An Examination of Privacy Policies of U.S. Government Senate Web Sites

Joanne Kuzma*

Worcester Business School
University of Worcester
Henwick Grove
Worcester, WR2 6AJ, UK
Phone: 01905 542023 email: j.kuzma@worc.ac.uk
*Corresponding author

Abstract: U.S. Government Web sites are rapidly increasing the services they offer, but users express concerns about their personal privacy protection. To earn user's trust, these sites must show that personal data is protected, and the sites contain explicit privacy policies. This research studied privacy policy protection of 50 U.S. Senate sites and found that few had comprehensive elements of privacy policies and a general lack of protection of personal data that could be obtain from the Web site. The study reviewed which specific privacy elements are most often mishandled, as well as suggestions for improving an overall online privacy practice.

Keywords: electronic government; e-government; privacy policies; privacy; consumer trust; cookies; personal data.

Biographical Notes: Joanne Kuzma is a Senior Lecturer in Computing at the Worcester Business School, University of Worcester, UK. She received her Ph.D. in Information Systems from Nova Southeastern University. Her research interests include: e-business, e-government, privacy issues and computer security.

1 Introduction

Considerable progress has been made in the types of services offered by U.S. e-government sites, including those of the members of the U.S. Senate. However, despite the potential advantages these services bring to online users, there are major challenges government Web owners face when designing their sites to protect the personal privacy of visitors. Studies have shown American consumers are very concerned about their privacy and personal information protection when they visit Web sites, so it makes sense for site owners to judiciously handle consumer personal data with a high level of protection. Besides voluntarily complying with industry privacy guideline design, sites also need to obey various legislation affecting privacy requirements.

However, despite legal mandates and industry tenants on privacy protection, many government sites are not fully protecting Web visitor data. This research analyses the level of privacy protection among 50 U.S. Senate Web sites. The results show that these sites are not fully compliant with U.S. privacy laws, and many of the sites do not even have basic safeguards, such as lack of a privacy policy link on their site. The results of the research serve to as a reason for Web owners to review their privacy policies for completeness. It also lists various suggestions on how site designers can improve their

privacy practice. Although this research was aimed at issues with U.S. government sites, privacy issues and suggestions for improvement can be applied to other government sites. Additional research can be taken to analyse sites within developed and developing countries to determine their level of privacy protection as well as specific improvements those governments could implement.

2 Discussion on Privacy, Trust and Implementation

2.1 Privacy and Consumer Trust

U.S. federal government Web sites offer Americans the ability to conduct business and access information about government offerings, resulting in more convenience for users. In order to improve services, government agencies creating these sites often collect information about their users to better target their market. However, this data collection has created concerns among consumers who are apprehensive about the amount of data collected, especially when it is collected without their consent (Rose, 2000). According to West (2001), public opinion places privacy concerns near the top of the list of citizen concerns about electronic government formats, and having a visible privacy statement is a valuable tool for reassuring consumers and leading to better trust of services. A study of international e-government usage by Tang (et al., 2009) found that trust of consumers has a direct influence on usage of e-government sites. According to Sheng and Trimi (2008), disclosing critical information such as personal or tax data via new technologies makes citizens more concerned about privacy issues. This concern and the increasing use of data collection has necessitated federal and state governments to adopt privacy laws, as well as individual sites adopting industry best practice policies to protect consumer information. According to Calzolari & Pavan (2001), the future of online commerce depends on the trust users have on the way the information is stored, collected and disclosed to other parties, and improving trust implies increasing the costs associated with misuse of private information. This is something that legislation will address in order to improve trust and protect private personal information. Legislation to protect privacy is important to consumers, with a 2003 study by Turow indicating that "consumers want legislation that will help them easily gain access to and control over all information collected about them online" (Turow, 2003). Also, government information technology managers should make privacy a factor and adequately address this issue when forming their information policy initiatives (Ghapanchi, et al., 2008).

