International Journal for Applied Information Management
Vol. 2, No. 1, April 2022, pp. 34-43

An Exploration into Trust and Privacy Management in a Digital Age

Yue Jer Lin *

Department of Accounting Information, Takming University of Science and Technology Taipei, Taiwan
larry@takming.edu.tw *
* corresponding author

Abstract

This study aims to inspect the effects of the privacy management and realize the relationship between use of trust and the quality of the privacy policy for the sites. This research applied four criteria of notice, access, choice and security that were identified by the FTC as Fair Information Practice to assess 476 websites for the trust and privacy management. Results indicated that approximately 36% of the websites used a trustmark, and that HiTrust/VeriSign was the most commonly used by businesses. The preferred trustmark varied by industry, such as sports sites preferring Verified by VISA, real estate sites preferring SOSA, telecommunication sites preferring HiTrust/VeriSign, and travel sites preferring TWCA. However, BBB Online and TRUSTe were displayed very hardly. The main findings showed that there were no obvious relationships between the use of trust marks and the notice criterion. On the contrary, there were very strong relationships between the use of trust marks and the access and choice criteria for all industries and overall.

Keywords: Privacy Management, Fair Information Practices, Digital Age

1. Introduction

E-business has changed both retail and direct marketing. Customers' lack of confidence regarding the gathering and processing of their private data is affecting the development of e-business. In direct marketing purchasers are conducted through a straight communication network, typically email or telephone. Based on databases existing models try to foretell the buyers that are more likely to reply. Such procedure private information about the shopper is dynamic. However, when personal information is used, sold, gathered, or processed users might feel that their privacy is occupied [28]. Internet use is nearly universal among youth; use risks to internet contain cyberbullying, personnel privacy protection violations and unwelcome solicitation. Internet safety education may prevent these negative consequences; nevertheless, it is indistinct at what age this education should create and what group is responsible for teaching this topic. Meanwhile, internet protection education should activate, as well as knowledge teaching and learning internet safety [16]. The Internet world greatly expands people's opportunities for communication. Space and time are no longer barricades. Friends, acquaintances, or even strangers need no longer live on the same road, in the same region, or in the same town to be in touch. The Internet world concentrates people's capacity to connect in various manners [2]. User web privacy rights remain to be in the attention, have been caught in some uncomfortable privacy mistakes, and concerned customer support groups continue to press for law. The government hoped to pass a related privacy regulation that will give individuals new authorized and technical tools to protect their private privacy [8].

Online privacy begins as a serious issue in an e-commerce environment because of a fundamental tension among business, customer, and government benefits. When people were requested to provide private information, their privacy policy announcement reading behavior was close to their self-report performance. Nevertheless, their personal data presenting manners was different from their self-reported behavior (Won Gyun, 2007) [27]. The WWW is the principal available distributed forceful repository of information, and has undergone enormous and rapid development since its inception. It is significant for successful e-business to have high quality websites [9]. Internet privacy has raised concern with the explosive development of Internet commerce [20]. Privacy concerns will remain important as long as humanity exists. However, the ways violations apparent could rise as people abilities to organize

and control data change over time and the sources of information become more sensitive. People have come to request that privacy and security policies must be included on websites. Successful privacy notices present a significant function in addressing risk issues related to E-commerce. Internet privacy notices are expected to enhance customer choice and reduce the risks of releasing individual information online [22]. On the other hand, these effects result only if customers read and use the information contained in the notices [15].

Trust is vital to E-business, but customers and E-businesses alike are failing to provide ways of ensuring such confidence. Privacy seals have been developed by the E-commerce industry to influence customers' belief that a special website can be trusted [16]. Consumer trust is commonly proclaimed as a crucial factor for the effectiveness of e-commerce [24]. Privacy is a fundamental need and due to an individual propensity to overrun others' privacy, governments are becoming more energetically engaged in studying and legislating information privacy [20]. Concerns about privacy are not new; businesses have been collecting customer information for decades. Nevertheless, with technology and particularly with the development of e-commerce, that increases capabilities for gathering, storage, use and communication of individual data, new encounters to privacy have emerged: personal data about customers can be collected, monitored and shared without their knowledge and they can lose control over the distribution of private information. Meanwhile, trust is significant since it aids consumers to overcome perceptions of uncertainty and risk and engage in "trust-related behaviors" with sellers, such as sharing private information or making purchases [14]. With the growing volume of Internet transactions, privacy concerns between shoppers and vendors have become pronounced [6].

