure Click and Click-and-Brick Retailers." *Journal of Retailing and Consumer Services* 20 (6): 538–548.

Trustwave Global Security Report. 2014. *Trustwave Solutions*. Accessed October 11, 2015. http://www.trustwave.com/Resources/Library/Documents/2014-Trustwave-Global-Security-Report/.

Udo, G. J. 2001. "Privacy and Security Concerns as Major Barriers for e-Commerce: A Survey Study." *Information Management and Computer Security* 9 (4): 165–174.

Usunier, J. C., N. Roulin, and B. S. Ivens. 2009. "Cultural, National, and Industry-Level Differences in B2B Web Site Design and Content." *International Journal of Electronic Commerce* 14 (2): 41–88.

Vasalou, A., A. J. Gill, F. Mazanderani, C. Papoutsi, and A. Joinson. 2011. "Privacy Dictionary: A New Resource for the Automated Content Analysis of Privacy." *Journal of the American Society for Information Science and Technology* 62 (11): 2095–2105.

Weber, S. 2012. *Information Technology in Supplier Networks: A Theoretical Approach to Decisions about Information Technology and Supplier Relationships*. Frankfurt: Springer Science & Business Media.

Williamson, O. E. 1979. "Transaction-cost Economics: The Governance of Contractual Relations." *Journal of Law and Economics* 22 (2): 233–261.

Wu, K. W., S. Y. Huang, D. C. Yen, and I. Popova. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust." *Computers in Human Behavior* 28 (3): 889–897.

Yayla, A. A., and Q. Hu. 2011. "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors." *Journal of Information Technology* 26 (1): 60–77.

Yenisey, M. M., A. A. Ozok, and G. Salvendy. 2005. "Perceived Security Determinants in e-Commerce among Turkish University Students." *Behaviour & Information Technology* 24 (4): 259–274.

Zwass, V. 2003. "Electronic Commerce and Organizational Innovation: Aspects and Opportunities." *International Journal of Electronic Commerce* 7 (3): 7–37.