Communications of the IIMA

Volume 13 | Issue 4 Article 7

2013

Privacy Policies on Global Banks' Websites: Does Culture Matter?

Donald R. Moscato
Iona College

Shoshana Altschuller
Iona College

Eric D. Moscato
Iona College

Recommended Citation
Moscato, Donald R.; Altschuller, Shoshana; and Moscato, Eric D. (2013) "Privacy Policies on Global Banks' Websites: Does Culture Matter?," *Communications of the IIMA*: Vol. 13: Iss. 4, Article 7.
DOI: https://doi.org/10.58729/1941-6687.1229
Available at: https://scholarworks.lib.csusb.edu/ciima/vol13/iss4/7

Privacy Policies on Global Banks' Websites: Does Culture Matter?

Donald R. Moscato
Iona College, USA
dmoscato@iona.edu

Shoshana Altschuller
Iona College, USA
saltschuller@iona.edu

Eric D. Moscato
Iona College, USA
emoscato@iona.edu

ABSTRACT

Information privacy, the ability to control the information about oneself, is increasingly relevant as advancing technologies provide opportunities for ever faster and more extensive data collection. Electronic business continues to see the collection and storage of various types of customer information for use in increasingly innovative ways, resulting in enhanced marketing and services as well as concern from the customer about privacy. Online banking, in particular, is strongly impacted by customers' concerns for privacy due to the sensitivity of the information it handles. Previous research has examined privacy concerns, including the impact of culture. This study is a global examination of global banks' privacy policies as promulgated on their websites designed to gain insight into the communication of privacy practices throughout the world. Results indicate that there is a great deal of variation among what is disclosed on banks' websites in different countries.

Keywords: Information privacy, online banking, privacy concern, culture, privacy policies

INTRODUCTION

Recent news reports of U.S. banking trends that include prevalent closings of bank branches (Sidel, 2013a) and increasing usage of mobile banking (Sidel, 2013b) reflect the growing centrality of online services in the banking industry. In fact, statistics confirm that "mobile banking represents roughly 8% of transactions, with online banking at 53% and branches, 14%, according to AlixPartners" (Sidel, 2013a, 2013b, para. 8). According to the American Bankers Association, the number of U.S. banking customers who prefer online banking to any other method has increased from 25 percent to 36 percent in just one year from 2009 to 2010 (American Bankers Association, 2009, 2010). In 2011, the number of Americans who prefer online banking has nearly doubled to 62 percent (American Bankers Association, 2011). A similar phenomenon is occurring world-wide as increasing online banking enables business growth in the developing world (Turban, 2009).

As a convenience for the customer and cost-saving opportunity for banks, it is in everybody's interest to encourage bank users to adopt and commit to new technological channels of conducting business. To this end, much research has been devoted to understanding what prompts and what prevents potential users to engage in online banking. Among the factors considered, concern for privacy has been discussed extensively as one of the major contributors to customers' choice of whether or not to adopt online banking (Lallmahamood, 2007; Lee, 2009; Wang, Wang, Lin, & Tang, 2003).

The current study delves into the issue of information privacy in the online banking environment. The approach taken is a global one in which we explore the portrayal of privacy issue in various regions throughout the world. Much research has shown that feelings toward and perceptions of privacy are intricately tied to personal characteristics and cultural influence. As our discussion below highlights, the understanding and expectations of privacy, and even its presentation in common law is vastly different throughout various regions of the world. It stands to reason that upon this backdrop, policies and attitudes toward privacy by banks and their customers would be impacted by culture as well. It has already been shown that online banking participants approach data security differently throughout the world (Moscato, Altschuller, & Moscato, 2013). This study is an exploration of whether a similar phenomenon extends to information privacy. We first review the relevant literature and then examine the policies of global banks as indicated on their websites. An analysis of the findings as well as insights for customers, banks, and researchers follow.

LITERATURE REVIEW

Information Privacy and E-Business

Information privacy is a complex matter that has been addressed extensively over the last few decades. Although there are a number of definitions for information privacy, information systems researchers have widely accepted it to be defined as the ability to control what happens to the information about oneself (Belanger & Crossler, 2011). Among the topics researched in this field, studies have explored the types and antecedents of privacy concerns and attitudes, their connection with other constructs, and their outcomes (Belanger & Crossler, 2011; H. J. Smith, Dinev, & Xu, 2011). As advancing technologies present opportunities for faster and more extensive data collection and sharing, these issues become intensified. This is particularly relevant to the case of electronic business, which many times depends on the collection, and storage of various customer information for use in increasingly innovative ways. Many studies have addressed this issue, finding that concerns about information privacy indeed affects customers' intention to use online services such that the higher the concern is for privacy, the lower the intention to participate in the business activities (e.g., Belanger, Hiller, & Smith, 2002; Chellappa & Sin, 2005; Eastlick, Lotz, & Warrington, 2006). Banks represent a special case of online business as far as privacy is concerned due to the nature of information being stored and shared during transactions. In fact, similar results have been found specifically for intentions to use online banking (Lallmahamood, 2007; Lee, 2009; Wang et al., 2003).

While it should be pointed out that intentions don't always translate to actions in what is known as the privacy paradox (H. J. Smith et al., 2011), clearly, information privacy is foremost on the minds of online banking patrons and should be addressed accordingly.

