Privacy-deprived E-commerce: The Efficacy of Consumer Privacy Policies on China's E-Commerce Websites from a Legal Perspective

Abstract

Purpose: Despite grave public concerns over information privacy and ongoing academic explorations of privacy policy, there is a general lack of understanding towards this issue in the legal context in China, the largest e-commerce market in the world. Departing from the extant literature of general discussion in nature, we undertook an exploratory study on the efficacy of e-commerce websites' privacy policies in China from the legal perspective.

Design/methodology/approach: We drew on a qualitative grounded theory approach to identify selective codes relating to the focal issue, and established a theoretical framework therefrom. We then conducted theoretical integration by linking them to the Theory of Development Blocks and the System Justification Theory.

Findings: The research identifies a general distrust of Chinese consumers towards privacy policies, and highlights that despite their growing concerns about privacy, the privacy policies are largely ineffective in reflecting legal enforcement, changing their perceptions, or influencing purchase behaviors. It also reveals that the current Chinese legislation is unable to fully render consumers' confidence in e-commerce websites' privacy policies effectiveness and privacy protection due to its limited recognition and influences among them.

Originality/value: The research has multiple ramifications. We empirically confirmed a mismatch between customers' perception of privacy policies and their actual behaviors, and then theoretically explained the seemingly conflicting scenario in the context of development block of legal enforcement and system justification. We theorized the absence of the legal enforcement in privacy policies to supplement the legal perspective to the literature. The research further leads us to suggest that the time has come to update and strongly enforce privacy regulation in China to fuel the further development of e-commerce sector in practice.

Keywords: privacy, privacy policy, e-commerce, Chinese law, China

INTRODUCTION

The exponential rise in information and communication technology[1] in the last decade has changed the way we live, including the mode in which we do our day-to-day shopping. Business-to-Consumer (B2C) e-commerce (e-commerce hereinafter) has become an integral part of our lives. However, studies have highlighted growing information privacy concerns amongst individuals as one of the main reasons for their reluctance to engage in B2C e-commerce transactions (e.g. Ghayoumi, 2016; Kim & Kim, 2017; Anic et al., 2019). Online vendors have adopted various methods to alleviate consumers' information privacy concerns, one of the most popular being to publish a privacy policy on their website (Bansal et al., 2015). The policy explains to online shoppers that their data will be treated in a fair, transparent and responsible manner (Wu et al., 2012). However, there could be inconsistency between the e-commerce websites' privacy policies and online vendors' conduct.

The aim of this study is to investigate China's e-commerce websites' privacy policies from a *legal perspective* i.e. an understanding of how the law and its enforcing mechanisms impact privacy policies[2]. This study will address two research questions:

(1) Why is there an inconsistency between the e-commerce websites' privacy policies and online vendors' conduct?

(2) How do the legal concerns of Chinese consumers about privacy relate to their behavioral changes induced by the e-commerce websites' privacy policy?

This study will build a theoretical framework to conceptualize the privacy-deprived e-commerce in China. In doing so it provides a preliminary understanding of the strength of e-commerce websites' privacy policies, if any, and the impact on consumers' privacy perceptions and related behaviors. This study also lends support to render a series of practical references for both online vendors and regulators by disentangling the seemingly contradictory yet complicated phenomenon widely observed in China's e-commerce market and delineating the attributive factors that they should be cognizant of.

Previous research on e-commerce websites' privacy polices primarily focuses on constricted scope of determinants, which can be categorized into dispositional factors and situational

[1] There are now more than 4.6 billion Internet users worldwide. This represents a meteoric rise from 1 percent of the world's population having access to the Internet in 1995, to estimated 59 percent in 2020. Real time user data is available at https://www.internetlivestats.com/internet-users/

[2] We thank anonymous reviewers for suggesting this.

factors. The dispositional factors, relatively stable over time, describing the consumers' distinct characteristics that shape their core values and beliefs, such as personality, propensity to trust, and cognitive style have received more emphasis (Earp et al., 2005; Yang, 2013). The situational factors, which relate to the external stimuli that influence consumers' perceptions, have garnered limited attention only with some sporadic explorations (Tsai et al., 2011; Aïmeur et al., 2016). The few existing research attempts to concentrate on some imminent factors, such as privacy policy wordings and layout, but fails to look into the *legal perspective*.

Over the years the Chinese government has passed more than 200 laws, rules, and related normative documents covering the protection of personal information but they are inadequate to protect personal information of netizens (Sheng, 2019). Consumer Protection Law (effective 15 March 2014), Cybersecurity Law (effective 1 June 2017) and E-Business Law (effective 1 January 2019) only establishes basic privacy requirements and do not protect personal information of online shoppers.[3] The amended Personal Information Security Specification, which will be effective from October 1, 2020 also fails to provide citizens a right to protection of their privacy because it is just a guideline and not a law (Sheng, 2019). The problem with most laws in China is that they are vague and non-binding text. "They set best practice standards that companies are encouraged to implement themselves voluntarily – *in theory*" (Pernot-Leplay, 2020, p. 74). Given that there exists a number of privacy related laws in China but are a 'toothless tiger', including the Personal Information Protection Law, which is in the draft stage (STDaily, 2020), our research is important and timely.

On the practical aspect, whilst the expansion of China's e-commerce market over the years would seem to suggest that Chinese consumers' privacy concerns have been alleviated by B2C retailers' adoption of privacy policies, empirical research indicates that Chinese consumers in fact have very little trust in even the most frequently used B2C e-commerce websites. Approximately two third (64 percent) of respondents in one survey expressed skepticism in the privacy policies of these websites (Wang & Yu, 2015). Another study conducted by China Consumers' Association (CCA) found that privacy policies of 47 percent *online vendors are inconsistent, lacking in content, or even inaccessible (CCA, 2018)*. Despite privacy policies not up to scratch and being looked at with skepticism by consumers, the Chinese online vendors have dominated the market recording high transaction volumes and revenues. On the contrary,

[3] These laws are available at the following website:http://www.moj.gov.cn/Department/content/2013-10/31/592_201244.html; http://www.moj.gov.cn/Department/content/2016-11/23/592_201322.html; http://www.moj.gov.cn/Department/content/2018-09/03/592_201363.html

foreign e-commerce giants such as Amazon, ebay, newegg, *provide much more comprehensive and accessible privacy policies (Zhou & Wang, 2017)* but are unable to generate online sales. They are unable to compete with Chinese vendors such as JD.com and TMall that control 82% of the e-commerce market (Reuters, 2019). To this end, the status of this affair is not only observed to be conflicting, but also contradicts to the empirically verified hypothesis in previous research (Tsai et al., 2011; Athey et al., 2017), that adequate privacy policies increase sales, which thus necessitates an exploration to explain the phenomenon.

The remainder of this paper proceeds as follows. First, it undertakes a comprehensive examination of the privacy literature to develop a ground for the investigation at hand. The next section describes the methodology adopted in this research. In this section we justify why we chose grounded theory for our research, the mode of data collection, the way sample population was selected, and the manner in which analysis was done. Following the methodology section, the findings and a general discussion are presented. This is followed by a proposed framework and its relation to existing theories. Finally, the paper concludes with the implications and limitations of the study.

LITERATURE REVIEW

Privacy is recognized as a fundamental human right by the United Nations. The UN Declaration of Human Rights 1948 (Article 12) states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation."[4] Everyone has the right to protection from the law against such interference or attacks.[5] Almost all nations in the world, including China, are signatory to the UN Declaration. However, unlike most other countries, China neither recognizes the right to privacy explicitly in its Constitution (Chinese Constitution 1982), nor has it ratified the international treaty that recognizes privacy rights, the International Covenant on Civil and Political Rights 1966 (ICCPR), despite having signed the treaty on 5 October 1998.

The judiciary in China has played an important role in linking provisions across much of the country's legislation (Chinese Constitution 1982; General Principles of Civil Law 1986;

[4] http://www.un.org/en/universal-declaration-human-rights/

[5] Article 17 of the International Covenant on Civil and Political Rights 1966 has a similar provision to Article 12 of the UN Declaration of Human Rights 1948. See http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Explanations of Several Problems in Reviewing Reputation Right Infringement Cases; Interpretation to Several Questions on Adjudicating Cases of the Rights to Reputation 1993 and 1998) in order to protect the privacy rights of its citizens (Ong, 2011). In *Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn* (Beijing Chaoyang District Court, No. 10930 of 2008), the court defined privacy as the right to private life, information, space, and those aspects of a person's interests and personality that he does not intend to share with others (Ong, 2011). The court identified five factors as important in determining whether an infringement of privacy has occurred: (a) the manner by which private information is acquired; (b) the manner by which the information is disclosed; (c) the scope of disclosure; (d) the purpose of disclosure; and (e) the consequences of disclosure. The privacy of an individual can be divided into four facets: bodily privacy, territorial privacy, privacy of communications and information privacy[6]. This paper focuses on information privacy.

Information Privacy

Information privacy may be defined as an individual's ability to control the circumstances in which his/her personal information is acquired and used (Galanxhi-Janaqi & Nah, 2004). Where the Internet is concerned, it has reduced the individual's power to control how their information is acquired, disseminated and used (Mansell, 2017). The growing capacity of new technologies to process information, which is further enhanced by its large-scale complexity of computing, has made privacy an increasingly important issue (Brown & Muchira, 2004). The meteoric rise in online shopping over the last decade has resulted in a huge amount of personal information about consumers being collected and utilized by retailers. As a result, the privacy issue started to garner increasing attention from academia. To begin with, most scholars undertook research based on the underlying assumption that privacy is stable and normally remains unchanged in a relatively short time window.