A U.S. Federal Trade Commission (FTC) study of general American Web sites in 2000 found that 99% of sites collected personal information and only 20% of the sample routinely observed fair information practices (overall guidelines to which firms should adhere to when conducting business) (U.S. Federal Trade Commission, 2000). Another FTC study in 2001 found that of 85 of the busiest Web sites, fewer had collected as much personal information than in the prior three years. Also, fewer were utilizing third party cookies and more were utilizing privacy notices (Adkinson, Eisenach, & Lenard, 2002). An analysis done in 2000 and 2001 of 1,813 federal and state government sites found that only 28 percent had some form of privacy policy on their site (West, 2001). Another study by Becker (2004) of 40 government sites found that most privacy policies lack the type of content to promote consumer trust, and the reading complexity of policies posed significant barriers to consumer understanding of the policies.

2.2 Privacy Protection

In the U.S., there is no overall federal policy protecting all online privacy, although some legislation and best practices guidelines are in place to offer some protection for certain classes of consumers and across certain industries. However, unless consumers fall within a specific protected class where they do have some legal protection, guidelines are merely voluntary for sites. One voluntary set of privacy guidelines has been established by the FTC. They have identified four key Fair Information Privacy (FIP) principles that Web sites should adhere to:

- Notice – Consumers should be provided clear notice of information practices, information collection, and how sites use information.
- Choice – Consumers should be offered a choice on how their information is used.
- Access – Consumers should be reasonable access to their personal information and correct inaccuracies.
- Security – Sites should take reasonable steps to protect consumer's personal information. (U.S. Federal Trade Commission, 2000).

The 2000 FTC study concluded that it is imperative that a combination of both legislation and voluntary self-regulation be in effect to provide maximum online privacy protection (U.S. Federal Trade Commission, 2000).

Several federal privacy laws have been enacted that protect some consumer groups. The health care industry and the financial services industry are governed by the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) respectively, providing privacy protection for consumers in these industries (Bowie and Jamal, 2006). In December 1999, President Clinton issued a memorandum on Electronic Government which required all federal agencies to develop and post privacy policies on their Web sites. In addition, in June 1999, the Office of Management and Budget (OMB) issues guidelines for agencies in designing the privacy portion of their sites, and in 2000 directed federal agencies to limit the use of cookies (Hiller & Belanger, 2001). By September 1, 1999, federal agencies were to post privacy policies on their Web sites, and by December 1, 1999, site were to add privacy policies to any other known, major entry points to the sites as well as at any Web page where the agency collected substantial personal information from the public. Each policy was to have clear language to inform site visitors what information the agency collects about individuals, why the agency collects it, and how the agency would use it (Office of Management and Budget, 1999). Consumer privacy protection on government Web sites was further strengthened by the E-Government Act of 2002. This Act requires the government to set standards and improve methods on how they assure protection of personal information of Web site visitors, and to explain to visitors what information is being collected, how it is being used and how it is maintained (National Archives, 2002).

Although e-government sites do not specially target their content towards an audience of children, as opposed to some specific retail sites, government site owners should realize the possibility that their site could be accessed by children. According to Liu and Arnett (2002), more than twenty-five million children in the U.S. are on the Internet, therefore site owners should more actively address privacy protection related to children. Congress passed the Children's Online Privacy Protection Act (COPPA) in 1998, setting rules for online collection of information on children (Bowie and Jamal, 2006). It requires online sites to secure parental consent before collect personal information from children under 13, and also forbids release of such information if it has been collected (Bhasin, 2006).

2.3 Web Site Privacy Implementation

There are several methods companies can implement to provide more effective online privacy protection. Bhasin (2006) explains that one way for consumers to be knowledgeable about dealing with a specific Web site is to view their privacy policy statement. This document is usually accessible through a link on the home page and should discuss the privacy policy elements of the Web site, including information about data collected and how they use personally identifiable information (PII). Privacy policies across industries contain the same overall structure, although specific elements and statements will differ among entities based on their specific business or service provided.

A comprehensive privacy policy should contain disclosures on specific technology and PII collection. One important disclosure would be information on the use of cookies for the site. According to Bowie and Jamal (2006) cookies are a type of technology that can collect indirect information about a user as a Web site is browsed. The authors explain that not only can the original Web site collect data, but third-party sites are also able to gain information about the person visiting the site. Without disclosure on the site's privacy policy, consumers would not know if their Web surfing or PII is being collected when they use a specific site. Turow (2003) indicates that 40 % of Web surfers are unaware that cookies are a key component of data retrieval and this technology is used to track online actions.