Internet marketing entails numerous approaches, including email marketing, online advertising, and business websites. In every circumstance, privacy concerns are increased. Additionally, at least 30% of the electronic stores listed online security, legal environment, public relations, low rate of investment return, and the frequency of phony credit cards as major problems that inhibited the development of online business [5]. Purchasers tend to think that personal data disclosure is less invasive to their own privacy, and less likely to lead to negative outcomes when they consider that can control when and how such data will release and use. Therefore, customers' Web privacy concerns are likely to be decreased by their perceived ability to control information collection and spreading. Online marketers targeting the consumers shall recognize the influencing factors and address them properly, in order that shoppers' web privacy issues are decreased and they are willing to release private information on the Internet, and join in e-marketing. This is significant, because vendors simply cannot ignore the enormous potential of the e-marketing [23].

2. Literature Review

Internet Privacy is important to personality, enabling us to express ourselves selectively. Use of internet services to support a wide range of profitable and social communications encourage user to share individual data with a more and more varied range of interested parties. Such relations increase susceptibility to privacy violations. Individual information is being used for unsolicited business activity, personality theft, and other deception. The developing range of internet services highpoints the need to improve new rules and metrics, since they pose privacy threats that most of users have no knowledge [25]. The Internet has allowed people to change and increase the way communicate with one another, doing away with some geographical and time obstacles. More significantly, it has changed the way people entree information and expands human knowledge. By the Internet, corporates can sell and connect with consumers. The Internet also allows corporations to categorize and learn about consumer base. Therefore, the Internet has had a certain impact on the way customers and business groups relate to one another, worldwide [13]. Current technology has accelerated people movement to social networking and other online activities. However, the convergence of the online world and life offline is inadequate, immature, and partial. People's habits, customs, and connections are going through deep changes that will have as-yet-unknown effects on them and society all together [2].

Internet privacy is a key concern for users. While privacy was a sensitive matter long before the advent of computers, the phenomenal expansion in E-commerce in recent years has brought privacy anxiety to the fore. Internet privacy relates to positive conduct of the Web site visited by the shopper. Users who suffered previous Internet privacy

invasions may purchase much less than those who didn't suffer any prior online privacy incursion. Also, shoppers with a high degree of Internet privacy concern are more likely to avoid surfing in specific sites for privacy reasons and to decide not to buy products and services online for privacy issues [29]. Users have identical anticipations about private privacy wherever they use the Web, regardless of which portals they visit and the number of places they use. With regards to this, there should be consistent principles to achieve these anticipations throughout Internet commerce. The FTC has a long track record of protecting customer privacy. With the emergence of e-commerce and the expansion of the Internet beginning in the mid-1990s, the FTC focused more on Web privacy concerns [4].

The World Wide Web is the crucial available distributed forceful repository of information, and has undergone enormous and rapid development since its inception. It is significant for successful e-business to have high quality websites. Privacy concerns will remain important as long as humanity exists. However, the ways violations apparent could rise as people's abilities to organize and control data change over time and the sources of information become more sensitive. People have come to request that privacy and security policies must be included on websites. With the growing volume of commerce transacted on the Internet, privacy concerns between shoppers and vendors have become pronounced [22]. Behaviors that were considered invasions of privacy include direct mailings, preference tracking, unnecessary eavesdropping, and outside distributions. These behaviors increase concerns about the improper gaining, use, or retention of private information. Since privacy is strongly related to information protection and usage, privacy policies serve as significant signals in terms of transaction reliability and information safety. Online trust is a vital issue that drives virtual interaction and transactions.