However, scholars have progressively found out that this state of affairs is complicated. Speaking from an economic perspective, Taylor (2004, p. 631) proposed that the "value of consumer information (privacy) derives from the ability of firms to identify individual consumers and charge them personalized prices". As for the behavioral aspect of privacy, people often lack enough information to make privacy-sensitive decisions. Even with sufficient information, their decision-making may be affected by various factors. The issues are sensitive,

[6] http://gilc.org/privacy/survey/intro.html

and there is a dichotomy between privacy attitudes and actual behaviors. Rather than assuming that consumers have stable, coherent privacy preferences, scholars have accepted the possibility that privacy may be unreasonably and unevenly utilized.

In terms of research topic, one of the main research enquires is to establish the theoretical framework in which the privacy was tentatively constructed, such as privacy measurement (Englehardt, et al., 2014) and privacy calculus model (Dinev & Hart, 2006). Scholars believed that by specifying how the privacy was framed, we may have a deeper understanding of the role of privacy in affecting individual's behavior and trust in the adoption of a certain service or IT product, such as e-commerce (Anic, et al., 2019).

In contrast, the research efforts at later stage have witnessed a fundamental change, when the scholars attempted to figure out the economic, behavioral, and some other societal transmission mechanisms that affect privacy (Zhu & Tao, 2015). To be specific, instead of mainly investigating how the privacy affects other constructs, the research focus shifted to how the privacy is affected by those (Smith, et al., 2011), for instance, certain behaviors (perceived security, perceived ease of use, etc.) (Limpf & Voorveld, 2015), and trust (Chellappa, 2008). This is because after assuming and accepting the fact that privacy is context-based and scenario-sensitive, scholars tend to examine the issue further and deeper – the "why and how" questions (Bélanger & Crossler, 2011).

Information Privacy in China

The rapid economic, technological, and social changes of the last 30 years have fostered a growing awareness of the concept of information privacy in China, and there have been steady advances both in terms of scholarly work and the legal system (Gao & O'Sullivan-Gavin, 2015). Concerns over information privacy initially emerged in the late 1990s, but it was not until the 2000s that the issue came into the spotlight for scholars and legislators in China. As the Internet infrastructure proliferated and China became increasingly connected to the world, scholarly research into information privacy expanded, with academics conducting empirical studies to evaluate the privacy policies of websites (Chen, 2009) and surveying the behavior and attitude of Chinese consumers toward online privacy issues (Yang & Miao, 2007).

In recent years, continuing digital development has brought with it growing threats to privacy, and information privacy has become even more of a priority. Chinese scholars have responded

by defining information privacy as an essential civil right rather than a personal property issue (Gao & O'Sullivan-Gavin, 2015). Their work has informed policy-making in regard to information privacy and its protection; not only has the Chinese government now formally recognized privacy as an independent civil right, but it has classed the violation of personal data privacy as a criminal act. In general, the current privacy protection policy in China largely embraces the fundamental principles embedded in international privacy protection practices whilst giving consumers enhanced protection on some specific fronts. However, China has failed to pass a dedicated, comprehensive national law on privacy protection despite the fact that the law was drafted and submitted to the State Council of China as far back as 2005 (Li & Xu, 2012).

It is true that legal measures for the protection of privacy in China are not comparable to those available in the West (Ong, 2011), though privacy law has developed significantly since 2009 and there are now a number of laws that govern the protection of privacy. For example, the National People's Congress (NPC) has amended the Criminal Law (effective 1 November 2015), adding several provisions related to data privacy and cybersecurity. The amended Article 253 states that anyone who violates relevant national regulations to sell or provide others with citizens' personal information, and where the circumstances are serious, will be imprisoned for a period of up to three years and/or fined. If the circumstances are extremely serious, imprisonment can be for between three and seven years and there is also a concurrent fine. However, the Criminal Law does not define what type of information would be considered 'personal', nor does it explain which circumstances it considers serious, extremely serious or not serious (Greenleaf, 2014).

Although some scholars are of the view that usage of personal data without consent should always be treated as a crime (Li, 2011; Meng, 2011), privacy is generally seen as a matter of offense rather than criminal law in China (law books often refer to tort of invasion of privacy). Offense as a statutory right is a recent development in China. The People's Republic of China (PRC) Tort Liability Law (TLL), which came into force in July 2010, includes a right to privacy in its list of protected 'civil rights and interests' (Article 2). It does not explicitly set out the rights of the consumer or the obligations of Internet retailers under tort law, but it does state that 'a network user or network service provider who infringes upon the civil right or interest of another person through the network shall assume tort liability' (Article 36). Livingston and Greenleaf (2015) are of the view that the term network service provider is meant to encompass

all those who provide Internet content, including websites. The breach of personal data by Internet retailers may, therefore, be considered a violation of privacy under the TLL.

Information Privacy, Trust, and E-commerce

Trust is pivotal in the context of e-commerce (Sullivan et al., 2018); numerous studies have argued that consumers' estimation of how risky online activity is likely to be depends on how much they trust the Internet retailer concerned (Milne & Culnan, 2004). This is supported by the Privacy-Trust-Behavioral Intention model (Liu, Marchewka, & Ku, 2004), which indicates that the success of the buyer-seller relationship depends on the level of buyer trust. This trust, and consequently the success of the e-business, can be materially impacted by privacy concerns (Odom et al., 2002).

The impact of privacy concerns on trust is discussed by Chan and Ma (2013), who suggest that heightened concerns over privacy lead to perceived lower credibility and higher risk during the information-sharing process. Wu et al., (2012) posit that such concerns may make consumers reluctant to provide personal information online or even unwilling to use e-commerce at all. Conversely, where there is trust, privacy concerns are likely to be reduced. Dwyer et al., (2007) found that the more users trust an Internet retailer, the more willing they are to share their personal information and develop contacts. Modelling analysis of privacy and trust has confirmed that the greater trust consumers have in an Internet retailer, the less worried they are about privacy (Shin, 2010).

Trust also influences consumer behavioral intentions when it comes to e-commerce transactions. In an interdisciplinary exploration into the complexity of trust, Pappas (2016) found that trust mediates consumer behavior in the context of e-commerce. This notion was subsequently empirically examined by Oghazi et al. (2018), who concluded that the level of trust the consumer has in an Internet vendor generally influences their intentions, particularly the purchasing process. To sum up, information privacy and trust are mutually influential, and both affect – either indirectly or directly – the success of e-commerce.

E-commerce Websites' Privacy Policies

Internet retailers have developed a number of solutions to alleviate consumers' privacy concerns, build trust and avoid potential losses. The adoption of privacy policy is one such solution. The privacy policy represents a long-term promise to the business's end users (Antón,

et al., 2007); in principle, it fills the information gap between the consumer and the vendor by providing a complete picture of the vendor's information practices.

The adoption of privacy policies started in the late 1990s, and the examination of their use and implications has been a matter of regular investigation since then (Meinert et al., 2006). Researchers have suggested that consumers who provide false personal information would be more willing to supply their real information if online retailers specified how this information is used (Bansal et al., 2016; Martin & Murphy, 2017). But whilst this implies that the privacy concerns of consumers can be mitigated simply by online merchants making their privacy policy available, other studies indicate that this only works if consumers actually read and use the information contained in the policy (Tsai et al., 2011). For example, some scholars point out that privacy policy that is too comprehensive may be difficult to understand (Fabian et al., 2017) and time-consuming to read (Vu et al., 2007), with the result that few consumers will bother to read it properly. Pollach (2007) criticizes the effectiveness and quality of privacy policies, suggesting that too many fail to address certain important areas of user concern. He recommends that they should contain information on at least five areas, namely data collection, third party data collection, data storage, data sharing, and marketing communications. This may create a situation where even those individuals who know that an e-commerce website has a privacy policy may still lack the information they need to make informed decisions.

All this points to the need for e-commerce websites' privacy policies that are easy to understand, effective, and transparent. A number of researchers (e.g. Meinert et al., 2006; Kasem-Madani & Meier, 2015; Le Métayer, 2016) have responded by focusing on how to enhance the effectiveness of privacy policies, whilst Tsai et al. (2011) have offered additional motivation to make privacy policies salient and accessible by advising that some consumers are willing to pay a premium to purchase from a privacy-protective website. This suggests that Internet retailers may even be able to leverage privacy protection as a selling point. In general, these scholars hold the view that a clear and credible privacy policy helps Internet retailers build a positive reputation and develop trust with consumers.

Legal Perspective in Privacy-related Research

That privacy and its related issues are inherently legally rich is initially discussed in the most influential article "Right to Privacy", written by Samuel D. Warren and Louis D. Brandeis in the Harvard Law Review in 1890 (Warren & Brandeis 1890). Warren and Brandeis argued that as political, social and economic changes incessantly occur in the society, new rights emerge

to “meet the demand of society” and ensure the full protection of the person. Internet has been the biggest change in recent history and poses a threat to privacy, and hence there has been a trove of researches on it in the legal (e.g. Lee 2018; Qi, Shao and Zheng, 2018; Greenleaf and Livingston, 2016) and IS (e.g. Kayworth et al., 2005; Lebek et al., 2013) disciplines. Studies in the IS are primarily surrounding privacy per se, such as the legally enabled management of privacy, the protection of privacy under legal systems, and the legal challenges in digitalized domains. In the legal discipline, scholars have focused mostly on evaluating the core principles and salient features of privacy law, to what extent they are stringent and comprehensive and comparing legislation of one jurisdiction with other jurisdiction(s).