Privacy Policies

To allay the concerns of customers, many businesses include on their website a privacy policy disclosing to the public their information practices related to various privacy issues. While government regulation often dictates notification of privacy information directly to bank customers, inclusion of such information on the banks' Websites seems to be at the banks' discretion. In the US, for example, the FDIC, the Fed, and the FCC all delineate very clear rules regarding delivery of privacy notices to customers, when the customer relationship is established, annually, and when there are any privacy changes. Regulations dictate the content of the notices as well as the delivery schedule (Federal Deposit Insurance Corporation, 2001). However, there does not seem to be regulation about what must be disclosed on a banks' Website. Since the Website is publicly available, viewers might be customers or non-customers. Inclusion of a privacy policy on a Website, and its contents would be a choice made by the bank to help portray itself publicly in the most attractive light. The choices made in that regard are the object of this study.

Much research has investigated the usefulness of the addition of a privacy policy to a website. Tsai, Egelman, Cranor and Acquisti (2011) found that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites" (p. 254), concluding that clearly communicating sound privacy practices can lead to business advantage. In addition, displayed, placed and timed properly, privacy information on the website can have significant impact on buying decisions (Egelman, Tsai, Cranor, & Acquisti, 2009). Still, many companies do not include privacy policies at all (Belanger & Crossler, 2011; Liu & Arnett, 2002) and those that do are found to present the information in long and complex verbiage (McDonald, Reeder, Kelley, & Cranor, 2009; Schwaig, Kane, & Storey, 2005) so that they are rarely read and understood (Egelman et al., 2009). Further, privacy policies often do not meet the standards set by the Fair Information Practices (Liu & Arnett, 2002; Yang & Chiu, 2002). Even so, a bank's privacy policy can provide insight into the privacy concerns at the forefront of bank-customer communications, which may or may not reflect the actual practices of the bank, but certainly indicate which concerns the banks feel it important to address.

Most of the research about privacy policies examines only websites of companies within the US, or do not explicitly address differences among policies of different countries (Belanger & Crossler, 2011). In addition, companies outside the U.S. have been said to be less likely to have a privacy policy on their web site (Schwaig et al., 2005; Yang & Chiu, 2002). Belanger and Crossler (2011) suggest that perhaps countries "where governments have long promoted and enforced legal protection for information privacy (e.g., European Union, Hong Kong, Australia, or New Zealand) may be less sensitive to information privacy issues, and therefore organizations in these countries are less likely to view the need for information privacy policies as crucial" (p. 1027). The current study collects and compares worldwide privacy policies to shed some light on national differences among them and the possibility of such explanations.

Information Privacy and Culture

In their expansive review of information privacy literature, Belanger and Crossler (2011) define information privacy as a multi-level construct, noting that empirical studies often focus on only one level. Just as individual factors, such as experiences and inclinations, determine individuals' attitudes about privacy, different countries have different laws and cultures that potentially impact concern for privacy (Belanger & Crossler, 2011). Therefore, we might expect that privacy practices in different countries would not be alike—rather that they would reflect those national differences. In fact, Hsu (2006) found that individuals from different countries "perceive Website categories in different ways, reflecting the influences of political systems" (p. 569). Numerous other studies have also examined information privacy within a geographic region allowing readers to compare outcomes among countries. For example, Dinev et al. (2006) studied privacy concerns in Italy, finding that they are lower as compared to the U.S. but that the relationship between privacy concerns and e-commerce use is weaker as compared to the US. These differences are attributed to disparate cultural norms regarding trust (lower in Italy), personal space (less in Italy), voice communication (more important in Italy), and group orientation (more collectivist in Italy). Similarly, Yang and Chiu (2002) attribute the lower incidence of privacy policies in Taiwan than in the U.S. to differences between the two societies regarding all components of Hofstede's culture theory. For example, since Taiwan is a more collectivist than the US, there is culturally less expectation of individual privacy. In a similar fashion, Mizutani, Dorsey, and Moor (2004) describe diverse manifestations of privacy in Japan and the U.S. and their implications for information privacy on the Internet. In addition, privacy practices in Australia (Belanger & Crossler, 2011; Brown & Muchira, 2004; Drennan, Sullivan, & Previte, 2006) and Asia (Belanger & Crossler, 2011; Tam, 2000; Zhao & He, 2009) have been examined, finding them to diverge from what is expected in the U.S. (Belanger & Crossler, 2011). Clearly, attitudes toward privacy are closely intertwined with culture extending its mark on electronic business accordingly.

Regional differences in the regulatory approach to privacy also stem from the fundamental beliefs within different cultures about privacy. While some cultures ascribe to the belief that privacy is a civil liberty that must always be protected, others view privacy as a commodity that can be valued and traded for benefit (H. J. Smith et al., 2011). These fundamental cultural values translate into laws, policies, and attitudes that are country-specific. Those societies that embrace the human right perspective, such as Australia, Canada, New Zealand, and countries in the European Union, have passed laws that protect privacy across the board. As a civil right, in these countries information is only available to organizations about those customers who have opted-in to the data collection and storage. In contrast, societies, such as the U.S., who view information as a commodity, have disjointed regulation in only some industries and view opting in as unnecessary (H. J. Smith et al., 2011). Thus, there is a direct cultural difference among different countries in their approach to information privacy. We can gain insight into these differences by examining how companies in different countries address the issues related to privacy.