Privacy is a key issue of Internet commerce. Privacy refers to the ability of a personal, group, or organization to control, manage, and decide the extent to which private data is communicated to outside [3]. One significant potential source of information for consumers is a web’s privacy policy. Web policy should transmit to users the privacy regulations and practices adhered to by the institution. Information about the personal data requested by Web and how the sites are designed to provide privacy and security concerns is essential to present a context which can be understood by visitors [18]. Issues regarding customer privacy and the privacy policies of organizations are of crucial concern to users interacting with the web. Consumers are often asked to present private data such as social security and credit card numbers, postal and email. The kind of information requested by Internet, and whether that request is appropriate, may differ depending on the nature of the web [20]. The OECD Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data have played an important role in framing privacy laws around the worldwide. Practices require that personal information must be: a) obtained reasonably and explicitly; b) used only for the original specified purpose; c) adequate, appropriate and not excessive to purpose; d) truthful and up to date; e) available to the subject for review and correction of wrongness; f) kept secure from unauthorized access or expose; and be subject to enforcement instruments.

Hundreds of millions of people all over the world provide private information on the web daily. Many individual data items are regularly submitted by and received from users of commercial sites. The collection and use of this information has become the subject of debate currently on the Internet. The collection and successive secondary use of the information can be regarded as a violation of privacy rights [1]. The US was traditionally known as having a strong culture based on individualism that emphasized independence of each individual within a society. Conversely, Asian culture, for example Taiwan, concentrated more on collectivism and stressed the objectives of the group over personal targets, stressed compliance and in-group concordance, and defined the self-concerning of the group. The individuals from the US and Taiwan may also vary in terms of their awareness, beliefs, and employment of ecommerce. For instance, so as to alleviate uncertainty avoidance, people from Taiwan may need more self-confidence in terms of privacy and security to raise their level of trust when making an online shopping than individuals from the US. [11] [12]. Privacy seals enhance trust in the Internet and anticipates that the site would report to the user of its information practices. It is significant to realize what privacy seals are-and what they are not and the differences between the major seal sources. Seal authorities afford a set of instructions and a voluntary enforcement method to reassure that the web stands by its privacy policy. By clicking on the privacy seal, visitors can test seal authority's Web page to verify validity [18]. The primary impediment to the expansion of B2C commerce by electronic stores seems to be the consumers’ trading habits and the rapid imitation by other stores [12]. Although

credit cards have been commonly used, the security of online credit card usage continued to be perceived as uncertain. Hence, a legal and financial environment that provided a convenient and secure method for online payment seemed to be the most essential factor that contributed to the distribution of B2C e-commerce. B2C e-commerce might not reach full potential until a secure environment has been definitely created [6].

3. Research methods

This study was to examine the quality of trust and privacy management offered by 476 companies. This research focused primarily on whether businesses met FTC guidelines on information privacy and security. This study applied the four FTC criteria (Notice, Choice, Access, Security) into sub-categories to examine if a Website was fully, partially or non-compliant with the criteria. The questionnaire included both realistic information (URLs, link presence, method of trust used) and subjective questions concerning the ease of finding a site's privacy policy, as well as an overall evaluation of the site's privacy policy. The questionnaire was a revision of one performed by the FTC and Ryker et al [14] [24]. This instrument applied the Fair Information Practices (Notice, Choice, Access and Security) presented by the FTC. Every element was subdivided into several particular attributes of the site's privacy and security policy. The primary analysis of this study was based on the industries category. The fair information practices were as follows:

a) Notice: The regulation requires that Websites need to post a privacy policy statement, notice of what information is collected, how the information is used internally and whether the information is distributed to third parties.
b) Choice: This regulation requires an option on using personal data to send information back to Internet users, and disclosure to third parties or statements that these will not be done .
c) Access: Internet users can review, correct, and delete personal information.
d) Security: This regulation requires a statement that steps are taken to "provide security" [7].

In addition, the relationship between trust marks and privacy concerns were also addressed. The percentage of websites displaying each trust mark was computed both overall and for each industry individually. Meanwhile, whether or not there is a relationship between the use of trust marks and the quality of the privacy statement for websites, composites for the notice, access, choice, and security criteria. Then, point-biserial correlations were computed between whether or not a website used a trust mark and scores on the four criteria. The point biserial correlations were computed within each industry and for the combined sample of websites.

3.1. Data Collection

The sample size of this research was based on 476 sites. The researcher assessed Internet privacy and security guidelines' compliance and examined trust marks used by 476 particular business websites that belong to 14 different industries. The selected sample sites currently were based by well-known corporations. Over four hundred sites were visited. A five-point scale was applied to classify each site ranging from very easy to very hard. Meanwhile, another five-point scale was applied to categorize each site ranging from very strong to very weak.