Earp et al., (2002) are the only scholars who have briefly discussed privacy policy from a legal perspective when designing a framework for privacy management and policies. According to them “since the law is the most obvious influencer in the privacy policy and privacy management arena, the legal perspective is designated as the framework’s outer layer…[that] …constrain the privacy practices of the inner layers” (Earp et al., 2002, p.5), which are technical, business, contractual and social perspective. We are not aware of any other empirical research that looks into privacy policy from a legal perspective and aims to fill that gap in the literature. This paper suggests that a legal perspective is not only important to deepen scholarly understanding of privacy policies, but also that understanding customers’ perceptions and behaviors and related analyses holds critical implications for online vendors and regulators.

METHODOLOGY

The design of a research project will be determined by the nature of the research questions raised and their context in the literature (Zhu, 2017). In this case, the research questions and the lack of literature around them indicated that it was necessary to have an in-depth exploration of the phenomena. The focus on consumer behavior called for an interpretive paradigm to identify the motivation and justification behind it and to understand its rationale as the way to formulate theory. Several quantitative studies have been done so far on the correlations between certain antecedents and e-commerce websites’ privacy policy (Flavián & Guinalíu, 2006; Warkentin, Johnston, & Shropshire, 2011; Wu et al., 2012). Most of them specify the linkages among the individual’s dispositional conditions, observed online behaviors, and privacy policy. However, considering the aforementioned research in literature review, the

efficacy of privacy policies seems to affect the actual users' behaviors in an unexpected manner, suggesting that the privacy policy may have been studied outside its own unique context. This leads to a series of studies on the variables which are relevant to our understanding of privacy policy, but it steers our attention away from the conditions under which privacy policy is more likely to be in effect. In this sense, quantitative research does not seem to tell the whole picture of privacy policy; it necessarily ignores the external ambience – the legal context – where privacy policy will be enforced. In addition, quantitative research cannot account for contingency, which is crucial for IS research due to the complexity of the phenomenon being investigated. Furthermore, quantitative research seldom leads to clear policy advice, which is of utmost importance in helping both regulators and adopters to maximize the effectiveness of privacy policy. As a result, qualitative methods were selected as the most likely to give an insight into Chinese Internet consumers and their social and cultural context (Myers, 1997).

In this study, the research approach used is the grounded theory (GT) method (Glaser, 1992, 1998; Strauss & Corbin, 1998), and it is used as both the method of data analysis, and as the technique for theory building. GT has proved to be extremely useful in largely understudied areas with little existing theory (Orlikowski, 1993; Strauss & Corbin, 1998), such as privacy policy in this case. It is also good at developing context-based descriptions and explanations of IS phenomena (Myers, 1997; Goulielmos, 2004). Grounded theory has become increasingly popular in the information systems domain (Lings & Lundell, 2005). Martin and Turner (1986) define it as: 'an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data'. As such, it fits well with the nature of the research at hand. It also lends itself to the exploration of under-theorized areas (Burck, 2005), helping the researcher to generate theory and in-depth understanding of the processes and to develop conceptual analyses of the social world. Indeed, the literature suggests that scholars employing grounded theory should not start with any pre-conceived concepts but allow the concepts to emerge from the data (Matavire & Brown, 2008). Given the understudied nature of e-commerce privacy policy in China, and our lack of pre-conceived concepts, GT is an appropriate tool for the current research.

Data Collection

Glaser (1992, 1998) recommends the collection of rich and versatile data for GT studies. The completion of semi-structured interviews thus followed this directive, assuring the validity of

the research (Bryman, 2004). The interview process contained seven questions, which were divided into three sections: basic information concerning consumers' general views of, and attitudes towards privacy policies were collected in Section 1 of the interview; their knowledge about privacy policy along with their habits and experience of accessing and utilizing these documents was collected in Section 2.

This information would be useful in two ways. First, knowing more about the current level of consumer awareness of privacy policy and consumer behavior would help us assess the appropriateness of current online vendor strategy, particularly in regard to human factors and potential privacy intrusion aimed at consumers and their behavior. Second, knowing more about consumers' habits and experiences would help us determine how privacy policy inter alia may be affecting behavior.

After completing these two interview sections, each subject was encouraged to share their ideas and opinions with the researcher in Section 3. The interviewees were allowed to express their views on issues they considered to be of importance. These interviews helped us fully understand their real thoughts. As the intention was for consumers to feel relaxed about communicating with us, no recording devices were used during the process (Silva & Backhouse, 2003). However, extensive notes were taken from which quotes could be drawn.

Semi-structured interviews were selected as the means of data collection for a number of reasons. Primarily, the varied professional, educational, and personal histories of the sample group precluded the use of a standardized interview. Semi-structured interviews were considered well-suited for exploring the respondents' perceptions and opinions around this complex and sometimes sensitive issue as they allowed us to probe for more information and clarification as necessary (Barriball & While, 1994). Furthermore, the inclusion of open-ended questions gave opportunities to identify new ways of seeing and understanding the topic at hand. Bernard (1988) argues that semi-structured interviews are best used when the researcher has only one chance to interview the subject, as was the case here. The semi-structured interview guide provides a clear set of instructions for interviewers and can provide reliable and comparable qualitative data (Cohen & Crabtree, 2006).

Subject Selection

The subjects were all active e-commerce users who have had at least two online purchase experiences. With the permission of the financial institution (C-bank) and supermarket (Y-

supermarket)[7], the potential subjects were identified as they finalized their transactions at the checkout. There were two reasons for this: (1) to do online shopping, consumers must register for online banking; and (2) most e-commerce transactions in China are conducted using the online payment tools Alipay or Wechat (these can also be used in supermarkets) (Qu et al., 2015). Consumers who were observed completing a relevant transaction of online banking at the bank counters or paying via Alipay or Wechat at the supermarket tills were invited to participate in the research. Thus, sample selection was purposive sampling (selecting with knowledge of the phenomenon) linked with a convenience sampling (random selection of those who happened to be there at the point of data collection). Those consumers who agreed to the interview request were taken to the VIP client lounge at the bank or to the café nearest to the supermarket. All interviews were done in Chinese and translation was done by the first author who is a native speaker. A total of 88 subjects (48 males and 40 females) participated in the research; they ranged in age from 24 to 66, with 57 people in the 24-35 age group, 19 in the 36-55 age group, and 12 in the 56-66 age group (Table 1 describes the detailed demographic profiles distribution). The sample size is considered to be within the range to provide validity for the study – even the gender split satisfies the average size of a valid sample for GT. Factors such as knowledge of the participants also affects the sample size.

Table 1 Demographic Profiles Distribution

Number of Respondents: 88

Demographic	Value	Count	Percentage (%)
Gender	Male	48	54.5
	Female	40	45.5
Age	24-35 years old	57	64.8
	36-55 years old	19	21.6
	56-66 years old	12	13.6
Education	High school and below	5	5.7
	Bachelor's degree	59	67.0
	Master's degree	22	25.0
	Doctorate degree	2	2.3
Employment	Employed	63	71.6
	Self-employed	11	12.5
	Student	6	6.8
	Retired	8	9.1
Internet	Less than 1 year	2	2.3

[7] The two organisations remain anonymous at their requests.

experience	1-2 years	5	5.7
	2-5 years	23	26.1
	5-10 years	41	46.6
	More than 10 years	17	19.3

Data Analysis

We started analyzing the data as soon as it was collected and followed the GT coding stages: open coding, selective coding, and theoretical coding. At the opening coding stage, the interview data was analyzed line by line, a coding method that is recommended by Urquhart (2007) and demonstrably useful. Selective coding thereafter facilitates the categorization of the preliminary codes that are derived from the first stage. Practically, we sorted all open codes into groups as the selective codes. Two authors discussed with each other the possible selective codes based on the meaning of the open codes until the final agreements were reached. We then proceeded to theoretical coding, where the correlations among those selective codes and the core theoretical cluster/s surfaced. During this stage, Hekkala and Urquhart (2013) suggested an analytical memo approach, rare in IS but well accepted in social science, where the scholars take notes of their own thoughts about the entire procedure of cluster development. Given its proven usefulness in theorizing, we employed the analytical memo approach in this work. Following the principle of constant comparison (Strauss & Corbin, 1998; Glaser & Strauss, 2009), we systematically compared each new piece of data with what we already had, looking for similarities and differences and developing categories until each category identified in the theory was saturated and no new insights in that category arose (Glaser, 1992).

FINDINGS

The interviews revealed some illuminating findings. All respondents admitted that e-commerce has brought tremendous convenience to their daily life by offering a great variety of products with more transparent prices. However, their answers highlighted several issues surrounding privacy and e-commerce and its possible personal influences. The preliminary results also interestingly suggest that there is no significant difference in responses among different demographics in terms of gender, age, and education.

We identified four primary categories – legal influence, privacy policy's manifestation, consumer perception, and consumer behavior – from the selective codes to form the basis of the core theme of e-commerce website's privacy policy's efficacy in detail, which together are illustrated in Table 2.

Table 2 Construction of Privacy policy's efficacy

Category	Selective code	Analytical summary
Legal influence	Chinese law	Legal influence is presented mainly in the forms of enacting laws and supervisory body: if the laws and body are widely known and in effect, significant influences are anticipated; otherwise, they are limited.
	Supervisory body	
Privacy policy's manifestation	Layout	Legal influence is also adversely affected by the privacy policy that is presented by each B2C website as its front to consumers. Layout and design of privacy policy are among the most important facets that are important to consumers: the former referring to its accessibility and the latter reflecting its understandability.
	Design	
Consumer perception	Past experience	Consumers' past experience shapes their decision-making towards e-commerce, and in general, the sentiment of distrust is pervasive among them, which further affects their thoughts and actions.
	Distrust	
Consumer behaviour	Self-protection	Self-protection activity is the most frequently witnessed behavior in e-commerce transaction, which leads to the awareness of its effectiveness in the context of information privacy and privacy policy.
	Self-awareness	
	Vigilance relaxing	Consumers relax their vigilance for privacy concerns as a result of the self-protection and self-awareness.
	Acceptance of privacy breach	Consumers have to accept a breach of privacy in their life.
	Price and product variety oriented online shopping	The preferences are given to price and product variety by consumers as the main proxies in online purchase despite the allegedly privacy concern.