Following, we discuss some of the common information issues and privacy policy features that companies might include on their websites.

PRIVACY ISSUES INVESTIGATED

Separate Security and Privacy Statements

There is no universal agreement among e-commerce companies regarding what to include on the companies' home pages of their web sites. However, it is common practice to discuss both security and privacy somewhere.

The first question to resolve is whether there should be separate disclosure statements regarding both privacy and security. Since these concepts are separate and distinct one could make a strong case that there should be two different disclosure statements. Nevertheless, some companies prefer to aggregate them in one statement that can be anywhere from one page to several pages.

The second issue is the company decision as to whether these statements should be on the home page or buried somewhere that will take the customer several clicks to locate them. Clearly, the more clicks it takes to find them, the less concern the e-commerce company has for the consumer's awareness of those policies.

The third issue is the determination by each company of which content it chooses to disclose to its customers on its web site. Obviously, this is a critically important point to highlight.

Cookies

A cookie is a file that a website can send to its visitors' browsers and may then be stored on their computer's hard drive. The cookie acts as an anonymous tag that identifies a user's computer, but not the user personally.

Cookies have the ability to store information about web pages viewed and the advertisements viewed or clicked. For registered customers, cookies can also save user information and screen preferences (Prudential, 2007). Banks would argue that the use of cookies contributes to better customer service in that the organization can learn from a customer's navigation patterns as they use a particular website. Once this information is analyzed, the bank can redesign its website to facilitate the customer's experiences on the bank's website. A legitimate question to pose is, "Is this a true win-win situation or does it simply enhance the bank's marketing efficiency and effectiveness?"

Pixel Tags

Pixel tags are also known as web bugs, web beacons, clear GIFs, invisible GIFs and "1 by 1" GIFs. According to the Prudential Corporation website disclosure section, a pixel tag "is an invisible tag placed on certain pages of our website but not on your computer. When you access these pages, pixel tags generate a generic notice of that visit. They usually work in conjunction with cookies, registering when a particular computer visits a particular page. If you turn off cookies the pixel tag will simply detect an anonymous website visit" (Prudential, 2007, "What Are Cookies and Pixel tags?, para. 3). Currently concern arises when these pixel tags are embedded in e-mail correspondence. Recent correspondence on the Electronic Frontier website

raises some very important questions on the privacy ramifications of using pixel tags on websites. "Clearly Web-site privacy policies need to disclose the use of Web Bugs as a minimum. Also the general practice of online profiling by third-party ad networks should be talked about in privacy policies. However, this important topic is rarely mentioned" (R. M. Smith, 1999, Advanced Topics, para. 2).

Importance of Website Currency

When consumers surf the web and engage in e-commerce activity, one of the subtle indicators of trust is how often the company updates its content and that it contains up-to-date information that will help the customer make more informed decisions. If a goal of a bank is to build trust, then an obsolete corporate statement(s) on privacy and security will retard rather than enhance this process. Also, with all of the activity surrounding the recent perceived and/or real invasions of privacy, an out-of-date policy statement might be perceived as a negative in the eyes of an aware client of an online bank.

Access to Customer Data

An important element for firms engaged in e-commerce is the ability to cross-market their products to customers. This activity typically involves the collection of consumer's data as part of the initial banking transaction. This data can then be deployed by the bank to its other divisions or affiliates for marketing purposes. Still, the bank might decide to sell selected parts of this data to third parties who would then use the customer information for their own needs. This disclosure can be problematical for the customer who is not aware of, nor condones, this policy by the bank. In the U.S., the Federal Trade Commission is the agency charged with guarding consumer privacy and the Congress is charged with providing the requisite legislation in this matter. In Europe, the Data Protection Act set guidelines for business. The Information Commissioner's Office in the UK discusses what an individual is entitled to under the Act's provisions. "This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available)" (Information Commissioner's Office, 2013a, Access to Personal Data, para. 1).

Identity Theft

If e-commerce by banking institutions is to achieve its lofty predictions for success, it must find a way to earn the trust of the consumer regarding the potential for identity theft. Consumers want to believe that their transactions are safe in transmission and that once the data is resident on the bank's system their personal data will not be compromised. The literature is replete with harrowing stories of people who had their identity stolen and had a very difficult time returning

to normalcy (Roth, Mehta, Boorstin, & Levinstein, 2005). "Pharming and evil twins aren't yet widespread and certainly haven't become the huge problems phishing and spyware are. But they are insidious because they are harder to detect" (Delaney, 2005, para 5). Banks are increasingly making explicit statements on their web pages regarding the steps that they are taking to protect against identity theft. David Myron, editor-in-chief of *Customer Relationship Management*, asserts that "identity theft victims' assurance of security reflects comfort levels with online banking, and not their loyalty to a particular bank" (Myron, 2005, Subtitle).