The checklist allowed the researcher to place a check, if the element was found on that site, and the rating scale permitted to rate a particular site's privacy policy using a Likert scale. The chosen Web site required the researcher to visit, assess and attempt to decide the overall evaluation privacy policy for each site. The questionnaire instrument was used to judge and measure the websites.

4. Analysis and discussion of results

4.1. Selected Industries

According to the selected sites survey (Table 1) of the study, there was no "Full" compliance found on "Notice and Security" two measures of this study. Overall, some sites presented both privacy policy and transaction security warranty. Some companies only provided privacy seals without contents. However, some companies even failed to present privacy policies to users. Meanwhile, the primary weakness of the sites was the inability to state what users' information was collected, how data was saved, safe delivered, and released to the outside world. In the main, many industries and enterprises should enhance Web privacy establishment to develop full protection promise for visitors.

Electronics: Fundamentally, most people would like to purchase electronics with traditional transaction style; this seriously impacts web privacy design for this industry. Only a few companies stated users' information safeguard for third parties, transmitted messages to buyers, and how customers were made aware of authorization to distribute data. In the meantime, several firms offered clear announcements of how the company protected their information in transit. In addition, as long as providing Web privacy, companies always allowed consumers to alter individual information. Further, these companies enabled consumers to ask to cease any promotional communications, such as e-paper or advertising. In fact, most traditional big electronics companies were not interested in online shopping. Therefore, they were not overly concerned with Web privacy design.

Insurance: Over 2/3 of the firms presented obvious and complete privacy pronouncements. Furthermore, over half of the companies described how customers' data was conserved, secured in companies systems, and provided safety in-transit. Firms that provided privacy policy always allowed other communications from insurers.

Travel & Hotels: Two-thirds of the sample provided both satisfactory privacy protection and transaction security in-transit guarantee, especially focused on famous companies. Many travel agencies and hotels also defined visibly how visitors corrected, safely, and eliminated individual data. Basically, smaller travel and local hotels were concerned with online advertising only, and ignored Internet privacy. In contrast, most international hotels presented intact privacy promises to visitors.

House Agency: Online transactions are currently not popular for this industry. A lot of agencies of the sample were incapable of offering privacy disclosure. In addition, many sites failed to explain how personal data was delivered, stored inside, and exposed to other organizations in detail. Further, some sites displayed consumers' privacy protection mark only without any contracts. Lastly, over half of the sample merely concentrated on online advertisements rather than web privacy protection.

Sports: The overall situation for selected sites failed to present great compliance, particularly in "Notice and Security". Primarily this is because these sites are created for fun, while customers might not be overly concerned with privacy. Basically, the sites of this industry mainly focused on sports merchandises sale.

Bookstore: Many stores established adequate privacy systems in order to defend online shoppers' personal data to secure current customers and attract more potential consumers. An extremely high degree of compliance was located in this industry. Since the character of the industry, most companies had excellent performance on Choice and Access measure. For example, individual message was saved, shoppers' data changed, removed, continuous communication, and disclosure under consumers' consent or released whenever government requested. In the meantime, some companies only presented transaction security warranty rather than entire privacy policy. There were also large differences for privacy design between companies, although they did provide the policy.

Foods & Beverages: There was not a very wide range of compliance found for this industry. However, the range was over 27% sites reaching partial compliance for "Security" and "Notice". Overall, consumers were not used to buying foods and beverages from the Internet.

Music: Over 30% of the sample reached partial compliance for Notice & Security, because some sites protected users' information released to third parties with obviously statements. On the other hand, only a few sites were concerned with shoppers' willingness to receive further information.

Computers: Mostly, most companies failed to offer enough protection on "Access & Choice", including deciding to accept further communication, or free to change individual information. Alternatively, this industry presented better level of Security detail than other industries.

Car Rentals: Traditionally, online transaction was not prevalent for this industry. Most firms were not interested in creating privacy statements. A small number of the sample built a complete and perfect privacy promise on their sites, such as private information protection, personal data secured, disclosure approval, and safe transmission. Also, few sites permitted visitors to change their personal data. On the whole, there was room for growth in this industry.