Legal influence

This category illustrates how e-commerce websites' privacy policy is influenced by the current Chinese law environment. Chinese law is one of the major concerns of the research, and the result suggests that the situation of its unawareness is compounded by the fact that currently there is lack of supervisory body to monitor privacy policy usage.

Lack of supervisory body: Respondents pointed out that organizations list privacy policies on their websites, but they were not independently verified by an influential and impartial third party, and there is no supervisory body within the government system that will check whether the privacy policies are proper or workable.

> *"I don't think there exists an organization that belongs to the government specifically dealing with privacy protection, let alone privacy policies, especially the privacy policies of Internet vendors." – Interviewee 10*

> *"They can publish all they want – some sweet nothings – because no one would regulate their manners or tell them how to make their promise to consumers. They just pick up the nicer words. I know the Consumer Association, but they are more concerned about the product quality (whether it is counterfeit) rather than privacy policies, aren't they?" – Interviewee 15*

Unaware of enacting Chinese law: As a result of the above, almost all of the respondents were unsure whether China had any legislative measures in place to oversee how the personal information of consumers is handled by the Internet vendors. The interviewees believed that the privacy policies on shopping websites were self-made regulations adopted by retailers rather than an obligation under Chinese law, and that as such, it is unlikely that they will adhere to this policy promptly or properly.

> *"I don't quite know if there is any relevant law or not. I guess so, but I have never heard of that or been aware of them." – Interviewee 19*

> *"Privacy policies? Aren't they self-claimed statements that appear to be very formal and official, but how knows? There's no national law or judicial rules that can be applied to them." – Interviewee 53*

Manifestation of privacy policy

The importance of this category's effect on the legal influence came to the attention in the process of analysis, which is mainly reflected in two dimensions – the layout and design of the privacy policy.

Layout of privacy policy: Only six respondents had read the privacy policies on shopping websites. A large proportion of interviewees complained that these privacy policies are not easy to find; one interviewee was of the view that all shopping websites are designed in such a way as to promote advertisements and sales information, with privacy policies being deliberately hidden behind the promotional material and consequently difficult to spot.

> *"If not were asked by you, I would never know they have privacy policies on their websites!" – Interviewee 33*

> *"I heard of that from TV news, but they (privacy policies) didn't come to my notice on their homepages. Apart from commercials and promoted products, what else?" – Interviewee 75*

All respondents expressed their frustration of the privacy policies posted by the Internet retailers. One respondent asked: *'How can you believe a statement (privacy policy) that is almost inaccessible? If they do not want us to even know the existence of this stuff, it is weird that they want us to trust it'*. He further added that: *'If they do have strong confidence in the contents and quality of the privacy statements, they should put them in a more eye-catching position instead of a place where you have to make efforts to locate it'*. *Interviewee 62*

Design of privacy policy: Among those who said they had managed to locate the privacy policies, a few admitted to not reading them or to just glancing at them. Various reasons were given for this, such as the privacy policy being *'excessively'* lengthy and too *'technical'* to understand. One respondent mentioned that the only privacy policy he had skimmed contained so much legal and computer jargon that it was almost entirely incomprehensible for a layman. Policies were also criticised as *'vague'* because they fail to specify how personal information will be processed. The respondents therefore deemed reading these policies a *'waste of time'*.

"I must be too bored to read it (e-commerce website's privacy policy) once – also the last time! It's extraordinary long like a formal contract!" – Interviewee 15

"Sometimes they have used many terminologies that sound very obscure to me – the trick they played to prevent us from reading, I guess." – Interviewee 36

"I have an impression that they don't want us to understand them (e-commerce websites' privacy policies). They only list something superficial or what we already know even from the newspaper." – Interviewee 48

As the respondents found that the privacy policies of these e-commerce websites are generally inaccessible and user un-friendly, they doubted whether there was any legal enforcement regarding this issue. Most of them concluded that the law pertaining to privacy policies was either '*absent'* or '*ineffective'*.

Consumer perception

The notion of consumer perception arose from the open coding process, where the past experience in privacy breach and the distrust towards cyberspace emerged. They together illustrate how this selective code focuses on the efficacy of e-commerce website's privacy policy.

Past experience in privacy breach: Almost all respondents were worried that their personal information was being gathered and utilized by online retailers and even disclosed to unauthorized third parties without their consent. Some respondents considered themselves *'victims'* of privacy breaches, citing *'an unprecedented scale of privacy intrusion'* into *'every aspect'* of their life. All respondents mentioned that in the recent past they had been frequently harassed through spam, text and phone calls, and that the harasser was aware of one or more pieces of their personal information such as full name, address, gender and purchase behavior.

"Literally I receive unsolicited texts every day from all different unknown numbers and they even know my name! Very scary!" – Interviewee 26

"I can't tell you how many calls I have received to tell me either I got a lottery or I received a court summon, or something even weirder. It didn't surprise me if they know my names, but it did when they even read out my national ID number and home address! How did they get them?" – Interviewee 69

Distrust towards Cyberspace (including privacy policies): Apart from their negative personal experiences in privacy breach, the respondents also admitted their distrust towards cyberspace, which was generally deemed as capricious and undistinguishable. They have been repeatedly advised of online scams, phishing attack, identity theft, etc. from news coverage and/or friends' experiences. To this end, most of them expressed skepticism to nearly all online commitments and/or '*self-claimed*' promises, for instance, privacy policies.

"I feel a bit uncertain and unsafe for everything online, and thus I have to be very (very) careful. I have known numerous online scams, some of which were not easily identified or avoided." – Interviewee 1

As highlighted above, some respondents attributed their distrust of cyberspace, including privacy policies, to the lack of regulation in this area. They also cited the lack of a supervisory body to oversee the activities of Internet retailers.

Consumer behavior

What people say is sometimes different from what they do, and extra attention was thus given to the selective code of consumer behavior, which consisted of four open codes – self-protection, self-awareness, vigilance relaxing, acceptance of privacy breach, and the use of privacy and product variety as the main parameters for choosing e-commerce vendors.

Patchy self-protection measures: In order to protect themselves from privacy breaches by Internet retailers, a few respondents adopted self-protection measures that could be viewed as passive and patchy. For example, one respondent mentioned that the Internet vendor she frequently used allows consumers shopping on its website using a pseudonym (though other personal details have to be genuine), whilst another described having bought an app that generates a new mobile phone number each week. He used the generated number when filling out personal information on the shopping websites.

"So every time I do online shopping, I just filled out the shipping form with a pseudonym. …… Yes indeed, the address has to be real, and

otherwise I wouldn't receive my parcel. …… (Laughing) I know it alone can't be very effective, but at least I have to do something to protect myself; at least they didn't know my name, did they?" – Interviewee 31

"I use an app, which enables me to provide a one-time mobile phone number for one week when I order something from Internet vendors. ……. Oh, yes! You are right. They still have my name and address!" – Interviewee 53

Self-awareness of inadequacy of the measures: However, the effectiveness of such privacy protection measures is very limited; pseudonyms and temporary phone numbers are unlikely to protect a person from breaches of privacy as long as they have to supply other personal details such as email and mailing address (for delivery). With the growing experiences of online shopping and privacy breach, the respondents came to realize that the self-imposed measures did not work to a satisfactory level regarding their privacy protection:

"I used to adopt a bunch of measures (learned from my friends and online articles) to protect myself from privacy intrusion, such as pseudonyms and a second phone number just for online shopping. They worked a bit into effectiveness, but far less than being useful – I realised this as the unsolicited emails/texts are never getting fewer. To be honest, I feel extremely frustrated but what else can I do, stopping shopping online?" – Interviewee 23

"I always doubt these measures which were introduced by TV programmes and/or from Wechat Moment posts are really working. The reason is simple – there are so many online e-commerce shops and websites, and it is almost impossible to make sure all of them treat our own information seriously and responsibly if there is no regulation; even there is, I am not sure how it will be effectively implemented." – Interviewee 84

Passive vigilance relaxing for privacy concern: Due to the fact that the self-protection measures are inconclusive, and their usefulness is limited, the respondents constantly face the possibility of privacy invasion. As this trend progresses, they gradually relaxed the vigilance for privacy breaches since their efforts were in vein:

"I tried to protect my own privacy, but to no avail. Given that privacy invasion is pervasive at an unprecedented scale (we do online shopping almost every day), it would be too effort/time-consuming to perform full protective measures – I would be exhausted as well. Then it would be much easier if I don't take it that seriously, at long as my key personal information is not compromised." – Interviewee 16

"I think the privacy breach is the by-product of digital life. An old Chinese proverb says 'no fish can survive if the water is too clean'; for the same reason, no online activities are possible if no personal information is provided. (Therefore) I decided to downplay the privacy." – Interviewee 32

Acceptance of privacy breach as one fact of life: The passive vigilance relaxing further leads to the acceptance that privacy breaches are 'unavoidable' and 'normalized by the introduction of digital life'. Respondents claimed that they try to strike a balance between the state of 'being moderately privacy breached' and the bottom-line of 'keeping key information safe and secure.'