Despite banks' attempts to improve security in the realm of identity theft, sometimes an embarrassing event occurs. That mentioned in the quotation below is Case Bank and is state owned, with more than 14,200 branches across China:

> A Chinese bank's server is hosting spoofed sites that phishers are using to dupe customers of American banks and e-tailers, a U.K.-based Internet monitoring company said Sunday.
>
> According to Netcraft, this is the first time one bank's network has been used by criminals to steal information from another bank's customers.
>
> The identity theft attack started Saturday when e-mails were sent to Chase Bank customers that directed them to a site hosted on IP addresses assigned to a Shanghai branch of the China Construction Bank Corp. (CCBC). The spoofed Chase and eBay sites were tucked away in hidden directories, and the CCBC's server's main page displayed a configuration error, said Netcraft (Keizer, 2006, paras. 1-3).

The problem of identity theft is worldwide and the number of instances reported is at frightening levels. Consider the case of phishing with a Swedish bank that was the scheme of Russian hackers.

> Russian hackers have used phishing techniques to get hundreds of customers of Sweden's largest bank to divulge their username and password without realizing it, resulting in losses well over $1 million.
>
> 250 [sic] customers have been affected so far, with at least 121 more customer accounts under investigation. The hackers used a phishing email that advised bank customers to download an anti-spam tool that loaded the 'haxdoor.ki' Trojan.
>
> The malware waited until customers tried to log into the online banking service of Nordea, displaying an error message asking the customer to re-enter their data. Once this was done by compliant customers, the crucially sensitive login details were sent to the Russian hackers servers for later use in stealing funds (Zaharov-Reutt, 2007, paras. 1, 3-4).

Many instances of identity theft can be cited as examples. More recently in 2013, there was an alarming incident affecting Europe.

> The malware, in conjunction with the attackers' command and control server, first infected the victims' computers, and then infected their mobile devices in order to intercept SMS messages to bypass the banks' two-factor authentication process.
>
> The theft involved a sophisticated combination of malware directed at computers and mobile devices of banking customers. (Check Point, 2013, para. 2, Key Findings).

Opt In vs. Opt Out

One of the most controversial issues in consumer privacy today is the efficacy surrounding the terms opt-in versus opt out. Anyone who has participated in an e-commerce transaction has been forced to decide which option to choose. Let U.S. first present some definitions. The University of Miami Privacy/Data Protection Project proffers this definition: "It is simple in principle:

- an 'opt in' requires an action or affirmation by an individual for inclusion; the default is exclusion;
- an 'opt out' requires an action or affirmation for exclusion; the default is inclusion" (University of Miami, 2013, opt in vs opt out, para. 1).

A European perspective is provided by the Information Commissioner's Office which is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. "In summary, the precise mechanisms by which valid informed consent is obtained may vary. The crucial consideration is that individuals must fully appreciate that they are consenting and must fully appreciate what they are consenting to" (Information Commissioner's Office, 2013b, p. 6).

Contrast the above with a statement prepared for the U.S. Office of Information Technology Policy by a law firm.

What is Opt-In?

When a company uses opt-in marketing, the consumer must affirmatively give the company permission to send information about new products or sales or to share the consumer's information with other companies in a business relationship with the company where that consumer has an opt-in agreement. Generally, a consumer must click on web site boxes or send an e-mail request to the company, or its affiliates in order to authorize consumer e-mail.

What is Opt-Out?

> When a company uses opt-out marketing, the company privacy policy indicates that the consumer is presumed to want information about sales or new products, and will be sent such information unless the consumer 'opts out' of receiving it. Consumers may also be given the option to opt-out of allowing a company to share the consumer's information with affiliated companies or third parties. Some companies make opting out very simple, using a similar click-box system that other companies use for opt-in agreements, only leaving the default setting as

> 'yes, you may send me information.' Others make it difficult, requiring regular mail or a phone call to remove a person from a marketing list (Leslie Harris & Associates, 2013, para. 3).

It should be clear to the reader that what on the surface appears fairly straightforward, is, in reality, something that can be both misunderstood by the customer and misleading by the company. Online banks must be very attuned to this issue if they are to attain a degree of trust in the mind of the customer.

METHODOLOGY

The focus of this ongoing research project was to explore the disclosure policies of global banks web sites' privacy policies. This particular component is part of a study that has been conducted by the authors for over six years. Two hundred and seventy-five global banks were selected and their web sites were examined by one of the authors during 2011. An English-based review was done for each of the sites. It is important to note that by reviewing actual disclosure policies of these banks we cannot infer whether these banks actually employ some of the policies under review. In addition, the privacy policy does not give U.S. direct information about the expectations or perceptions of potential or actual bank customers. Instead, the focus is only on what is actually disclosed to the consumer. We believe that since the privacy policy is essentially a marketing tool that the bank uses to communicate positive impressions to the public, they will include information that addresses the most likely concerns of their target populations. In this sense, the published privacy policies are a proxy for the privacy issues that are important in the banks' areas of the world. While we do not study actual privacy practices, we expect that banks will learn of common cultural concerns for various aspects of privacy and communicate via the Website how they are being addressed.

For purposes of this analysis the banks were clustered in the following five categories for reporting the results: United States, Canada/Mexico/South America (the Americas), Europe/Australia, Africa and Japan/China (Asia).

In addition to individual area results, a total percentage calculation was also computed. In all but one table, the column headings were the percentage of **yes** responses and the percentage of **no** responses.

