An Examination of Privacy Policies of Global University Web Sites

Joanne Kuzma
University of Worcester, Worcester, UK, WR26AJ
j.kuzma@worc.ac.uk

ABSTRACT

Due to demand in online services, universities throughout the world are increasing the content of their Web sites and adding features, such as online applications and e-learning. However, adding online services requires that personal data is kept within computerized systems, thus putting personal private information at risk. Online consumers express concern about the risk of their personal private data and demand to know how organizations will protect their records. It is imperative that firms have mechanisms to guard their data and publish protection information within online privacy policies to mitigate user distrust. However, although industry privacy groups may recommend better protection and some countries may legislate its use; this is not universal in all university sites. This study analyzes 90 universities site throughout the world to determine the use of privacy protection. The results show a lack of use of certain privacy mechanisms. The research suggests methods for improving protection.

Keywords: *Privacy, privacy policies, consumer trust, universities, higher education, cookies, personal data*

1. INTRODUCTION

The higher education industry has found that the Internet is an important method to reach a greater number of students and provide a greater variety of services and information to their stakeholders. However, adding online services brings a myriad of issues, such as how to protect consumer's online personal information. Studies have shown that consumers are concerned with how their data is being used, and what means organisations use to safeguard personal information. Thus, it makes sense for universities to judiciously handle personal data with an appropriate level of protection, and to obey legal mandates on privacy protection. They should also create policies to educate their consumers about the steps firms take to ensure privacy. There were two major aims addressed in this study:

1. What common privacy mechanisms are not being successfully used?
2. Is there any relationship between sites within specific geographic markets in dealing with privacy issues?

The study starts with a literature review of consumer trust, legislation, privacy mechanisms and prior studies in the field. Next, the research methodology is covered, followed by an explanation of the survey results. Finally, implications for the findings are highlighted, along with suggestions for the higher education industry to consider when strengthening their policies.

2. LITERATURE REVIEW

2.1 Privacy and Consumer Trust

The growth the Internet has allowed higher education institutes the ability to reach a wider audience and offer more applications to consumers and staff. To improve their services, universities may collect information about Web users to target their campaigns and better understand demographics. However, the increasing use of Web applications has not come without a growing number of concerns, especially related to online security and personal data privacy. Privacy is increasingly a major concern that prevents Internet users from fully enjoying the convenience, variety, and flexibility offered by online services [1]. A study by Harris Interactive and the Privacy Leadership Initiative found that 40 percent of Internet users claim privacy and security concerns kept them from buying things online [2]. While customers may accept a certain degree of privacy and risk when engaging in online commerce, it is in a firm's best interest to create a climate where Web users perceive that risk levels are reduced, thus increasing the level of trust [3].

Higher education institutions collect vast amounts of personal information, but do little to adequately protect the data and tend not to take privacy and security seriously [4]. New technologies are threatening student privacy and have made this issue more complex [5]. Trustworthy privacy protection can only be attained by a multi-phased approach [1]. Technical solutions are important, but firms must review human, legal and economic perspectives as well to gain the trust of their consumers.

2.2 Privacy Protection, Legislation and Culture

One issue with online privacy protection is that there is no overall global legislation addressing this issue; consumers are faced with a myriad of rules and regulations for each country. While the American opinion is that most online privacy should be voluntary and driven by self-regulation, the Europeans have a stronger legislative direction regarding this issue [6]. In the US, there is no requirement that an online site have a privacy policy, yet other countries, such as the UK, require the privacy policy to be provided before any personal data are collected [7].

Members of the Gulf Corporation Council (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE) currently have no regulations dealing with privacy or privacy issues in general [8]. The Asia-Pacific Cooperation (APEC) Privacy Framework is an approach developed to encourage APEC member economies to develop effective privacy protection of personal information, such as posting privacy policies on Web sites [9]. However, this is merely a framework of privacy policy, and not a legally binding document. The Indian government passed the Information Technology Act of 2000 to provide a regulatory environment for electronic commerce. However, the Act has no provision for protection of personal data [10]. There is no overall Asian consortium on privacy law in Asia, with a myriad of different regulations based on each country [11]. Central privacy enforcement agencies generally have limited power and resources.