Pages that collect data without the ability for consumers to opt-in or opt-out are another concern in the privacy arena. The legal definition of opt-out is that an entity that intends to share non-public information must give consumers the opportunity to deny them permission to do so, or opt-out (Lacker, 2002). Thus, consumers can decide whether to accept or reject the ability for firms who plan to share the information or use it for internal/secondary purposes. According to Degryse and Bouckaert (2006), in the U.S., those industries where laws currently require individuals be given a choice, the opt-out option is most commonly used. For example, the 1999 Gramm-Leach-Bliley Act for financial institutions requires that consumers be given the possibility to opt-out when the institution shares non-public information. A study by Liu & Arnett (2002) showed that 53.3% of Fortune 500 Web sites with privacy policies did not address opt-out concerns. As opposed to opt-out, the opt-in alternative permits the use of personal data within a firm, but first requires opt-in consent before information is disclosed to third-parties (Degryse and Bouckaert, 2006). The authors also state that most studies show that consumer's opt-in rate is very low.

Pages should have a link to the Platform for Privacy Preferences (P3P). P3P provides a standardized set of best practices to describe a site's privacy practices that can be that can be retrieved automatically and interpreted easily by user agents. Sites which implement P3P policies make their practice explicit and available for consumers to easily review (W3C, 2007). A privacy factor surveyed in this research study was the use of the 'GET' method when using forms. Pages that collect PII using the GET method of form submission may introduce vulnerabilities, as the information may be visible during collection (IBM, 2007). Other site features can cause privacy issues for consumers, especially factors related to third party collection of data. Lawton (2002) explains that there are a variety of ways that third parties can collect data, such as Web beacons, links and mail-to features. Because it is difficult for the original site to control what the third party site does with data, use of these elements should be avoided.

3 Methodology

The research was accomplished through completing an analysis of 50 U.S. Senate sites to determine adherence to privacy policy guidelines and to determine the most prevalent problems for these sites. The project consisted of four phases:

Title

1. Choosing an online testing tool
2. Picking a list of US Senate sites to test
3. Run a software analysis
4. Perform an in-depth analysis on the results

The first phase of this study was to choose an online privacy testing tool to analyse the sites. For this study, a software product from Erigami, called Truwex, was chosen. This product is an online testing tool that Web developers can use to develop Web pages that apply to industry standards or regulations such as COPPA or privacy information rules of the US Gramm-Leach-Bliley Act privacy rules. It matches privacy items in the Internet Explorer browser and contains a set of rules which reveal issues with gathering, using and storing private information such as:

- Tracking third party content such as cookies and Web beacons.
- Visitor tracking by cookies and Web beacons.
- P3P policy usage.
- PII analysis such as Web forms that collect names
- Compliance with COPPA laws
- Privacy policy hyperlinks (Erigami, 2008a)

The designer types the Uniform Resource Locator (URL) of the Web site to be tested into a selection box, and can choose to analyse the site based on one or several of the various privacy checkpoints. The tester then receives a detailed compliance report on whether the site meets or fails the test, along with the numbers of errors or warnings per page. (Erigami Home Page, 2008a). The software analyses the pages and produces a diagnostic report on the number of detected errors and warnings where the site is not in compliance with specific privacy standards and regulations. Errors are defined as serious non-compliance problems that should be fixed in order to be in compliance with the standards, such as P3P. Warnings are informational message about possible problems, but are not critical to meeting standards (Erigami, 2008c). This software has been used by other researchers to analyse government Web sites. In the spring of 2008, the Government of Saskatchewan, Canada used Truwex 2.0 to evaluate perform Web accessibility testing (Wu, 2008).

The second phase of the project involved choosing a list of government sites in order to analyse their adherence to privacy guidelines. Although a myriad of agencies exist among the three branches of government, this study involved analysing Web sites of the U.S. Senate. There are 100 members in the Senate, and 50 Web sites were chosen from the register of Senate Web sites at http://www.senate.gov/. Since each state has two members of Congress appointed, and one member from each state was randomly chosen for evaluation. These Senate sites were chosen for evaluation because they are considered federal Web sites, thus under jurisdiction of privacy legislation of OMB and the E-Government Act of 2002. This study was taken to determine if the owners of these sites adhere to their own mandated laws.