"I chose to accept it (privacy breach) as something normal or the cost you have to pay for the convenience received from shopping online; but of course, the cost can't be too high to afford." – Interviewee 23

"Personally, I would argue it (privacy breach) is common, and with the online activities become increasing diverse and essential to our daily life, it will get even worse. We have no better choice but accepting it. However, if there were some regulations, the scenario would be different I assume." – Interviewee 48

Using price and product variety as the main parameters for choosing e-commerce vendors: In view of all the above, all respondents were of the view that a wide product range and competitive prices are more important to them than the privacy policy; even if a lesser-known retailer were to provide a clearer and more comprehensive privacy policy than its better-known competitors, consumers would still prefer the latter because they sell a wider variety of goods, offer better prices, and are more well-known. They were dismissive of Internet vendors' self-drafted privacy policies – which have not been independently verified by a trusted third party – seeing them as unlikely to influence their purchasing behavior.

"To be honest, I don't bother to read them (privacy policies). As long as they are not verified or regulated by laws, I won't believe what they said at all. In this regard, the most important (thing) for me is the price. And maybe the bigger brand will be more cautious in handling our personal information? At least it cares about the reputation, I guess." – Interviewee 55

"There's no watchdog to oversee if what they said there are consistent with what they did. I don't feel very assured from them. So, I'd rather choose the one (Internet vendor) at least provided me some benefits, such as good price, more choices of products." – Interviewee 47

DISCUSSION

In this paper, we presented the efficacy of e-commerce websites' privacy policies derived from a GT study, which studied the seemingly conflicting phenomena leveraged by the absence of the legal enforcement. This section discusses the findings in the light of the literature in an effort to address the two research questions.

The study finds that whilst consumers in China are taking advantage of digital technologies to shop online in ever greater numbers, they are also concerned about privacy breaches and unwanted approaches from Internet retailers. These concerns are understandable, given the growing problems with online shopping security over the recent years (CNNIC, 2019). In 2018, 28.1 per cent of online consumers were victims of fraud, up by 1.5 percentage points from 2017 (CNNIC, 2019). Crucially, breaches in privacy are positively correlated with the amount of data collected by Internet retailers from their consumers. Wen (2013) states that 70 per cent of Internet retailers in China make it mandatory for consumers to provide at least three personal details – name, phone number, and mailing address – if they want to buy products from their website. This huge body of data is stored on web servers, offering a fertile environment for privacy invasion (iResearch, 2012). Our study finds that consumers in China are indeed bombarded with unsolicited content in the form of spam and texts, but that they are uncertain as to whether the legislative measures exist to protect them from this harassment. They are *aware* that there is no regulation regarding privacy policy or its verification through independent organizations.

The Chinese government's most recent move to protect online consumers' privacy rights is the PRC Law on the Protection of the Rights and Interests of Consumers (Consumer Law) (effective 15 March 2014) and the corresponding Measures for Penalties for Infringing upon the Rights and Interests of Consumers (Measures) (effective 5 January 2015). According to the Measures, business operators collecting or using the personal information of consumers must follow the principles of legality, appropriateness, and necessity. They must clearly state the purpose, manner, and scope for collecting and using the information, and obtain consent from the consumer. Finally, they are forbidden from leaking, selling, or illegally passing consumers' personal information on to other entities (Article 11(1), (2)). Unlike the Criminal Law, the Measures define what constitutes personal information:

> 'personal information of consumers refers to a consumer's name, gender, occupation, date of birth, identification number, residential address, contact information, status of income and assets, health status, consumption habits, and other information collected by business operators during their provision of goods or services that may independently or in combination with other information identify the consumers' (Article 11).

The Measures also take care of spam by prohibiting business operators from distributing unsolicited commercial content. Article 11(3) states that business operators must not send commercial information to a consumer without consent or request from the consumer, or after explicit objection by the consumer. Business operators who breach the above provisions will face penalties from the State Administration for Industry and Commerce (Article 2). Furthermore, their details will be recorded in a defaulters file and their name will be made public. The government has thus demonstrated its willingness to enact both criminal and civil legislation to protect the privacy of its citizens, the Consumer Law and Measures being the most relevant to online consumers. It must now promote awareness of these laws and advise the connections between laws and privacy policies – whether the laws enforce the privacy policies, oversee the privacy policies, or are symbolized by the privacy policies. To this end, the inadequate awareness of law and e-commerce website's privacy policy indirectly results in the contextual privacy-deprived e-commerce in China.

Regarding the consumers' perception, their understanding of the *nature* of privacy has significantly changed since the late 1990s as the Chinese society has gradually come to accept an expanded definition of the concept. Yu and Wu (1999) argue that historically, the right to

privacy was not regarded as a property right, the general view being that the violation of privacy (e.g. through the revelation of embarrassing personal secrets) resulted in mere emotional rather than property damage. However, this began to change since China joined the World Trade Organization in 2001. Chinese policy makers expanded their understanding of the nature of privacy, concluding that the predominant focus of privacy protection should be personal data rather than personal information or personal activity, and accepting that the right to privacy encompasses both reputation rights and property rights. In accepting this, they were acknowledging that privacy violation may have both emotional and economic consequences (Feng & Rong, 2007; Xin & Shi, 2009). This led Feng and Rong (2007) to argue that if privacy is seen as a property right, consumers should be able to control their own data: that they have the right to consent, to know, to query, to protect, to correct and to gain economic interest from this data.

However, the development of new digital technologies has made it necessary to further elaborate the nature of privacy. Li (2011), for example, points out that personal data protection includes but is not limited to privacy protection, and should center on the subject's right of control. This reflects the policy change that has happened in recent years as the emphasis has shifted from privacy as a property right to privacy as an essential civil right. To sum up, although the concept of privacy is now widely accepted in China, there is to date no consensus on the nature of privacy; that is, whether it is a personal property right or a civil right. In other words, the asynchrony between the understandings of consumers and online vendors towards privacy directly leads to the perceived privacy-deprived e-commerce.

The research highlights contradictory behaviors in that the heightened privacy concern and lowered e-commerce website's privacy policy trust revealed here are being accompanied by an increase in online purchase activities. In addition, consumers are not willing to be charged premium for privacy as suggested by the literature but primarily rely on price and product variety as the key factors for online shopping. It is a long-held belief that individual privacy, especially information privacy, is not a priority in China. Tang (2002) attributes this to the Chinese society's long tradition of collectivism over individualism, the government's tight control over its citizens, and a crowded living environment in which private space is seen as an unlooked-for luxury. Yao-Huai (2005) suggests the last two factors are no longer relevant, but the first warrants closer examination.

In traditional Chinese society, the collectivism that repelled individual interests certainly had no serious interest in protecting individual privacy. Before the 1980s, if someone in China publicly expressed his/her intention to pursue their individual interest, he/she would certainly be viewed as an egoist. Since then, however, drastic changes in the economic structure and political domain have also driven significant shifts in thought and attitudes in Chinese society. But whilst the concepts of individual interests, freedom, and rights, no longer viewed as taboo, have undeniably impacted on social life and norms, the prevailing value system has only adapted to a point: that is, it now emphasizes the importance of unifying collective and individual interests instead of simply denying individual interests altogether. Collective and individual interests are both recognized as important, but the former is still seen as more important than the latter. This assumption impacts the moral evaluation of and moral thinking about all aspects of social activity, including privacy. Even though it leaves some space for individual privacy, the belief that collectivism outweighs individualism means that the concept will never carry as much weight as it does in the western societies (Yao-Huai, 2005).

Although people are becoming more aware of privacy, it has not yet become an overriding consideration. As their sense of individualism is reinforced, consumers are starting to care more about their own privacy, but when it comes to the disclosure of personal information to a large or influential organization, they are still likely to conform to existing norms and an undefined collectivism.

THEORETICAL FRAMEWORK

Relating the selective codes

The final stage known as theoretical coding is to first build relationships between the selective codes to form the theoretical framework, which is specified in Figure 1. The unawareness of the Chinese law, and the lack of supervisory body together with consumers' past experience of privacy breach illustrate the current situation of a privacy-deprived e-commerce in China; whereas the layout and design of privacy policy relate to its basics. Regarding the ramifications of the privacy-deprived e-commerce, consumers' perception and behavior are centered: their past experience in privacy breach and general distrust towards cyberspace show their perceptions to this issue, while the self-protection self-awareness, vigilance relaxing, and the acceptance of privacy breach delineate consumers' behavior as a whole.