Telecommunications: Nearly all the sample displayed visible signs and great descriptions of privacy protection; particularly outstanding performance on Choice and Access criteria. Without customers' approval, companies did not release personal information. Sites also allowed users to change, revise, and cancel their personal data without exception. Some firms provided extra password systems to avoid data being stolen and erased. In order to promote new products, consecutive communications always continued. However, customers could determine whether to receive, and disclose their message to outside world.

Job Bank: Human resource is the primary asset of this service industry. The basic personal information collected included age, sex, marital status, profession, educational background, and e-mail. Most of the sample described full privacy security with noticeable signs. In fact, one company emphasized privacy protection void if personal data was forged. As well, some companies sent e-paper or mail to communicate with members and not shared members' information with others except the laws required. This industry merely disclosed personal information to specific area, companies, or people, not for the public. Thus, they also failed to offer entirely guaranteed protection.

Pharmaceuticals: Nearly all selected sites of the sample failed to define for users how to change personal data, personal willingness to release information, and communication acceptance. Moreover, over 65% companies also did not clearly explain individual data being safely stored, or in transit. In general, there was not good compliance in this industry.

Banks & Investment Securities/Trust: Virtually, these industries constantly provided apparently privacy seals to customers. It was easy to find privacy for many websites. Most of the selected sample of this industry provided consumer information to their subsidiaries companies but not to third parties. Additionally, the majority of companies failed to offer absolute security for consumer's information protection, such as safe in-transit or safe storage in the system.

Table. 1. Ratio Compliance by Industry to Four FIP criteria

Selected Industries	Fair Information Practices Criteria (Access Decision for Compliance)											
	Notice			Choice			Access			Security		
	Full	Partial	Non	Full	Partial	Non	Full	Partial	Non	Full	Partial	Non
Electronics	0%	29%	71%	22%	0%	78%	33%	0%	67%	0%	42%	58%
Insurance	0%	34%	66%	17%	0%	83%	22%	0%	78%	0%	72%	28%
Travels	0%	34%	66%	37%	0%	63%	50%	0%	50%	1%	64%	35%
Real Estate Agency	0%	34%	66%	20%	0%	80%	27%	0%	73%	0%	40%	60%
Sports	0%	34%	66%	4%	0%	96%	5%	0%	95%	0%	10%	90%
Bookstores	0%	34%	66%	27%	0%	73%	36%	0%	64%	0%	46%	54%
Foods	0%	34%	66%	9%	0%	91%	12%	0%	88%	0%	27%	73%
Music	0%	34%	66%	7%	0%	93%	10%	0%	90%	0%	33%	67%
Computers	0%	34%	66%	13%	0%	87%	17%	0%	83%	0%	41%	59%
Car Rentals	0%	34%	66%	38%	0%	62%	50%	0%	50%	0%	50%	50%
Telecommunications	0%	34%	66%	4%	0%	96%	5%	0%	95%	0%	57%	43%
Job Banks	0%	34%	66%	0%	0%	100%	0%	0%	100%	0%	31%	69%
Pharmaceutical	0%	34%	66%	4%	0%	96%	5%	0%	95%	0%	33%	67%
Banks	0%	34%	66%	9%	0%	91%	10%	1%	89%	0%	57%	43%
Total	0%	34%	66%	15%	0%	85%	20%	0%	80%	0%	44%	56%

4.2. Overall Sites Evaluation

The questionnaire mainly contained two vital assessment questions of all selected websites. A five-point scale was employed to classify each site ranging from very easy to very hard. Table 2 indicated the results of two evaluation questions of all sites. On average, about 60% of the sites across industry classifications were regarded as have either very ease or easy to find privacy policy announcements. On the other hand, nearly 30% of the sites failed to provide the privacy policy from this survey. In addition, half of the visited sites offered a hyperlink on the main page to the privacy policy as long as privacy seals were presented. On reviewing the average, about 24% of the sites were evaluated as either very strong or strong. The evaluating ranged from a highest of 43% (Telecommunications) to a lowest zero percent (Car Rentals). Overall, 65% of the sample maintained above the middle of level evaluation. Some industries displayed high rate owing to the few sample size. Furthermore, some websites were easy for locating the privacy policy but provided no contents of privacy promise.