The diversity between government regulations may be due to a myriad of reasons. Several authors have argued that cultural values and Internet experiences may contribute to differences among national privacy regulations. Kumaraguru performed a privacy study between US and Indian online users, and found that a basic difference in privacy perceptions between the two countries, with Web users in India having less concern about online privacy and less need for formalized laws in this area [10]. Bellman theorised that differences related to cultural values and desires of political institutions can explain some differences in Internet privacy policies among various nations [12]. The study indicated that consumers in countries with sectoral regulation have less desire for more privacy regulation. The notion of confidentiality and anonymity is uncommon among many Asian cultures, and a patriarchal structure is common. This could affect the overall use of privacy mechanisms by the online Asian community [11].

Although many organizations now post online privacy polices, these organizations must realize that simply posting a privacy policy on their Web site does not guarantee compliance with existing legislation [1]. Jamal found that even with strong privacy laws in the UK, the compliance level with online disclosures is very low [7].

2.3 Web Site Privacy Mechanisms

One of the research questions in this study was to determine which privacy mechanisms were most at risk within university sites. To answer this question first requires a discussion on the various types of privacy tools and methods that are most common within Web sites. Web entities and online marketing firms can often use these mechanisms and technologies to serendipitously collect information about consumers.

One of the most critical privacy needs is the inclusion of a privacy policy within the site, preferably on the home page in order to reassure customers and to help build branding and image [13]. Hooper and Voss [3] corroborate this, indicating that organizations can create a more positive climate by implementing strong privacy policies. Beldad [14] indicates that many people are reluctant to read them due to their length and complicated legalistic nature. The authors also mention that demographics may also be a contributing factor when accessing privacy policies, as older users or those with lower levels of education were more likely to consult privacy statements than younger users or those having higher levels of education,.

One issue with creating an overall online policy is that many are written based on the organization’s legal concerns, rather than addressing the user’s interests [1]. A firm should include a comprehensive policy accessible via the home page and should include information about data collected and PII [15]. Another problem with privacy policies is that although users express their concerns about privacy protection, they often do not bother to read online policies due to a myriad of factors.

Cookies are a technology mechanism that can have an adverse effect on consumer privacy, as they can collect indirect information about users when they are surfing Web sites [16]. One insidious problem with cookies is that not only can the original site collect data, but also third-party sites can use the cookies to gain customer data [16]. Sites may use Web beacons, small electronic files, to keep track of the numbers of users or access information from cookies. Beacons can allow targeted advertisements to be sent to members and can be used to track user’s shopping habits [17].

Coding with a GET command allows information to be retrieved from Web page forms. However, the W3C indicates that GET queries that are unencrypted can be intercepted and easily read, thus creating privacy lapses [18]. The Platform for Privacy Preferences Project (P3P) has other privacy mechanisms that could be included in sites. These are a set of flexible guiding principles and technologies that can be used to maximize privacy and user confidence and trust on the Web. Specific guidelines may be used by different Web sites to indicate to users how data is used on a specific page [19]. Although P3P provides flexible options, Anton [1] indicates that some firms are reluctant to provide P3P policies on their sites because of the possibility they may be misinterpreted.

2.4 Prior Studies

Culnan and Carlin [20] conducted a study of 129 US national doctoral universities and 107 national liberal arts colleges. They collected three types of privacy data: data about actual practices based on an automated software audit (such as third-party cookies), a content analysis to measure the extent to which the online privacy notices reflected fair information practices and readability assessment of privacy notices. Nearly all institutions in the study engaged in online practices that posed a potential privacy risk. Only 36% of schools had a privacy notice that could be accessed from the home page. The researchers also scanned for third-party cookies and found them on only 4% of school sites, indicating this was not a major risk factor in higher educational sites.

Meade [21] reported on security breaches at 38 US colleges and universities in 2008 and 2009, many were caused by careless handling of personal information or data breaches. He attributed one factor contributing to these breaches was the lack of adequate controls and resources dedicated to maintain privacy.

Although a small number of studies have been completed on online privacy issues with higher education, these studies have concentrated on institutions in the US. No comprehensive studies of international universities have been completed at this time, contributing to a lack of research in this area. Thus, the research in this paper contributes to the field and expands the knowledge of privacy issues among universities in a global setting.