During February 2009, the third phase was completed and this consisted of analysing the sites using the Truwex tool to determine the main types of online privacy checkpoint problems. For each government site, the software tool tabulated various privacy errors and warnings. For each checkpoint type, a government site could then have a various number of errors per page. Within a specific checkpoint, the results could have a wide range of numbers of problems. Some sites could have no errors, while others could contain a large number of issues per page. For example, one of the privacy factors to be tested is to determine if the site uses Web beacons. The Truwex software report would produce a report listing if the page contained Web beacons and how many specific

beacons on that page. The fourth phase of this study was to take the raw data from the Truwex results and to compile it into tabular format. The total numbers of errors for each checkpoint was tabulated.

4 Results

The tables in this section show the resulting privacy errors and warnings for the 50 Congressional sites, with Table 1 containing the critical privacy errors and Table 2 listing minor privacy warnings. For each table, the first column provides a list of the descriptions of either errors or warnings. The second column displays the count of the total number of home pages that had errors or warnings. Since 50 home pages were tested, the maximum value for this column is 50. The final column lists the total number of specific errors or warnings for all pages. In some cases, each home page could contain many instances of a specific issue, so the maximum number could be significantly higher than 50. For example, the error 'privacy policy link is missing' is a type that can only have one specific instance per page. Alternatively, the specific warning 'third party links are found' could have a different quantity for each page.

Results in Table 1 show that the two most common errors on individual pages are 'Form with method GET is used', (30 pages with this error) and 'Privacy policy link is missing,' (23 pages with this error), showing a high propensity for these problems. This indicates that over half of Senate sites are not adhering to these policy guidelines. In addition, the majority of pages contain a series of PII collection data. Thirty pages each contain the following PII problems: a) Page collects PII, b) Page collects PII and opt-in/opt-out inputs are missing, c) COPPA: Page collects PII and does not ask parent email, and d) COPPA: Page collects PII and has no kid's privacy policy link. The total error count column showed 'Web beacons without cookies' (44 total errors) was the most prevalent error in terms of total quantity. This was followed by 'Form with method GET is used' (34 total errors) and lack of privacy policy link (23 errors) were the other two common problems.

Table 1 Number of Privacy Errors

Error Types	*Pages with errors*	*Total error count*
Privacy policy link is missing	23	23
Web beacon with cookies is found	1	1
Web beacon without cookies is found	10	44
Third-party cookies are found	2	3
Cookie blocked by IE is found	1	2
Mailto link is used	4	4
Form with method GET is used	30	34
PII: Page collects PII	15	15
PII: Page collects PII and opt-in/opt-out inputs are missing	15	15
PII: COPPA: Page collects PII and does not ask parent email	15	15
PII: COPPA: Page collects PII and has no kids privacy	15	15

policy link		
PII: Page collects age revealing information	1	1

Table 2 is a compilation of privacy warnings, which are issues that should be addressed, but are not serious issues. Ninety-eight percent of home pages did not contain a P3P policy reference file, only one site did have this file. Over half of the sites (26 total pages) had third party links, with a total of 140 warnings for this problem.

Table 2 Number of Privacy Warnings

Warning Types	*Pages with warnings*	*Total warning count*
P3P policy reference file is missing	49	49
Third party links are found	26	140

5 Implications and Recommendations

The purpose of this study was to determine the level of privacy policy protection gaps for users of federal Senate Web sites. There existed a considerable variation in the kinds and amount of errors and warnings, with some types only showing on one site with other problems found in almost all pages. Data obtained from the survey of 50 sites showed a disappointing aspect to the study, that only approximately half the sites (54%) provided a policy link on their home page. Most of the sites (60%) had forms with method GET, about half (52%) had third party links and all but one had a missing P3P policy reference file. Also, one-third of the sites had personal policy information problems: a) page collects age data, b) page collects PII, c) COPPA: page collects PII and does not ask parent email and d) COPPA: page collects PII and has no kid's privacy policy link. Smaller numbers of issues were found for Web beacons, mail-to and cookie issues.