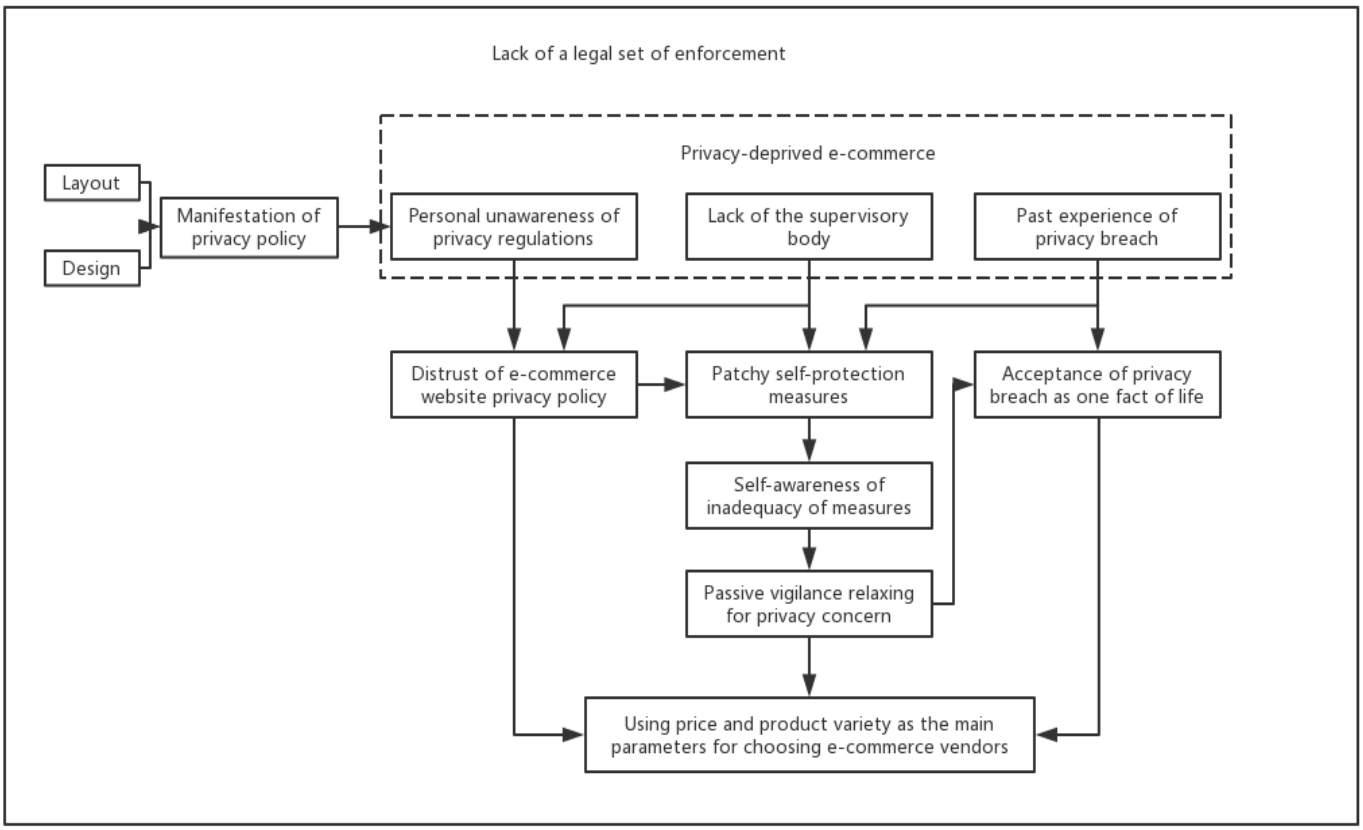

Figure 1 Theoretical Framework Based on Selective Codes

Indicated by the proposed theoretical framework, in this case, we further established the relationship between the three clusters surfacing from the process, namely, lack of a legal set of enforcement, privacy-deprived e-commerce, and price and product variety oriented online purchase. Figure 2 illustrates how the final stage linked them and allowed us to theorize about how the research focus was understood from the core theme of efficacy of privacy policy.

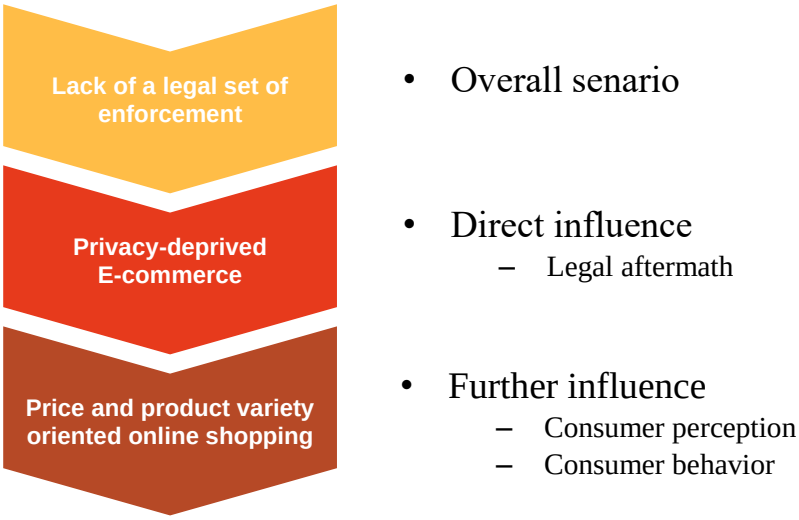

Figure 2 Relationship between clusters

The current status of privacy-deprived e-commerce was drawn upon the lack of enforced Chinese law and/or regulations regarding privacy policy. Due to the observed and foreseeable weaknesses in the enforced Chinese law and the e-commerce websites' privacy policies, consumers have developed a complex set of perceptions and behaviors in regard to privacy concern, privacy policies, and purchase activities. Likewise, the surprising choice of price and product variety as the main parameters for online shopping, which contradicts the notion of privacy as premium, was also seen to be affected by the general privacy-deprived e-commerce. In this regard, consumers further cultivated their self-actions and purchase preferences on the basis of their formed perceptions.

Theoretical Integration

Theoretical integration is an important step in building theory in a GT study (Hekkala & Urquhart, 2013), which relates to the process of comparing the generated concepts and/or theory with existing theories at the same level abstraction (Glaser, 1992). In this study, we link the codes arising from the selective codes regarding the efficacy of privacy policy to Dahmen's (1989) Theory of Development Blocks (TDB) and Jost et al.'s (2004) System Justification Theory (SJT) with examples to illustrate the linkages.

TDB starts with the definition of development block, which refers to a set of interconnected and interdependent factors in industrial development. The factors can be new products, new

markets, new methods of marketing, or new policies. The constant conflict between 'new' and 'old' components, which is named as entrepreneurial activities, implies an interaction between industrial developments and economic changes. In this process, incomplete development blocks generate both difficulties and opportunities for firms. In other words, industry development to a certain stage will require a realization of some further resources, which implies development potentials as complementary stage(s). If the complementary stage is missing, it will cause structural tension; as long as the missing stage come into place, the development potential will be realized. However, practically, such tension is crucial in the industry but difficult to cope with given the fact that it is generally caused by institutional factors, such as resistance of groups with vested interests, government regulations and legal framework.

TDB proves to be useful in contributing to closing the gap between micro and macro analysis, it may give some insight into the complex situation of privacy policy issue where several shareholders are involved. Furthermore, as TDB describes the institutional factors that exist in industry development, it should also lend a support in understanding the e-commerce sector in China. In theorizing the e-commerce business, TDB is implemented at the industry level which consistent with the scale of research method and paradigm of this study. According to Zhu and Janczewski (2016), the theory used should be compatible with the rest of the components of an article regarding the level, such as individual, organizational, industry, or societal, where the research is undertaken. In light of this threefold premise, we employ TDB in an attempt to understand this understudied area as a whole.

As a supplement, we also borrowed SJT as the lens to examine consumers' activities as certain surprising perceptions and behaviors are observed. SJT posits that people tend to use stereotypes to justify and normalize the status differences regarding social dominance. In particular, disadvantaged groups, when influenced by these conventional beliefs, are more likely to accept the status quo while legitimizing the same stereotype beliefs (Mullen et al., 1992; Jost and Hunyady, 2003).

Consumers have long time been implied or told that privacy is a type of property right, which can be transferred for various purposes, such as customized service and better price. However, they were normally treated by the online retailers as a way to dispel consumers' discomfort or emotional unrest regarding their personal data or to rationalize the utilization of consumers' own information. It thus contradicts with the concept that privacy is a civil right that has been

instilled to consumers in the digital era. Facing unprecedented privacy invasion and elusive privacy policies, consumers consequently accept the fact that privacy breach is one facet of the daily life.

Speaking from an industry level perspective, e-commerce sector in China has enjoyed a long-lasting prosperity in both transaction volume and amount, and the business is expected to further develop onto a next stage. When encountering a new requirement from the consumers pertaining to their personal information usage and protection, the online vendors, as deemed by consumers, refrained from specifying the nature of privacy policy, either as a marketing strategy, an advertisement, or a commitment. It hence implies a development potential for consistent and further adoption by consumers, but practically leads to a depressive pressure in stage which is 'premature' in terms of privacy policies as long as the legal enforcement is missing. This creates the so-called 'structural tension' and represents the development block that may fall into the area of government regulations. As such, the premature stage would be stimulant to entrepreneurial activities in the next course once the development block is removed to ease the structural tension. We anticipate that the involvement of legal enforcement on the privacy policies in China's e-business sector will help maintain and increase its robust upwards trend.

IMPLICATIONS AND CONCLUSION

This paper explores the efficacy of privacy policies by introducing the legal perspective as a critical lens through which to examine areas where the legal context affects customers' behaviors and, more broadly, e-commerce. It does so through a qualitative GT approach. The implications of our research are threefold. Empirically, we examined consumers' perceptions regarding the level of information privacy they can expect from the Internet retailers, confirming that there is a mismatch between their concerns and their actual behaviors. Theoretically, by drawing on the grounded theory method, we discovered the development block of legal enforcement that impedes the further development of e-commerce in China while explaining the seemingly conflicting scenario of consumers using price and product variety as the main proxies for online shopping in the context of system justification.

We theorized the rationale of consumers' e-commerce shopping in the legal context and thus identified three factors (Personal unawareness of privacy regulation, Lack of the supervisory

body, and Past experience of privacy breach) that are directly or indirectly brought forward by the legal enforcement. They formulate the ambience of the privacy-deprived e-commerce and are further implicated with other derivatives to justify the contradiction between consumers' perceptions and behaviors of privacy policies. The finding sheds light on why privacy policies in China's e-commerce market have such unexpected impact on consumers' concerns and behaviors. Our research suggests that a lack of legal capability can pose a grave threat to the sound and orderly developments of e-commerce. Thus, the findings underline the need for improved regulation in China regarding privacy and privacy policy. In the absence of such regulation, the e-commerce websites' privacy policies are of limited use because there is no systematic, specific guidance on what information needs to be disclosed to consumers and what commitment(s) online retailers should make. Furthermore, without regulators, it is impossible to evaluate the effectiveness of the privacy policies or to monitor whether the regulations are being strictly enforced.