3. METHODOLOGY

The research in this paper was accomplished through analyzing 90 university sites in 9 different countries (three geographical areas) to determine the levels of privacy protection. The project consisted of three phases:

1. Choosing a testing tool
2. Choosing sites to test
3. Running the test and analyzing results

3.1 Choosing a testing tool

The first phase of this study was to choose an online privacy testing tool to analyze the sites. Several criteria were important when choosing a tool, the most important being robust testing functionality. It was important that the tool could analyze a variety of privacy factors including privacy policy inclusion, web beacons usage, and third-party links inclusion. The second criteria were to use a product that was either free or minimal cost (under $100) due to budget constraints.

The first tool considered was HiSoftware's Compliance Sheriff Privacy Module. The privacy monitoring and reporting was extremely robust with checks such as privacy statement links and P3P policy reference checks [22]. However, as the software is geared towards the enterprise-wide market instead of individual PC users, its use was deemed as overkill. A second validation product from W3C.org was reviewed. The tool was a free online tester, but was limited in it functionality, such as not providing information on Web beacons [23]. Erigami's software tester, Truwex, was also examined. This is a free online testing product that allows Web site developers to test against privacy rules and industry standards such as:

- Tracking third party content such as Web beacons.
- P3P policy usage.
- PII analysis
- Privacy policy hyperlinks [24]

It should be noted that Erigami also has more robust enterprise-wide products that could be purchased. However, as the 'free' online testing tool had the required functionality required for this research project, it was chosen as the appropriate tool to use.

3.2 Choosing sites to test

The second phase of this project was to select 90 university sites within three geographical regions a) Africa, b) Asia and c) Europe. From each of these three areas, 10 universities from three countries were selected. Several factors were used to choose universities and various countries. First, countries where English was a dominant language in university education was a prime consideration. This would allow easier manual cross-checking of software results. Second, the countries chosen needed to have a viable number of universities to test (at least 10 or more). Countries within each geographical region chosen for testing included:

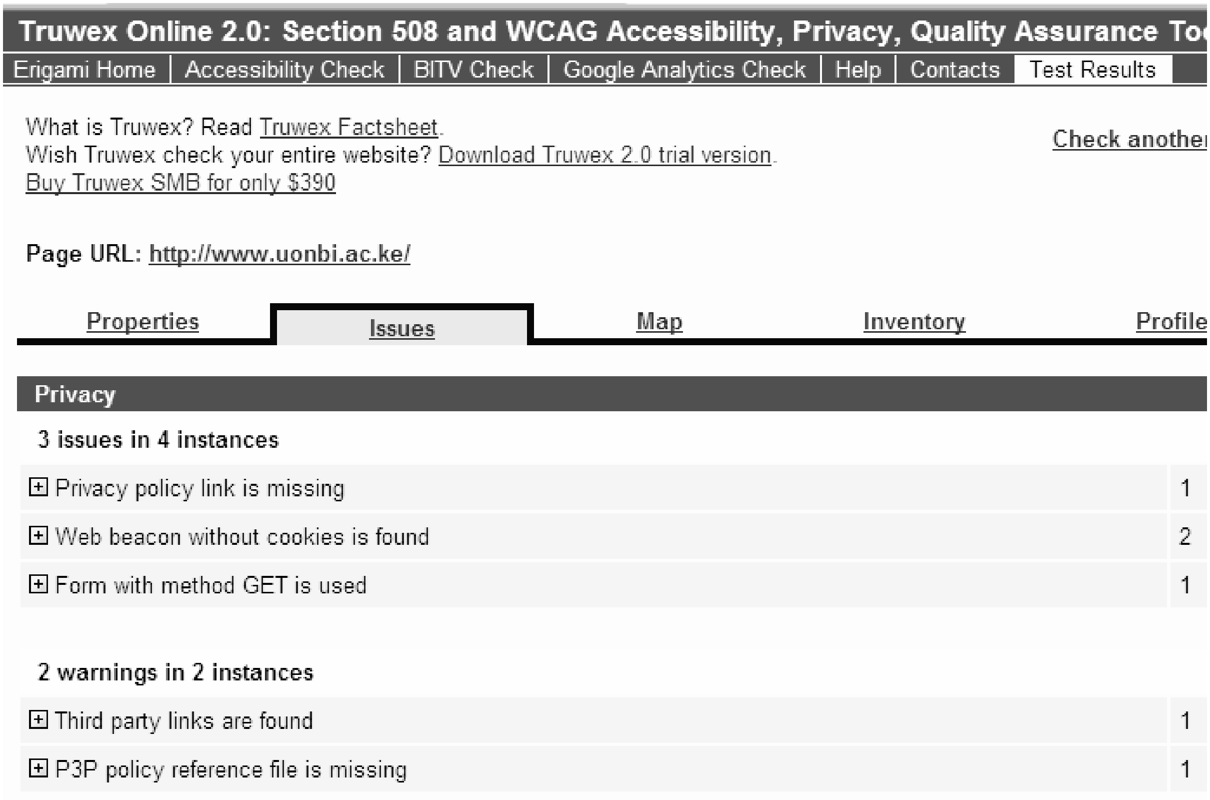
1. Africa (Kenya, South Africa Nigeria)
2. Asia (India, Philippines, Indonesia)
3. Europe (UK, Ireland, Austria)