According to Bhasin (2006), the OMB memorandum for federal agencies requires these entities to follow certain privacy principles, such as not using cookies on their Web sites. However, even with this mandate, the study showed that some federal sites are still using cookies. Third-party cookies were found on two sites, and one site had a cookie blocked by IE. This is a small percentage of sites using cookies, but it still indicates that legal mandates are not followed.

Fifteen of the fifty sites had one of two different COPPA issues; either the page does not ask parent email it has no children's privacy policy link. Although it is possible that some children could access the site, the main business practice of these government sites is not geared towards children. However, it is still advisable for government sites to comply with COPPA law in lieu of the possibility children could access the site and the site would gather children's personal data.

A serious implication of privacy policy implementation is the issue of why sites do not implement effective privacy policies, or even do not include any privacy information on their site. One study done by Liu and Arnett (2002) addressed this problem. They surveyed almost 500 Fortune 500 Web sites, and those without a privacy policy were selected for a more detailed study. The Webmasters of these sites were sent an email asking why the business did not have a privacy policy on the home page. Most businesses did respond to this inquiry, and the three main reasons sites did not post a policy on the home page were: a) the policy was in development, b) a policy appears in an appropriate

place of the home page of the business's subsidiary and c) there is no strong need to have a policy because customer contact is limited. A subsequent follow-up could be conducted with the Senate sites to determine if the same reasoning exists for government site owners compared to Fortune 500 sites.

Future research in this field should address consumer attitudes towards privacy policy elements within the sites. A study to understand which elements the users find most helpful and relevant would help site owners to determine if specific elements should or should not be addressed within the policy. Although it would be assumed that FIP principles would be important to Web users, a study in 2005 found that FIP principles were not valued highly by Internet users (Earp, et.al, 2005). In addition, research could be expanded to other areas of e-government to determine if a difference in the level of privacy protection exists between sites of the members of the U.S. Senate versus other federal and state government entities. In addition, a potential weakness of this research was that it was limited to U.S. government sites. Further studies could analyse other government sites throughout the world to determine if government sites in those countries have the same issues as those within this study. A further study would be especially useful for e-government sites in developing nations, as these are a prime area for growth. Choudrie (et al, 2009) indicate that government Web sites of developing countries are pertinent to more studies because they form a 'large part of e-government efforts occurring on a global scale.' Also, suggestions for improvement of e-government sites may differ somewhat in specific countries based upon their own national or local privacy laws. A final suggestion for further study would be to differentiate between privacy inclusion among different national and local government agencies to see if federal sites or those based in larger metropolitan areas. A study of Vietnamese e-government sites found that in general, sites in larger cities and provinces had better content services and consumer satisfaction (Tsai, et al., 2009). It would be interesting to determine if this also correlates with privacy issues as well.

Because of the rise in consumer awareness of privacy issues, as well as an increasing number of American consumers using e-government sites, it is helpful for consumers to understand not only the legal policy legislation, but to also understand which sites are actually meeting the legal requirements and industry guidelines for privacy issues. Additional efforts need to be made by owners of e-government sites to address privacy protection for their users. This study has shown that legal mandates or industry guidelines alone do not guarantee adherence to full privacy protection, therefore, implementing a comprehensive privacy practice must follow a multi-dimensional approach. The first recommendation is that all consumer and government sites, not just the Senate sites found in this study, need to develop and include a link to a privacy policy. Second, privacy policies must include a series of comprehensive elements to fully cover and protect consumer's personal data. Specific elements may differ depending upon the type of business or services the business or government entity takes part in. For example, a health care Web site policy would be customized to meet stricter standards to comply with HIPAA legislation. A site catering to children may develop a more comprehensive set of rules related to opt-in and opt-opt for children under the age of 13 to comply with COPPA law. Third, site designers must understand the legal requirements for their specific industry. Government sites should comply with OMB guidelines and the E-government Act when implementing Web privacy design. Finally, no matter what category of industry the site is in, periodic reviews of the policy in relation to the firm and updated legislation or industry guidelines should be enforced.

6 Conclusion

With the rise in the number of e-government Web sites, consumers have the opportunity to access an ever-increasing range of information and services. However, in order to gain the trust of consumers in using these sites, the site owners must address issues related to protecting consumer's personal information.