4.3. Trust Marks Assessments

This paper performed a survey with several trust seals that used more frequently from websites, including SOSA, TWCA, TRUSTe, HiTrust/VeriSign, BBB Online, and Verified by VISA. Table 3 contains the percentage of websites

that used each trust mark as a function of industry. According to survey (Table 3), the most repeatedly used trust seal by businesses was HiTrust/VeriSign, particularly in the travel industry of travels, bookstore; while BBB Online was never displayed. In this paper, trust seals are primarily applied by sample sites including the HiTrust/VeriSign, Verified by VISA next, and then used the SOSA and TWCA, respectively. Basically, only 32% companies used trust seals from over 400 sampled websites. In fact, the main reason was shoppers were not actually concerned with online trust, while they were more focused on the price comparatively. Overall, over 98% of the sample focused on the seals, SOSA, HiTrust/VeriSign, and Verified by VISA. Meanwhile, around 95% selected industries did provide trust seals on their websites with different marks. The most repeatedly used by businesses was HiTrust/VeriSign, particularly in the industry of travels, and bookstores. BBB Online was never displayed and TRUSTe was displayed very infrequently. In this study, trust seals primarily applied by sample sites including the HiTrust/VeriSign, Verified by VISA next, and then used the SOSA and TWCA, respectively. Furthermore, different industries always preferred to use varied trust seals, such as all sports sites with Verified by VISA, 40% Real Estate Agency with SOSA, telecommunication concentrated on HiTrust/VeriSign, and nearly over one-third of Travel sites with TWCA seals. No trust seals were used by the industry of Job Banks.

Table 3. Trust Marks Assessment

Selected Industries	Trust Marks					
	SOSA	VeriSign /Hi trust	Verified by Visa	TWCA	TRUSTe	BBB Online
Electronics	12%	28%	21%	0%	0%	0%
Insurance	6%	22%	0%	6%	0%	0%
Travels	17%	30%	14%	37%	0%	0%
Real Estate Agency	40%	5%	0%	0%	0%	0%
Sports	0%	0%	8%	0%	0%	0%
Bookstores	4%	35%	15%	4%	0%	0%
Foods	6%	12%	6%	0%	0%	0%
Music	3%	6%	6%	6%	0%	0%
Computers	9%	13%	11%	0%	4%	0%
Car Rentals	0%	25%	75%	25%	0%	0%
Telecommunications	0%	7%	0%	0%	0%	0%
Job Banks	0%	0%	0%	0%	0%	0%
Pharmaceutical	0%	8%	4%	0%	0%	0%
Banks	3%	14%	0%	3%	0%	0%

4.4. Correlation between privacy statement and trust marks

The inferential statistical analysis was performed to examine the relationships between the Privacy Statement and the Trust marks. Each of the 476 websites was assigned a score of '1' if they used a trust mark and a score of '0' if they did not use a trust mark. To compute scores for notice, access, choice, and security, the following values were assigned for each of the components of each criterion: 1 if the Web site was fully compliant, .5 if the web site was partially compliant and 0 if the website was non-compliant. There are three components to notice, choice, and security, and two components to access. Total scores for notice, access, choice, and security were computed by summing the scores on the components for each criterion. For example, a company with one full compliance component and two partial compliance components for the notice criteria would receive a score of: 1*1 + .5*2 + 0*0 = 2. Or, a company with two partial compliance components and one non-compliance component would receive a score of: 1*0 + .5*2 + 0*1 = 1. To examine the relationships between the four criteria and whether or not a trust mark was included in the website, point-biserial correlations were used. Point-biserial correlations are used to examine the

 ISSN 2776-8007

relationship between a dichotomy (in this case, whether a trust mark was included or not) and a continuous variable (the composite scores for notice, access, choice, and security).

These correlations were computed for the total sample of 476 and for each of the 14 industries. Results of this analysis are shown in Table 4. For the correlations between notice scores and whether or not a trust mark was included on the Web site, most of the correlations could not be computed because the notice scores were the same for each Web site in most industries. The exceptions are the electronics websites and the search sites, for which the correlations were not significant, and for the combined sample of 476 sites, for which the correlation was not statistically significant. For the access score, all of the correlations were perfect (i.e. 1.00) and statistically significant ($p<.05$), and this was also the case for the choice scores (except for banking websites, for which the correlation was .99). This indicates that those sites with a trust mark had higher scores on the access and choice criteria than those sites without a trust mark. Lastly the correlation between whether or not the website had a trust mark and the security score was positive and statistically significant for: (a) real estate; (b) sports; (c) bookstore; (d) food; (e) music; (f) computer; (g) car rental; and (h) for the combined sample. This indicates that for those industries and overall, websites with a trust mark received higher scores on the security criterion.