Seven privacy issues were investigated. They are as follows:

1. Is there a separate statement on security and privacy?
2. Is there a statement on cookies?
3. Is there a statement on the use of pixel tags?
4. Is there an effective date of the policy specified on the site?
5. Is there a statement on who has access to the data?
6. Is there a statement on identity theft?
7. Is there a statement on the use of either "opt in" or "opt out"?

RESULTS

In this section, we analyze the results of the data for each of the seven questions. Each of the following seven tables reports the percentage of **yes** responses in the second column. The second column shows the percentage of **no** responses. For clarity and purpose of comparison, the row and column order is maintained for the first six questions. The final table adds a third column.

Region	Yes (%)	No (%)	Number
United States	84	16	75
Canada/Mexico/South America	70	30	75
Europe/Australia	64	36	50
Africa	28	72	25
Japan/China	42	58	50
Total Percentages	63	37	275

Table 1: Responses: Is there a separate security and privacy statement?

Almost two-thirds of global banks have references to separate statements for security and privacy. When we look at Table 1, it is quite clear that the groups of African, Japanese and Chinese banks have the opposite response rate from the other area banks. Interestingly, of the three, Japan has the lowest rate. It is not obvious why this is the case. It is a bit of a dilemma.

Region	Yes (%)	No (%)	Number
United States	39	61	75
Canada/Mexico/South America	44	56	75
Europe/Australia	70	30	50
Africa	36	62	25
Japan/China	38	62	50
Total Percentages	45	55	275

Table 2: Responses: Is there a statement on cookies?

From Table 2, Europe and Australia have the highest number of **yes** responses (70 percent) and the group of Africa, Japan and China has the lowest number (37 percent). The other areas reported about 40 percent in the **yes** category.

Overall, the results were 45 percent in the **yes** category and 55 percent in the **no** response area. Even though the extensive use of cookies in e-commerce has been a source of great discussion and debate, it appears that this state has not affected the online global banking environment.

Region	Yes (%)	No (%)	Number
United States	9	91	75
Canada/Mexico/South America	5	95	75
Europe/Australia	4	96	50
Africa	4	96	25
Japan/China	6	94	50
Total Percentages	6	94	275

Table 3: Responses: Is there a use of pixel tags?

From a review of Table 3, it is obvious that global banks do not disclose on their web sites whether they employ pixel tags as part of their online banking strategy. Of all the seven questions in this study, this one had the highest number of **no** as the response.

There are a couple of plausible explanations for this phenomenon. One is that their use is not that well known among consumers in general and, as such, they would not materially benefit by its disclosure by the banks. A second explanation could be that it is not considered a material privacy issue and/or concern by the banks themselves.

Region	Yes (%)	No (%)	Number
United States	15	85	75
Canada/Mexico/South America	11	89	75
Europe/Australia	6	94	50
Africa	8	92	25
Japan/China	18	82	50
Total Percentages	12	88	275

Table 4: Responses: Is there an effective date of policy specified?

A review of Table 4 illustrates the overwhelming response that almost 90 percent of global banks do not specify the effective date of the policy on their home page. These results were consistent across all regions under study.

It is quite common for savvy consumers to seek out the currency of updates to e-commerce companies' web sites in order to gauge the company's attention to maintaining up-to-date information for its customers. Stale data often connotes a sloppiness that can erode a consumer's trust in the overall faith in a company's policies.

Region	Yes (%)	No (%)	Number
United States	43	57	75
Canada/Mexico/South America	15	85	75
Europe/Australia	54	46	50
Africa	32	68	25
Japan/China	62	38	50
Total Percentages	40	60	275

Table 5: Responses: Is there a statement on who has access to the data?

Table 5 shows that the areas of Australia and Japan and China, when disaggregated, have the strongest responses of **yes** to this privacy question. The lowest number was associated with Europe, Canada, Mexico and South America.

Overall, the results show that 48 percent showed a **no** response, while 52 percent showed a **yes** response regarding the statement indicating who has access to customer data of global banks. An explanation might be that this issue is understood via the regions' culture and law as in Europe and other areas.

Region	Yes (%)	No (%)	Number
United States	75	25	75
Canada/Mexico/South America	52	48	75
Europe/Australia	28	72	50
Africa	0	100	25
Japan/China	10	90	50
Total Percentages	41	59	275

Table 6: Responses: Is there a statement on identity theft?

The results from Table 6 show that the U.S. global banks have the highest percentage of **yes** responses (75 percent). A distant second is the group Canada, Mexico and South America. A very low result was found for the cluster from Africa (0), Japan and China (10 percent).

Overall, the results for a **no** response were almost 60 percent, while that of a **yes** response was 41 percent. Clearly, there was a great deal of variability in global banks on this question. The results probably reflect the degree of e-commerce activity present in the respective areas.

With all of this awareness of the critical nature of identity theft, it would imply that companies would be very sensitive to the consumer's fear of becoming a victim when they were conducting online business with them. Therefore, what measures should a reasonable e-commerce provider pursue to enhance consumer confidence? Should each site have a formal statement on identity theft as an integral component of this trust-building process? (Moscato & Moscato, 2008)

Region	Opt Out (%)	Opt In (%)	No Reference (%)	Number
United States	88	12	0	75
Canada/Mexico/South America	9	0	91	75
Europe/Australia	98	2	0	50
Africa	0	100	0	25
Japan/China	88	12	0	50
Total Percentages	60	15	25	275

Table 7: Is there a statement on "opt in" or "opt out"?