The firm '4 International Colleges & Universities' (www.4icu.org) is an international higher education search engine and directory reviewing accredited universities throughout 200 countries, and ranking the sites based on Web search popularity rankings [25]. This site was used to choose the 10 top ranked universities for each of the nine countries.

3.3 Running the test and analyzing results

The first phase of using the software was to type the university's home page Uniform Resource Locator (URL) into the 'page URL' box and choose the 'privacy' function option. Truwex then was used to analyze the entire university site for a variety of privacy checks. A report was generated (see Figure 1) which listed problems with the various checks, and is divided into 'serious' problems and 'non-serious' warnings. Although the software tested for a myriad of different privacy checks, not all types of checks were recorded in this research paper due to limitations of space and relevance to this research. Only eight types of checks were recorded; functions such as 'form with GET method' were not collected, although they could be used to expand the scope of future research.

Each of the 90 university sites was tested, and raw data compiled into an Excel spreadsheet. For this test, the researcher encountered two issues. First, the software sometimes indicated that a 'privacy policy link was missing' (see Figure 1). However, a manual search of the site did have a privacy policy page, although this page may have been named something such as 'site information.' The second issue was that for one of the universities, Universitas Negeri Malang (http://www.um.ac.id), the provided URL did not work at the time testing was done, although the site appeared to work several weeks after the original testing. Because of this, another Indonesian university site was substituted for testing.



What is Truwex? Read Truwex Factsheet.
Wish Truwex check your entire website? Download Truwex 2.0 trial version.
Buy Truwex SMB for only $390

Page URL: http://www.uonbi.ac.ke/

Privacy

3 issues in 4 instances

⊞ Privacy policy link is missing	1
⊞ Web beacon without cookies is found	2
⊞ Form with method GET is used	1

2 warnings in 2 instances

⊞ Third party links are found	1
⊞ P3P policy reference file is missing	1

Figure 1: Truwex Screen Print

4. RESULTS

Data for this study was compiled into three worldwide categories. Table 1 shows results of policy data for African universities, Table 2 shows Asian results and Table 3 displays European data. . Each table contains privacy data for three different countries (10 universities per country) related to that category. For each site, eight privacy criteria were compiled:

A. Privacy policy missing
B. Web beacon with cookies found
C. Web beacon without cookies found
D. Third party cookies found
E. PII: page collects personal information identifier
F. Form with method get is used
G. Third party links found (warning)
H. P3P policy reference file missing (warning)

The first six criteria are considered 'critical' privacy issues, and can cause serious problems with privacy protection. The last two criteria (G and H) are merely privacy concern warnings, and are not critical to privacy protection, but designers should still review these issues. For several criteria, only one outcome could be produced for each Web site. For example, column A (privacy policy missing) usually had a result of zero or one for each site, as only one policy is relevant per each university site. For these two columns, some sites (such as University of Pretoria), the Truwex software indicated that a privacy policy (column A) or P3P policy reference file (column H) was missing. However, as the software performed a search of the pages for the term 'privacy policy', this sometimes resulted in incorrect findings. To verify the results of the software scan, the researcher also performed a manual search of the university site. In the example of the University of Pretoria, the privacy information was contained within a page called 'terms and conditions.' Several other sites had various names for their privacy policy: 'terms of use', 'site information,' 'right to information act.' Any site that with this situation was marked with an 'x' in the column and its totals were counted towards the cumulative results for column A.

Results of Table 1 show that 93% of African sites (28 of 30) did not contain a privacy policy (Column A). A P3P policy reference file (Column H) was not present in 97% of sites (29 or 30). Another critical problem for Asian sites was the large number of Web beacons without cookies (89 total in Column C). Nineteen university sites had these Web beacons, with the University of Benin containing the greatest number of problems (35 throughout the site). There were over 136 total third party links found in 26 African university sites (Column G).