Table. 4. Relationships between Criteria and Trust Marks

	Criteria			
Selected Industries	Notice	Access	Choice	Security
Electronics	0.21	1.00*	1.008	0.12
Insurance		1.00*	1.00*	0
Travels		1.00*	1.00*	0.21
Real Estate Agency		1.00*	1.00*	.67*
Sports		1.00*	1.00*	.68*
Bookstores		1.00*	1.00*	.72*
Foods		1.00*	1.00*	.55*
Music		1.00*	1.00*	.42*
Computers		1.00*	1.00*	.41*
Car Rentals		1.00*	1.00*	1.00*
Telecommunications		1.00*	1.00*	0.06
Job Banks				
Pharmaceutical		1.00*	1.00*	0.29
Banks		1.00*	.99*	0.31
All Websites	0.05	1.00*	1.00*	.41*

*p<.05.
Note: Point-biserial correlations could not be computed for empty cells because at least one of the two variables was a constant.

5. Conclusion

In spite of potential privacy problems in online social webs, people remain to post all methods of individual information to the internet. In the digital world, personal privacy is basically a misapprehension. The more we use the internet, the more others will know about us. Technology has aided this occurrence and must thus discourse the privacy issues it presents [2]. This research focused on the importance of consumer privacy on the Internet, and applied the Fair Information Practices four norms to assess the degree of compliance for different industries' websites. In fact, there exist considerable discrepancies between industries on privacy protection. Privacy policy characteristics should be designed with the user's viewpoint in mind. The main findings of the research revealed that online privacy may still be regarded as immature for most enterprises. This paper also attempted to examine a

relationship between the use of trust marks and the quality of the privacy statement for websites. This study conducted surveys with several trust seals that used more frequently from Websites, including SOSA, TWCA, TRUSTe, HiTrust/VeriSign, BBB Online, and Verified by VISA. The most repeatedly used by businesses was HiTrust/VeriSign, particularly in the industry of travels, and bookstores. BBB Online was never displayed and TRUSTe was displayed very infrequently. In this study, trust seals were primarily applied by sample sites including the HiTrust/VeriSign, Verified by VISA next, and then used the SOSA and TWCA, respectively. Overall, about 36% of the 476 sampled sites used trust seals.

In fact, the main reason was shoppers were not actually concerned about online trust, while they were more focused on the price comparatively. Overall, over 96% of the sample focused on the seals, SOSA, HiTrust/VeriSign, and Verified by VISA. Meanwhile, around 95% of the selected industries did provide trust seals on their websites with different marks. Additionally, different industries always preferred to use varied trust seals. No trust seals were used by the industry of Job Banks. For the correlations between notice scores and whether or not a trust mark was included on a Web site, most of the correlations could not be computed because the notice scores were the same for each website in most industries. The exceptions are the electronics websites and the search sites, for which the correlations were not significant, and for the combined sample of 476 websites, for which the correlation was not statistically significant. For the access score, those websites with a trust mark had higher scores on the access and choice criteria than those websites without a trust mark. Also, the correlation between whether or not the website had a trust mark and the security score was positive and statistically significant for: (a) real estate; (b) sports; (c) bookstore; (d) food; (e) music; (f) computer; (g) car rental; and (h) for the combined sample. This indicates that for those industries and overall, websites with a trust mark received higher scores on the security criterion. For the most part, many companies shall increasingly endeavor to prepare effective trust and privacy management to protect consumers.

References

[1] Alan, R. P., (2006). Internet Privacy Policies of the Largest International Companies. Journal of Electronic Commerce in Organizations, 4(3), 46-62.

[2] Almeida, Virgilio AF., (2012). Privacy Problems in the Online World, IEEE Internet Computing, 16(2): 4-6.