More importantly, we argue that the absence of the legal enforcement in privacy policies is expected to be a detrimental factor blocking the full-speed and sustainable development in e-commerce sector. The structural tension has to be alleviated by drawing on related legal references before the development potential being realized. A concerted effort among online vendors, consumers, supervisory bodies, and academic scholars to adopt the legal perspective will provide knowledge critical to informing insights relating to privacy policies and how it can best advance e-commerce. It highlights the pivotal role of legal enforcement in sustaining a robust e-commerce trajectory with the introduction of relevant laws in China. To this end, this research supplemented the legal perspective to the existing investigations on privacy policies and exemplified it with a study in the most e-commerce developed market – China.

Practically, the research supports both online retailers and regulators working on privacy policy-related strategies. To be specific, it demonstrates to online retailers the inadequacy of their current privacy policies. On the one hand, many retailers deliberately make their privacy policy difficult to find or word it ambiguously for fear of putting off potential consumers. On the other hand, most consumers would not trust these policies even if they could find them; they dismiss them as either too long to read or too short to be informative. As long as there is no supervisory body to independently monitor or verify the privacy commitments embodied in these e-commerce websites' privacy policies, this attitude is unlikely to change; it will be difficult – if not impossible – to obtain the understanding and trust of online consumers.

Internet retailers themselves also need to act if they want consumers to trust them and their privacy policy. One way China can increase consumer confidence in privacy policies is by appointing a trusted regulatory body such as the China Internet Network Information Center (CNNIC) to protect the interests of online consumers.

The study found that respondents favor those Internet retailers who offer the widest variety of products, the lowest prices, and highest popularity, *regardless of their privacy policy*. However, it should be noted that these views were based on their understanding that privacy policies are self-drafted by Internet retailers. The respondents may have a different view when a privacy policy is verified and approved by a trusted third party such as the CNNIC. They may prefer to buy from an Internet vendor displaying a trust mark, even if they have to pay a premium price. Tsai et al. (2011)'s observation that consumers are willing to pay a premium to purchase from a privacy-protective website suggests that the Internet retailers may be able to leverage privacy protection as a selling point.

Our research is not without limitations. The first concern is over the data source. It was not possible to interview the online merchants involved in the study and, although we made strenuous efforts to understand their privacy policy strategy through various means, we still feel that it is necessary to obtain first-hand information from them. The second limitation relates to the data sample. Potential subjects were identified mainly based on their use of the Alipay and Wechat online payment tools. Although these are the leading online payment tools in China, this may have narrowed the sample unnecessarily. Thus, we would recommend a large-scale study being done across China via a survey based on the findings of this study.

REFERENCES

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015), "Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness", *Journal of Retailing, 91*(1), 34-49.

Aïmeur, E., Lawani, O., & Dalkir, K. (2016), "When changing the look of privacy policies affects user trust: an experimental study", *Computers in Human Behavior, 58*, 368-379.

Anic, I. D., Škare, V., & Milaković, I. K. (2019), "The determinants and effects of online privacy concerns in the context of e-commerce", *Electronic Commerce Research and Applications*, 36, 100868.

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.

Athey, S., Catalini, C., & Tucker, C. (2017). "The digital privacy paradox: Small money, small costs, small talk (No. w23488)", *National Bureau of Economic Research.*

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern", *European Journal of Information Systems*, 24(6), 624-644.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). "Do context and personality matter? Trust and privacy concerns in disclosing private information online", *Information & Management*, 53(1), 1-21.

Barriball, L. K., & While, A. (1994), "Collecting data using a semi‐structured interview: a discussion paper", *Journal of Advanced Nursing, 19*(2), 328-335.

Bélanger, F., & Crossler, R. E. (2011). "Privacy in the digital age: a review of information privacy research in information systems", *MIS Quarterly*, 35(4), 1017-1042.

Bernard, H. R. (1988), *Research methods in cultural anthropology*: Sage Newbury Park, CA.

Bryman, A. (2004), *Triangulation and measurement*. Department of Social Sciences, Loughborough University Loughborough, Leicestershire.

Burck, C. (2005), "Comparing qualitative research methodologies for systemic research: the use of grounded theory, discourse analysis and narrative analysis", *Journal of Family Therapy, 27*(3), 237-262.

CCA. (2018), "Evaluation report on personal information gathering and privacy policies for 100 online applications", Retrieved from http://m.cca.cn/zxsd/detail/28309.html

Chan, W. W. L., & Ma, W. W. K. (2013), "Exploring the influence of social ties and perceived privacy on trust in a social media learning community", *Hybrid Learning and Continuing Education* (pp. 134-144): Springer.

Chellappa, R. K. 2008. "Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security". Unpublished paper, Emory University, Atlanta, GA.

Chen, L. (2009), "Exploring the state of privacy protection policies of Chinese websites", *Library Tribune, 29*(4), 60-64.

CNNIC. (2019), "Statistical Report on Internet Development in China", Retrieved from https://cnnic.com.cn/IDR/ReportDownloads/201911/P020191112538996067898.pdf

Cohen, D., & Crabtree, B. (2006), "Qualitative research guidelines project", Retrieved from http://www.qualres.org/

Dahmén, E, (1988). "Development blocks' in industrial economics", *Scandinavian Economic History Review, 36*(1), 3-14.

Dinev, T., & Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions". *Information Systems Research,* 17(1), 61-80.

Dwyer, C., Hiltz, S., & Passerini, K. (2007), "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", *AMCIS 2007 proceedings,* 339.

Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005), "Examining Internet privacy policies within the context of user privacy values", *IEEE Transactions on Engineering Management, 52*(2), 227-237.

Earp, J. B.; Antón, A. I. and Jarvinen, O. (2002), "A Social, Technical and Legal Framework for Privacy management and Policies", *Proceedings of the Eighth Americas Conference on Information Systems,* Dallas, TX, USA.

Englehardt, S., Eubank, C., Zimmerman, P., Reisman, D., & Narayanan, A. (2014). "Web privacy measurement: Scientific principles, engineering platform, and new results", Manuscript at http://randomwalker.info/publications/WebPrivacyMeasurement.pdf

Fabian, B., Ermakova, T., & Lentz, T. (2017). "Large-scale readability analysis of privacy policies", *Proceedings of the International Conference on Web Intelligence* (pp. 18-25).

Feng, X., & Rong, W. (2007), "Reflections on several issues concerning the legislation of personal data protection", *Journal of South China Normal University (Social Science Edition)* (4), 20-24.

Flavián, C., & Guinalíu, M. (2006), "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site", *Industrial Management & Data Systems, 106*(5), 601-620.

Galanxhi-Janaqi, H., & Nah, F. (2004), "U-commerce: emerging trends and research issues", *Industrial Management & Data Systems, 104*(9), 744-755.

Gao, Z., & O'Sullivan-Gavin, S. (2015), "The development of consumer privacy protection policy in China: a historical review", *Journal of Historical Research in Marketing, 7*(2), 232-255.

Ghayoumi, M. (2016), "Review of security and privacy issues in e-commerce", *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, 156.

Glaser, B. G. (1992), *Emergence vs forcing: Basics of grounded theory analysis*, Sociology Press.

Glaser, B. G. (1998), *Doing grounded theory: Issues and discussions*, Sociology Press.

Glaser, B. G., & Strauss, A. L. (2009), *The discovery of grounded theory: strategies for qualitative research*, Transaction Publishers.

Goulielmos, M. (2004), "Systems development approach: transcending methodology", *Information Systems Journal, 14*(4), 363-386.

Greenleaf, G. (2014), *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, OUP Oxford.

Greenleaf, G., & Livingston, S. (2016) "China's New Cybersecurity Law – Also a Data Privacy Law? 144 UNSWLRS 1

Hekkala, R., & Urquhart, C. (2013), "Everyday power struggles: living in an IOIS project", *European Journal of Information Systems, 22*(1), 76-94.

Hochhauser, M. (2003), "Why patients won't understand their HIPAA privacy notices. Privacy Rights Clearinghouse", Retrieved from https://www.privacyrights.org/blog/why-patients-wont-understand-their-hipaa-privacy-notices-hochhauser

iResearch. (2012), *Personal Internet Security Report*, iResearch

Jost, J. T., Banaji, M. R., & Nosek, B. A. (2004), "A decade of system justification theory: accumulated evidence of conscious and unconscious bolstering of the status quo", *Political Psychology, 25*(6), 881-919.

Jost, J., & Hunyady, O. (2003), "The psychology of system justification and the palliative function of ideology", *European Review of Social Psychology, 13*(1), 111-153.

Kasem-Madani, S., & Meier, M. (2015). „Security and privacy policy languages: a survey, categorization and gap identification", arXiv preprint arXiv:1512.00201.

Kayworth, T.; Brocato, L. and Witten, D. (2005), "What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles", *Communications of the Association for Information Systems*, 16-2005, 110-126.

Kim, S., & Kim, J. (2017), "Impact of privacy concern and institutional trust on privacy decision making: a comparison of e-commerce and location-based service", *Journal of the Korea Industrial Information Systems Research*, 22(1), 69-87.

Le Métayer, D. (2016). "Whom to Trust? Using Technology to Enforce Privacy", *Enforcing Privacy* (pp. 395-437). Springer, Cham.

Lebek, B., Degirmenci, K., and Breitner, M.H. (2013), "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices," *Volume 56 Issue 1, Fall 2015 Journal of Computer Information Systems 9 Proceedings of the 19th Americas Conference on Information Systems*, Chicago: 2013.