For this question, we depart from the tabular presentation of the responses to the other questions. A column entitled **no reference to either** is included. The **opt out** option was the most frequently occurring option. Only 15 percent of the global banks identified **opt in**; and in 25 percent, there was no option specified on the global banks' web sites.

Apparently, there is a long way to go before this choice becomes more favorably disposed in the consumer's favor in the business relationship.

DISCUSSION

The results of this study indicate that there are some privacy features that are more widely discussed by banks in their published policies than others are. Both pixel tags and effective date have universally low rates of occurrence in banks' privacy policies. However, the remaining features are present in relatively many privacy policies. Privacy policies, like their security

counterparts, will portray their privacy measures "in a light that addresses the customers' most likely fears. Thus, the policy can be used as a proxy to gain insight into the bank's perception of its users' most likely concerns" (Moscato & Altschuller, 2012). Seemingly, banks are choosing the contents of their privacy policies to include the issues most obvious and impactful to their users.

The data analyzed in this study also indicate support for the suggestion that privacy is approached differently in different countries around the world. We have seen that for each of the seven privacy concerns, there is often wide variation in the way that banks convey their practices to their customers. It is conceivable that many of these differences depend on cultural and historical differences among the nations. For example, the most varied response is to that of the threat of identity theft. Identity theft, which is most closely associated with credit card use, was found mentioned most within the privacy policies of U.S. banks. Culturally, the U.S. is known to use credit cards much more than many other countries (Holmes, 2011). In addition, there have been many incidences of credit card security breaches and identity theft problems in the U.S. in recent years (e.g., Sidel & Johnson, 2012). Perhaps U.S. banks understand the heightened awareness of the common practice and in response are more likely to ensure their customers about their privacy practices regarding identity theft. In a recent study conducted by Citibank, "respondents in China were quite open to the idea of a credit card serving as a form of personal identification. On the flipside, Australians strongly opposed the idea with 33% strongly disagreeing with the concept" (Citibank, 2007, p. 13). Likewise, our data might be reflecting this association between credit cards and identity—banks in Australia are much more likely to address identity theft issues than Chinese are.

While prior research in information privacy has indicated the possibility of national differences through privacy studies that take place in various countries around the world, this study addresses the issue first-hand by examining and comparing a global sample of banks' privacy policies which are a proxy reflecting the prevalent privacy concerns of the region. The results drawn from an examination of privacy policies relies on the assumption that the policies reflect an accurate picture of customers' actual feelings about privacy. While this assumption limits the results in some way, it depicts a plausible representation of what the regional privacy concerns are based upon how the banks address them. In future research, it would be appropriate to further explore the implications drawn from analysis of the privacy policies.

Implications for the Customer

A major consideration for potential customers in any e-commerce environment is the perception of trust. Trust has several dimensions from the point of view of the consumer. There is trust related to the extent that a company provides adequate levels of security concerning all business transactions. "A Pew Research Study found 73% of respondents considered it an invasion of privacy if a search engine tracked their activity to personalize future search results" (Bussey, 2012, para. 5). "Like it or not, a truism of digital technology is that if information is stored, it will get out . . . ." (Kessler, 2013, para. 3). ". . . 400,000 ATMs that record video of your transactions" (Kessler, 2013, p. 16).

Is the site safe from hackers or identity thieves? Another dimension of trust stems from the consumer's attitude towards privacy of his/her information entrusted to the company. In a global

banking environment, both of these dimensions are particularly relevant. While some customers readily divulge their personal information to their bank in exchange for a service, they often do not expect this information to be shared with other third parties. The degree to which the privacy concern is present may well vary with a culture's attitude toward either the government or business institutions in general. "In August, 2012, a survey by the Public Opinion Foundation showed that 13 percent of Russian citizens use Internet banking" (Titov, 2012, para. 4).

Implications for Future Bank Policies on Privacy

Banks, unlike other businesses engaged in e-commerce activities, are typically held to a higher standard by consumers. This position is the result of the assets of the consumer entrusted to the banking institution. It is not like the purchase of a book online or the purchase of a theater ticket. The magnitude of the commitment is significantly greater in that one's life savings may be at risk. Banks, therefore, must convince a potential e-commerce customer that the e-commerce environment is safe for the consumer to conduct his/her financial transactions. Proper security policies must be in place and followed in order to protect the institutions assets as well as those of its customers. In a similar manner, any bank engaged in e-commerce activities must convince its customers that it respects their privacy as it relates to conducting its business. As we have reported in this study, there is a substantial discrepancy across global banks with respect to how they disclose their policies with respect to privacy of customers' data. Some regions take a more aggressive position on divulging their privacy policies while others apparently do not believe the consumer needs to be informed. One can speculate as to the reasons for the differing attitudes on this seemingly volatile topic in today's e-commerce environment.

Implications for Future Research

There are several unresolved questions after reviewing global banks' privacy disclosure policies that represent fertile areas of potential future research.