[3] Chen, Y. H., Chien, S.H., Wu,J.J., & Tsai,P.Y., (2010). Impact of Signals and Experience on Trust and Trusting Behavior. Cyberpsychology, Behavior, and Social Networking, 13(5).

[4] Congressional Documents & Publications., (2010). Consumer Online Privacy: Hearing Summary, Federal Information & News Dispatch, Inc., Lanham.

[5] Dixon, J. H., (2005). Privacy Laws and Doing Business Online. Intellectual Property & Technology Law Journal, 17(2):11-20.

[6] Eastlick, M. A., Sherry L. L, & Patricia W., (2006). Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment, Journal of Business Research, 59: 877-884.

[7] FTC Study., (2000). Privacy online: Fair information practice in the electronic marketplace, a report to Congress, May.

[8] Hane, P. J., (2012). Privacy Issues in a Digital Age. Information Today, Medford 29(4): 10.

[9] Levis, M., Helfert, M. & Brady, M., (2008). Website Design Quality and Form Input Validation: An Empirical Study on Irish Corporate Websites. Journal of Service Science and Management, 1(1): 91-100.

[10] Liu, W. C., (2001). Current status of Taiwan's electronic stores. Taipei: Institute for Information Industry.

[11] 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, 12(1): 18.

[12] Lu, L.C., Rose, G.M., & Blodgett, J.G., (1999). The effects of cultural dimensions on ethical decision making in marketing: an exploratory study. Journal of Business Ethics, 18(1): 91-105.

[13] Lozada, H. R, Kritz, G. H. & Mintu-Wimsatt, A., (2013). The Challenge of Online Privacy to Global Marketers. Journal of Marketing Development and Competitiveness, 7(1): 54-62.[14] Manon, A., Jacques, N., Mathieu, A. D., & Anne, V., (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust, Online Information Review, 31(5): 661.

[14] 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.

[15] Moores, T., (2005). Do consumers understand the role of privacy seals in e-commerce? Association for Computing Machinery. Communications of the ACM, 48(3): 86.

[16] Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D., (2013). Internet safety education for youth: stakeholder perspectives. BMC Public Health, 13(1): 1-6.

[17] Moscato, D. R., (2003). An empirical analysis of web site privacy and security by industry. IACIS: 264-270.

[18] Nora J, R., Robert,L. & Sejung M. C., (2005). Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. The Journal of Consumer Affairs, 39(2): 339-362.

[19] Peslak, A. R., (2005). Internet Privacy Policies: A Review and Survey of the Fortune 50. Information Resources Management Journal, 18(1): 29-41.

[20] Proctor, R. W., Ali, M A. & Vu, K. P. L., (2008). Examining Usability of Web Privacy Policies. International Journal of Human–Computer Interaction, 24 (3): 307–328.

[21] Rapp, J. Hill, R.P., Gaines, J. & Wilson, R. M., (2009). Advertising and Consumer Privacy: Old Practices and New Challenges. Journal of Advertising, 38(4): 51-61.

[22] Soumava, B., (2011). Online Privacy Concerns of Indian Consumers. The International Business & Economics Research Journal, 10(2): 93-100.[24] Tan, F. B. & Southerland, P., (2004). Online Consumer Trust: A Multi-Dimensional Model. Journal of Electronic Commerce in Organizations, 2(3): 40-59.

[23] VO Kayhan & CJ Davis (2016). Situation Privacy Concerns and Antecedent Factors. The Journal of Computer Information Systems, 56(3): 228-237.

[24] Wang, Y. D. & Emurian, H. H., (2005). Trust in E-Commerce: Consideration of Interface Design Factors. Journal of Electronic Commerce in Organizations, 3(4): 42-61.

[25] Won Gyun, N., (2007). An empirical investigation of Internet privacy: Customer behaviour, companies' privacy policy disclosures, and a gap. University of Waterloo (Canada), ProQuest, UMI Dissertations Publishing. NR35149.

[26] Zorotheos, A. & Kafeza, E., (2009). Users' perceptions on privacy and their intention to transact online: a study on Greek internet users. Direct Marketing, 3(2): 139-153.

[27] Zviran, M., (2008). User’s perspectives on privacy web-based applications. The Journal of Computer Information Systems, 48(4): 97-105.