Lee Jyh-An, (2018) "Hacking into China's Cybersecurity Law", 53 *Wake Forest Law Review* 57-98

Li, L. (2011), "Research on several issues concerning the crimes of selling and illegal providing personal information", *Journal of Inner Mongolia University (Philosophy and Social Sciences), 43*(5), 113-118.

Li, L., & Xu, W. (2012), "Why has legislation on personal information protection stopped?" *China Youth* (23 May), 5.

Limpf, N., & Voorveld, H. A. (2015). "Mobile location-based advertising: how information privacy concerns influence consumers' attitude and acceptance". *Journal of Interactive Advertising*, 15(2), 111-123.

Lings, B., & Lundell, B. (2005), "On the adaptation of Grounded Theory procedures: insights from the evolution of the 2G method", *Information Technology & People, 18*(3), 196-211.

Liu, C., Marchewka, J. T., & Ku, C. (2004), "American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce", *Journal of Global Information Management (JGIM), 12*(1), 18-40.

Livingston, S., & Greenleaf, G. (2015), "Tort liability for online privacy violations in China: The 2014 SPC Regulation".

Mansell, R. (2017). "Are we losing control?", *Intermedia*, 45(3), 4-7.

Martin, K. D., & Murphy, P. E. (2017). “The role of data privacy in marketing”, *Journal of the Academy of Marketing Science,* 45(2), 135-155.

Martin, P. Y., & Turner, B. A. (1986), “Grounded theory and organizational research”, *The Journal of Applied Behavioral Science, 22*(2), 141-157.

Matavire, R., & Brown, I. (2008), “Investigating the use of grounded theory in information systems research”, Paper presented at the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research In Developing Countries: Riding the Wave of Technology.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006), “Privacy policy statements and consumer willingness to provide personal information”, *Journal of Electronic Commerce in Organizations, 4*(1), 1.

Meng, C. (2011), “Criminal law protection of personal information”, *Journal of Shanxi Politics and Law Institute for Administrators, 24*(2), 85-87.

Milne, G. R., & Culnan, M. J. (2004), “Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices”, *Journal of Interactive Marketing, 18*(3), 15-29.

Mullen, B., Brown, R., & Smith, C. (1992), “Ingroup bias as a function of salience, relevance, and status: an integration”, *European Journal of Social Psychology, 22*(2), 103-122.

Myers, M. D. (1997), “Qualitative research in information systems”, *Management Information Systems Quarterly, 21*(2), 241-242.

Odom, M. D., Kumar, A., & Saunders, L. (2002), “Web assurance seals: how and why they influence consumers' decisions”, *Journal of Information Systems, 16*(2), 231-250.

Oghazi, P., Karlsson, S., Hellström, D., & Hjort, K. (2018). “Online purchase return policy leniency and purchase decision: mediating role of consumer trust”, *Journal of Retailing and Consumer Services,* 41, 190-200.

Ong, R. (2011), “Recognition of the right to privacy on the Internet in China”, *International Data Privacy Law, 1*(3), 172-179.

Orlikowski, W. J. (1993), “CASE tools as organizational change: investigating incremental and radical changes in systems development”, *MIS Quarterly, 17*(3), 309-340.

Pappas, N. (2016). “Marketing strategies, perceived risks, and consumer trust in online buying behavior”, *Journal of Retailing and Consumer Services*, 29, 92-103.

Pernot-Leplay, E(2020), “China’s Approach on Data Privacy Law: A Third Wave Between the U.S. and the E.U.? *Penn State Journal of Law and International Affairs* Vol. 8(1), 51-117.

Pollach, I. (2007), "What's wrong with online privacy policies?" *Communications of the ACM, 50*(9), 103-108.

Qi A., Shao, G., & Zheng W. (2018) "Assessing China's Cybersecurity Law" 34 *Computer Law and Security Review* 1342 -1353.

Qu, Y., Rong, W., Ouyang, Y., Chen, H., & Xiong, Z. (2015), "Social aware mobile payment service popularity analysis: the case of Wechat payment in China", *Advances in Services Computing* (pp. 289-299): Springer.

Reuters. (2019), "Amazon, facing entrenched rivals, says to shut China online store", Retrieved from https://www.reuters.com/article/us-amazon-com-china/amazon-facing-entrenched-rivals-says-to-shut-china-online-store-idUSKCN1RT2A7

Sheng, W. (2019), "One year after GDPR, China strengthens personal data regulations, welcoming dedicated law", Retrieved from https://technode.com/2019/06/19/china-data-protections-law/

Shin, D.-H. (2010), "The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption", *Interacting with Computers, 22*(5), 428-438.

Silva, L., & Backhouse, J. (2003), "The circuits-of-power framework for studying power in institutionalization of information systems", *Journal of the Association for Information Systems, 4*(1), 14.

Smith, H. J., Dinev, T., & Xu, H. (2011). "Information privacy research: an interdisciplinary review". *MIS Quarterly*, 35(4), 989-1016.

STDaily. (2020), "Personal Information Protection Law hammered out this year", Retreived from http://www.stdaily.com/index/kejixinwen/2020-01/09/content_852081.shtml

Strauss, A., & Corbin, J. (1998), *Basics of qualitative research*. Thousand Oaks, CA: Sage Publications.

Sullivan, Y. W., & Kim, D. J. (2018). "Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments", *International Journal of Information Management*, 39, 199-219.

Tang, R. (2002), "Approaches to Privacy--The Hong Kong Experience", *I WAYS, 25*(1), 10-21.

Taylor, C. R. (2004), "Consumer privacy and the market for customer information", *RAND Journal of Economics, 36*(4), 631-650.

Thomson, S. B. (2010), "Grounded Theory - sample size", *Journal of Administration and Governance,* 5(1), 45-52

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011), "The effect of online privacy information on purchasing behavior: an experimental study", *Information Systems Research, 22*(2), 254-268.

Urquhart, C. (2007), "The evolving nature of grounded theory method: the case of the information systems discipline", *The Sage Handbook of Grounded Theory*, 339-359.

Vu, K. P. L., Chambers, V., Garcia, F. P., Creekmur, B., Sulaitis, J., Nelson, D., & Proctor, R. W. (2007). "How users read and comprehend privacy policies". *Symposium on Human Interface and the Management of Information* (pp. 802-811). Springer, Berlin, Heidelberg.

Wang, Z., & Yu, Q. (2015), "Privacy trust crisis of personal data in China in the era of big data: the survey and countermeasures", *Computer Law & Security Review, 31*(6), 782-792.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011), "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems, 20*(3), 267-284.

Warren S.D., & Brandeis L.D, (1890), "The right to privacy", *Harvard Law Review* 4:193–220

Wen, Y. (2013), "A study of the use of personal information and privacy protection in e-commerce", *E-Business Journal, 3*, 37-40.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, 28(3), 889-897.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012), "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior, 28*(3), 889-897.

Xin, C., & Shi, Y. (2009), "New interpretation of concepts in online privacy right", *Journal of Gansu Institute of Political Science and Law* (7), 152-158.

Yang, H. C. (2013), "Young Chinese consumers' social media use, online privacy concerns, and behavioral intents of privacy protection", *International Journal of China Marketing, 4*(1), 82-101.

Yang, H., & Miao, X. (2007), "A study of consumers' trust in bank information practices", *Soft Science, 23*(7), 21-25.

Yao-Huai, L. (2005), "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology, 7*(1), 7-15.

Yu, H., & Wu, X. (1999), "On citizens' privacy right and its legal protection", *The Academic Journal of Anhui Agricultural University (Social Science)* (2), 50-53.

Zhou, S., & Wang, W. (2017), "A comparative study of Chinese and American (e-commerce) website privacy policy – in the case of Alibaba and Amazon", *Journal of Modern Information*, 37(1), 138-142

Zhu, R. (2017). "Pattern, practice, and potency of information systems security research: a methodological perspective". Doctoral dissertation, The University of Auckland, New Zealand

Zhu, R., & Janczewski, L. (2016), "A proposed framework for examining information systems security research: a multilevel perspective", In *Transforming Healthcare Through Information Systems* (pp. 49-61). Springer, Cham.

Zhu, R., & Tao, Y. (2015), "A ten-year longitudinal review of information privacy research from 2005-2014", *25th Workshop on Information Technologies and Systems (WITS)*, Dallas, USA.

APPENDIX

Semi-Structured Interview Plan[8]

I Demographics

Collect the information about interviewees, such as age group, gender, occupation, education, Internet usage (make all data unidentifiable)

II Basic-fact/Warm-up

1. Have you ever heard of information privacy? Do you have any idea about that?
2. Online purchase
   2.1 Which website (in China) do you shop most/second?
   2.2 Think of a time/times when you encounter privacy breach (how often did you have that situation? What was your reaction?)
   2.3 How do you protect yourself from privacy breach?

III E-business Website's Privacy Policy

1. Describe your understanding towards e-business website; privacy policy.
2. Did you ever read/notice privacy policy on the website you frequently shop?
   2.1 Yes: which website(s)? Do you trust it? Why?
   2.2 No: do you think if they have one? (Presenting a sample document of privacy policy) Do you trust it? Why?
3. Purchase behaviour
   3.1 Think about how you do shopping online. Tell us how you make purchase intention
   3.2 Which one would you buy: the website you shop most or the second but with more obvious and thorough privacy policy?

IV Wrap-up

1. What comments or questions do you have for me?
2. Is there anything you would like me to explain? What would you like to tell me that you've thought about during this interview?

[8] The original copy is in Chinese given the fact that the research was undertaken in China.