Given the worldwide discrepancy noted by this study, we might further explore, how do cultural forces impact a region's privacy disclosure practices? Will there eventually be an evolution to a common policy on privacy as globalization intensifies? If so, who will initiate the movement: Governments, trading blocs or the market itself? In light of a changing global political environment, will new experiences and events change regional perceptions of privacy risk or impede the move toward a common policy? For example, the recent serious attacks that impacted U.S. banks and those in South Korea (PBS, 2013) might compel banks in those regions to modify their privacy policies. "PNC, which acknowledged the attacks, referred to its statement to customers that the bank 'has taken steps to block this [attack] traffic and maintain online and mobile banking access for the vast majority of its customers'" (Gorman & Yadron, 2013, para. 21).

In addition, to best understand the message of the privacy policy and its impact, we need to understand, who is/should be the entity that sets the bank's privacy disclosure policy: lawyers, information technology, marketing or regulators? What might a best practices policy on privacy disclosure policies of a bank be?

As we have said, the policy communicated on the web site does not necessarily reflect the company's actual practices. How can the researcher move from web site privacy disclosure policies (or lack thereof) to the actual practices in place by global banks? Furthermore, if a bank does not have a privacy policy, what does it mean about their practices?

REFERENCES

American Bankers Association. (2009). *ABA survey: Consumers prefer online banking*. Retrieved from http://www.mybanktracker.com/news/2009/09/29/aba-survey-consumers-prefer-online-banking/

American Bankers Association. (2010). *ABA survey shows more consumers prefer online banking.* Retrieved from http://www.prnewswire.com/news-releases/aba-survey-shows-more-consumers-prefer-online-banking-104087868.html

American Bankers Association. (2011). *Popularity of online banking explodes, ABA survey says. ABA Bank Marketing,* 43(9), 37. Retrieved from http://connection.ebscohost.com/c/articles/67236325/popularity-online-banking-explodes-aba-survey-says

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35,* 1017-1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11,* 245-270. doi: 10.1016/S0963-8687(02)00018-5

Brown, M., & Muchira, R. (2004). Investigating the relationship between internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62-70.

Bussey, J. (2012, December 14). Are digital foxes guarding the web's privacy hen house? *The Wall Street Journal,* p. B1.

Check Point Software Technologies, Ltd. (2012, December 5). Media alert: Check Point and Versafe uncover new Eurograbber attack. Retrieved from http://www.checkpoint.com/press/2012/120512-media-alert-cp-versafe-eurograbber-attack.html

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6,* 181-202. Retrieved from http://www.bus.emory.edu/ram/Papers/per_priv_chellappa_sin.pdf

Citibank. (2007, June). Citibank payment evolution report. Retrieved April 29, 2013, from http://www.citibank.com.au/global_docs/pdf/Payment_Evolution_Report.pdf

Delaney, K. J. (2005, May 17). "Evil twins" and "pharming." *The Wall Street Journal,* p. B1.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce: A study of Italy and the United States. *European Journal of Information Systems, 15,* 389-402. doi:10.1057/palgrave.ejis.3000590

Drennan, J., Sullivan, G., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing, 18*(1), 1-22. doi: 10.4018/joeuc.2006010101

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59,* 877-886. doi: 10.1016/j.jbusres.2006.02.006

Egelman, S., Tsai, J., Cranor, L. F., & Acquisti, R. (2009). Timing is everything? The effects of timing and placement of online privacy indicators. In *CHI '09: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paper presented at the Chi Conference on Human Factors in Computing Systems, Boston, MA, April 4-9 (319-328). New York, NY: Association for Computing Machinery.

Federal Deposit Insurance Corporation. (2001). *Privacy rule handbook.* Retrieved December 3, 2013, from http://www.fdic.gov/regulations/examinations/financialprivacy/handbook/

Holmes, T. E. (2011, January 5). How different cultures handle credit cards. *Credit Card News*. Retrieved April 29, 2013, from http://www.creditcards.com/credit-card-news/credit-cards-in-different-cultures-1267.php

Gorman, S., & Yadron, D. (2013, January 16). Banks seek U. S. help on Iran cyberattacks. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424127887324734904578244302923178548

Hsu, C. -W. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review, 30,* 569-586. doi: 10.1108/14684520610706433

Information Commissioner's Office. (2013a). *Access to personal data: In brief--what is an individual entitled to?* Retrieved May 1, 2013, from http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/access_to_personal_data

Information Commissioner's Office. (2013b). *What do opt-in and opt-out mean?* Retrieved May 1, 2013, from http://search.ico.org.uk/ico/search?q=opt+in

Keizer, G. (2006, March 13). Chinese bank hosts phishing site. *InformationWeek.* Retrieved from http://www.informationweek.com/chinese-bank-hosts-phishing-site/d/d-id/1041303?

Kessler, A. (2013, January 3). In the privacy wars, it's ispy vs. gspy: Big brother is watching us. But we are watching back. *The Wall Street Journal,* p. A13.

Lallmahamood, M. (2007). An examination of individual's perceived security and privacy of the internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce, 12*(3), 1.