A positive result from this data is that only two sites contained Web beacons with cookies (Column B). Also, only two sites had pages that collected PII information (Column E).

Table 2 results show that 83% of Asian sites (25) did not contain a privacy policy (Column A) and 97% did not have a P3P policy reference file (Column H). Like their

African counterparts, a large number of Asian university sites contained Web beacons without cookies and third party links.

The most positive statistics was that only one site had pages that collected PII information (Column E).
Results for the European university sites in Table 3 shows similar results for Columns A, C, H and G. Most sites 56% did not contain a privacy policy, although this result was much better than the results for African (93%) and Asian (83%) universities. This was especially true for Irish universities, where all sites did have a privacy policy.

Table 1: Africa Results

Univ.	Country	A	B	C	D	E	F	G	H
U Nairobi	Kenya	1		2			1	1	1
Jo Kenyatta	Kenya							1	1
Kenyatta U	Kenya	1		2				2	1
Strathmore	Kenya	1		2				1	1
Moi U	Kenya	1							
US Intern.	Kenya	1		1	1	1	1	3	1
Daystar U	Kenya	1						3	1
KCA U	Kenya	1		1				5	1
Kenya Methodist	Kenya	1		2				6	1
Catholic U	Kenya	1						9	1
CapeTown	SA	1	2	11	5			14	1
U Pretoria	SA	x		3				9	1
Stellenbosc	SA	x							1
Witwatersran	SA	1		3				3	1
KwaZulu-Natal	SA			3				2	1
Rhodes U	SA	1		1					1
U SA	SA	x		4				2	1
JBerg	SA	x		2				4	1
Cape Peninsula U	SA	1		2				7	1
N Mandela Met U	SA	x							1
U Lagos	Nigeria	x		2				4	1
U Ilorin	Nigeria	1		1				1	1
U Ibadan	Nigeria	1						2	1
U Benin	Nigeria	1		35				5	1
Lagos State	Nigeria	1						18	1
P. Harcourt	Nigeria	1		10			1	10	1
Federal U Technology, Akure	Nigeria	1		2				7	1
Babcock U	Nigeria	x				1	1	2	1
U of Uyo	Nigeria	1					1	10	1
Redeemer's	Nigeria	1					1	6	1
Total		28	2	89	6	2	6	136	29

Table 2: Asia Results

Univ.	Country	A	B	C	D	E	F	G	H
Indian Ins Bombay	India	x					1	3	1
U Delhi	India	x		1				1	1
Anna U	India	1							1
Indian Ins Delhi	India	1						5	1
Indian Ins	India	1		3			1	8	1
Jawaharla	India	1		2			1	7	1
Amity U	India		3	75	4	1		106	1
Mumbai	India	x					1	2	1
Birla Ins	India	1		2				8	1
U Pune	India	x							1
PhDiliman	Philipp	1	1	1	1		1	3	1
S Tomas	Philipp	1		2				2	1
Los Baños	Philipp	1		2					1
Manila	Philipp	1						3	1
Visayas	Philipp			1				1	1
DeLa Salle	Philipp	1	2	12	4			8	
Ateneo Manila \	Philipp	1		11	1			18	1
Iligan	Philipp			43				22	1
Mapúa	Philipp		1	6	2			5	1
Eastern U	Philipp	1						4	1
InsTeknol	Indon			3	1			5	1
Indonesia	Indon	1		4				8	1
Gadjah	Indon	1		12				6	1
Tek Sepul	Indon	1		5				9	1
Gunadar	Indon	1						1	1
Nusantara	Indon	1		29				39	1
Kristen P	Indon	1					1	1	1
Sebelas M	Indon	1		5				1	1
Sumatera	Indon	1		3			1	5	1
Pendidika	Indon	1		2			1	4	1
Total		25	7	224	13	1	8	282	29