Lee, M. -C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications, 8*(3), 130-141. doi: 10.1016/j.elerap.2008.11.006

Leslie Harris & Associates. (2013). *The distinction between opt-in and opt-out*. Retrieved May 1, 2013, from http://www.fontanalib.org/Privacy_Tutorial/the%20distinction%20between%20opt.htm

Liu, C., & Arnett, K. P. (2002). An examination of privacy policies in Fortune 500 web sites. *American Journal of Business, 17*(1), 13-22. Retrieved from http://www.bsu.edu/mcobwin/ajb/?p=214

McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009). *A comparative study of online privacy policies and formats.* In I. Goldberg & M. J. Atallah (Eds.), Lecture Notes in Computer Science: Vol. 5672. Privacy Enhancing Technologies (pp. 37-55). Berlin, Germany: Springer. doi: 10.1007/978-3-642-03168-7_3

Mizutani, M., Dorsey, J., & Moor, J. H. (2004). The internet and Japanese conception of privacy. *Ethics and Information Technology, 6*, 121-128. doi: 10.1023/B:ETIN.0000047479.12986.42

Moscato, D., & Altschuller, S. (2012). International perceptions of online banking security concerns. *Communications of the IIMA, 12*(3), 51-64.

Moscato, D., Altschuller, S., & Moscato, E. (2013, January 9-12). Thinking locally about global banks' security policies: A longitudinal comparison. In *Conference Proceedings*. Paper presented at the 12th International Business & Economy Conference, Caen, France, January 9-12.

Moscato, D., & Moscato, E. (2008). Pursuing trust in e-commerce: Are vendors doing enough to build consumer confidence? In *2008 IACIS Conference Program & Referred Proceedings.* Paper presented at the 48th Annual IACIA International Conference, Savannah, GA, October 1-4 (78). Retrieved from http://www.iacis.org/conference/proceedings/IACIS_2008_Proceedings.pdf

Myron, D. (2005, September). Online banking: Consumer trust versus loyalty. *CRM Magazine.* Retrieved from http://www.destinationcrm.com/Articles/PrintArticle.aspx?ArticleID=43284

PBS. (2013, April 1). *South Korea hit hard by massive cyber-attack*. Retrieved April 29, 2013, from http://www.pbs.org/newshour/extra/2013/04/south-korea-hit-hard-by-massive-cyber-attack/

Prudential. (2007). *About cookies and pixel tags*. Retrieved April 17, 2009, from http://www.prudential.com/aboutcookies

Roth, D., & Mehta, S., Boorstin, J., & Levinstein, J. (2005, May 16). The great data heist. *Fortune,151*(10), 66-75.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2005). Privacy, fair information practices and the Fortune 500: The virtual reality of compliance. *ACM SIGMIS Database, 36*(1), 49-63. doi: 10.1145/1047070.1047075

Sidel, R. (2013a, March 31). After years of growth, banks are pruning their branches. *The Wall Street Journal,* p. A1. Retrieved from http://online.wsj.com/news/articles/SB10001424127887323699704578326894146325274

Sidel, R. (2013b, February 12). Banks make smartphone connection. *The Wall Street Journal,* pp. C1, C2. Retrieved from http://online.wsj.com/news/articles/SB10001424127887323511804578298192585478794

Sidel, R., & Johnson, A. R. (2012, March 30). Data breach sparks worry: Hack attack at card processor compromises potentially thousands of accounts. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702303816504577313411294908868

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*, 989-1015.

Smith, R. M. (1999). *The web bug FAQ*. Retrieved September 7, 2007, from http://w2.eff.org/Privacy/Marketing/web_bug.html

Tam, J. C. (2000). Personal data privacy in the Asia Pacific: A real possibility. In *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions*. A paper presented at the 10th Conference on Computers, Freedom and Privacy, Toronto, OH, Canada, April 4-7. doi: 10.1145/332186.332296

Titov, S. (2012, December 10). Online banking gaining wider acceptance. *Russia Beyond the Headlines*. Retrieved from http://rbth.ru/articles/2012/12/10/online_banking_gaining_wider_acceptance_20967.html

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*, 254-268.

Turban, E., Lee, J. K., King, D., Liang, T. P., & Turban, D. (2009). *Electronic commerce: A managerial perspective*. Englewood Cliffs, NJ: Prentice Hall.

University of Miami. (2013). P*rivacy/data protection project*. Retrieved May 1, 2013, from http://privacy.med.miami.edu/glossary/xd_opt_in_out.htm

Wang, Y. -S., Wang, Y. -M., Lin, H. -H., & Tang, T. -I. (2003). Determinants of user acceptance of internet banking: An empirical study. *International Journal of Service Industry Management, 14*, 501-519. doi: 10.1108/09564230310500192

Yang, H. -L., & Chiu, H. -K. (2002). Privacy disclosures of web sites in Taiwan. *Journal of Information Technology Theory and Application*, *4*(3), Article 4.

Zaharov-Reutt, A. (2007, January 20). Swedish bank loses $1 million through Russian hacker phishing attack. *iTWire*. Retrieved from http://www.itwire.com/business-it-news/security/8772-sweish-bank-loses-$1-million-through-russian-hacker-phishing-attack

Zhao, H., & He, M. (2009). Study on social culturology of the Internet sharer. In T. Zhu, J. Yan, & Q. Zhou (Eds.), SWS '09: *1st IEEE Symposium on Web Society*.