Table 3: European Results

Univ.	Country	A	B	C	D	E	F	G	H
Cambridge	UK			3			1	6	1
Oxford	UK	1		6					1
Imp London	UK	1		3				2	1
U C London	UK			3				1	1
Manchester	UK		1	7	2		1	2	1
UEdinburgh	UK			2			1	1	1
U Leeds	UK			1			1	1	1
Nottingham	UK								
London Sch Econ	UK	x		3				1	1
U York	UK	x		2			1	1	1
UCollege Dublin	Ireland			2				11	1
Trinity	Ireland			2			1	7	1
UCollege Cork	Ireland		1	7	4			4	1
Dublin City	Ireland			6				8	1
Nat U Galway	Ireland			2			1	4	1
U Limerick	Ireland			1			1	1	1
Dublin Ins Tech	Ireland	x		3				6	1
Nat U Maynooth	Ireland			4				42	1
Royal C of Surgeons	Ireland	x		2	1		1	1	1
Waterford	Ireland	x		3				4	1
UWien	Austria	1		3				4	1
TechU Wien	Austria	1						3	1
Innsbruck	Austria	1					1	5	1
Graz	Austria	1					1	3	1
U Linz	Austria	x							
Bodenkultur Wien	Austria	1					2		1
Alpen-Adria-U	Austria	x	1	8	1		1	11	1
Salzburg	Austria	1		6				1	1

Medizinische U Wien	Austria	x							1
Musik Kunst Graz	Austria	x						1	1
Total		17	3	76	8	0	14	125	27

5. IMPLICATIONS AND RECOMMENDATIONS

This paper had two research aims, with the first to determine which common privacy mechanisms were not being successfully used. The research showed that for many of the African and Asian sites, privacy policies were not utilized, although European sites did better. Two of the most challenging issues were the vast number of pages and overall numbers for web beacons without cookies and third party links. Other privacy mechanisms did not have as serious issues regarding the number of occurrences.

The second aim of this study was to determine if there was any relationship between sites of different geographical markets in dealing with privacy issues. For the results, the most obvious different in results was the number of sites in Europe (especially the UK and Ireland) that did have privacy policies on their sites, compared to the majority of universities in Africa and Asia which did not. This result was especially telling, as the legal mandates in the UK and the EU are relatively strong concerning the requirement for privacy, and privacy policies. However, even with strong EU mandates, the Austrian universities (and some from the UK and Ireland) did not have policies. Thus, it may be inferred from this study that strong legal mandates may result in a more positive adherence to privacy protection, but it is no guarantee that laws are being met.

Privacy protection is a multi-dimensional issue and requires site owners to understand a myriad of issues and possible protection mechanisms. Bellman suggests that privacy policies and protection is dependent upon individual areas. Site managers should select a range of options at the regional or country level and personalize privacy policy preferences based on law and culture of that area [12]. Privacy protection encompasses a collaboration of people in a wide variety of areas in higher education: alumni relations, registration, legal affairs, and marketing [5]. When compiling their privacy policy and protection mechanisms, all these departments should be consulted for a wider range of protection. It is recommended that all sites have privacy policies, but they be customized based on legal, organizational and other factors. A second recommendation to site owners is that better training needs to be implemented in order to understand the legal requirements, and to periodically review their site for adherence to the legal mandates.

Several aspects of the study could be expanded into further research. First, the types of privacy mechanisms tested could be increased and different types could be reviewed. For example, the use of mail-to links, long-life persistent cookies and PII collection of age could be reviewed. A robust cross-reference between specific country-based laws and privacy could also add to the research in this area. For example, the US has a specific privacy law to protect children – Children's Online Privacy Protection Act (COPPA) of 1998 – which sets rules for online collection of children [16]. Specific laws such as these could be analyzed. It would be useful to determine the reasons why sites do not implement strong privacy protection. A future phase of the research could be to contact each of the universities to ask the reasons why policies and strong privacy is not followed, and if the same recurring reasons exist for each institution.

6. CONCLUSION

With the number of universities throughout the world growing and adding more services on their Web sites, the collection of personal information in their databases will grow. This creates privacy concerns for consumers who utilize the sites, and studies have shown that online users are consistently concerned with how their information is being used and protected. Although some countries have enacted laws to protect privacy, this study has shown that legal mandates do not always translate into strict enforcement. Also, there is a wide range of privacy mechanisms, but little consistency with how universities enforce individual protection with each of these mechanisms. Some areas of the world have better privacy protection than others. This paper indicates that university site owners have a great deal of work to do in order to address their consumer's privacy needs and should take greater steps to enforce laws and industry guidelines.

REFERENCES

[1] A. Anton, E. Bertino, N. Li, and T. Yu, "A roadmap for comprehensive online privacy policy management", *Communications of the ACM*, 2007, Vol. 50, No. 7, pp. 109-116.

[2] M. Desai, T. Richards, and K. Desai, "E-commerce policies and customer privacy", *Information Management & Computer Security*, 2003, Vol. 11, No. 1, pp. 19-27.

[3] T. Hooper and M. Vos, "Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices", *Online Information Review*, 2009, Vol 33, No. 2, pp. 343-361.

[4] F. Cate, "The Privacy and Security Policy Vacuum in Higher Education", *Educause Review*, 2006, Vol. 41, No. 5, pp. 19-28.

[5] M. O'Donnell and C. Parker "How Colleges Can Navigate the Thicket of Federal Regulations", *Chronicle of Higher Education*, 2005, Vol. 51, No. 38.

[6] C. Gurau, A. Ranchhod and C. Gauzente, "To legislate or not to legislate": a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites", *Journal of Consumer Marketing*, 2003, Vol. 20, No. 7, pp.652 – 664.

[7] Jamal, K., Maier, M. and Sunder, S. (2005), "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom" *Journal of Accounting Research*, Vol. 43, No. 1, pp. 73-96.

[8] Z. Shalhoub, "Trust, privacy and security in electronic business: the case of the CGG countries", *Information Management & Computer Security*, 2006, Vol. 14, No. 3, pp. 270-283.

[9] Asia-Pacific Economic Cooperation (APEC), "APEC Privacy Framework", 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[10] P. Kumaraguru, L. Cranor, and E. Newton, E. "Privacy Perceptions in India and the United States: An Interview Study", In The 33rd Research Conference on Communication, Information and Internet Policy (TPRC), Sep 23 - Sep 25, 2005, The National Center for Technology and Law, George Mason University School of Law, USA. Available at: http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf.

[11] J. Tam, "Personal data privacy in the Asia Pacific: a real possibility", Proceedings of the tenth conference on Computers, freedom and privacy, April 4-7, 2000, Toronto, ON, Canada.

[12] S. Bellman, E. Johnson, S. Kobrin and G. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers", *The Information Society*, 2004, Vol. 20, No. 5, pp. 313-314.

[13] S. McRobb S. and Rogerson, "Are they really listening? an investigation into published online privacy policies at the beginning of the third millennium", *Information Technology & People*, 2004, Vol. 17, No. 4, pp. 442-461.

[14] A. Beldad, M. deJong, and M. Steehouder, M. "Reading the least read? Indicators of user's intention to consult privacy statements on municipal websites", *Government Information Quarterly*, 2010, Vol. 27, No. 3, pp. 238-244.

[15] M. Bhasin, "Guarding Privacy on the Internet", *Global Business Review*, 2006,Vol. 7, No. 1, pp. 137-156.

[16] N. Bowie and K. Jamal, "Privacy Rights on the Internet, Self Regulation or Government Regulation", *Business Ethics Quarterly*, 2006, Vol. 16, No. 3, pp. 323-342.

[17] Nielsen Company, "Global Faces and Networked Places: A Nielsen report on Social Networking's New Global Footprint", March 2009, http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf. niels

[18] W3C, "The World Wide Web Security FAQ", 2003, http://www.w3.org/Security/Faq/wwwsf4.html.

[19] W3C, "Make Your Web Site P3P Compliant", 2002, http://www.w3.org/P3P/details.html.

[20] M. Culnan and T. Carlin, "Online privacy practices in higher education: making the grade?", *Communications of the ACM*, 2009, Vol. 52, No. 3, pp. 126-130.

[21] M. Meade, "Data Security and Privacy at Colleges and Universities", *The Computer & Internet Lawyer*, 2009, Vol. 26, No. 10, pp. 26-31.

[22] HiSoftware, "HiSoftware Compliance Sheriff Privacy Module", 2011, http://www.hisoftware.com/solutions/hisoftware-compliance-sheriff/privacy-reports.aspx.

[23] W3C, "P3P Validator", 2011 http://www.w3.org/P3P/validator.html.

[24] Erigami, "Compliance monitoring of a corporate website: accessibility, privacy, quality, interactive activity", 2011, http://www.erigami.com/truwex/accessibility-privacy-monitoring.html.

[25] 4ICU, "4ICU About Us", 2011, http://www.4icu.org/menu/about.htm,