There has been a greater concern among consumers with regards to how their data is protected and what information is collected by online sites. In addition, some laws have been enacted to address some of these issues for certain industries, and certain federal policies, such as OMB guidelines, do address privacy with federal Web sites. However, despite these factors, there are still major challenges for e-government sites fully protecting personal information. This study has shown that a subset of federal sites, U.S. Senate sites are inadequate in fully protecting their Web visitors. Guidelines do exist for the site designers to implement, as well as legal mandates to protect consumers. However, the results show that most of the sites contain a variety of privacy errors and warnings, and nearly all sites do not even have a functional privacy policy. The research show that these site owners still have work to do in addressing the privacy needs of their Web users, and should take steps to follow laws and industry guidelines.

References

Adkinson, W., Eisenach, J., & Lenard, T. (2002, March). 'Privacy online: A report on the information practices and policies of commercial Web sites.' *The Progress & Freedom Foundation.* Available online at: http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf (accessed on 9 February 2009).

Becker, S. (2004) 'A usability study of internet privacy policies for state and commercial websites', *International Journal of Services and Standards*, Vol. 1, No. 1, pp. 52-68.

Bhasin, M. (2006) 'Guarding Privacy on the Internet', *Global Business Review*, 7(1), 137-156.

Bowie, N. & Jamal, K. (2006) 'Privacy Rights on the Internet, Self Regulation or Government Regulation', *Business Ethics Quarterly*, Vol. 16, No. 3, pp. 323-342.

Calzolari, G. & Pavan, A. (2001) 'Optimal Design of Privacy Policies', Technical Report, Gremaq, University of Toulouse and Northwestern University, Available online at: http://www.unicatt.it/seminaridelmartedi/seminari20002001/pp.pdf (accessed on 12 February 2009).

Choudrie, J., Wisal, J. & Ghinea, G. (2009) 'Evaluating the usability of developing countries' e-government sites: a user perspective', *Electronic Government, An International Journal'*, Vol 6, No. 3, pp. 265-281.

Earp, J., Anton, A., Aiman-Smith, L., & Stufflebeam, W. (2005) 'Examining Internet Privacy Policies Within the Context of User Privacy Values', *IEEE Transactions on Engineering Management*, 52(2), pp. 227-237.

Degryse, H. & Bouckaert, J. (2006) 'Opt In versus Opt Out: A Free-Entry Analysis of Privacy Policies', September 2006. CESifo Working Paper Series No. 1831, CentER Discussion Paper No. 2006-96. Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=939511 (accessed on 14 February 2009).

Erigami (2008a) 'Compliance monitoring of a corporate website: accessibility, privacy, quality, interacti ve activity', Available online at: http://www.erigami.com/truwex/accessibility-privacy-monitoring.html (accessed on 20 February 2009).

Erigami (2008b) 'Erigami Home Page', Available online at: http://www.erigami.com/ (accessed on 2 February 2009).

Erigami (2008c) 'Quality Issues Description', Available online at: http://www.erigami.com/pagecheck/Truwex-Online-Issues-Help.htm (accessed on 2 February 2009).

Ghapanchi, A., Albadvi, A., & Zarei, B. (2008) 'A framework for e-government planning and implementation', *Electronic Government, An International Journal'*, Vol 5, No. 1, pp. 71-90.

Hiller, J. & Belanger, F. (2001) 'Privacy Strategies for Electronic Government', *The PricewaterhouseCoopers Endowment for the Business of Government.* Ed. M. A. Abramson and G. E. Means, Rowman & Littlefield Publishers, Lanham, Maryland, pp 162-198. Available online at: http://www.businessofgovernment.org/pdfs/HillerReport.pdf (accessed on 19 February 2009).

IBM (2007) 'IBM Rational Policy Tester', Available online at: ftp://ftp.software.ibm.com/software/rational/web/datasheets/r_ds_policytester.pdf (accessed on 19 February 2009).

Lacker, J. (2002) 'The economics of financial privacy: To opt out or opt in?', *Economic Quarterly*, Vol. 88, No. 3, pp. 1-16.

Lawton, G., (2002). 'Invasive Software: Who's Inside Your Computer', *Technology News*. July 2002, pp. 15-18.

Liu, C. & Arnett, K. (2002) 'An Examination of Privacy Policies in Fortune 500 Web Sites', *Mid-American Journal of Business*. Spring 2002, Vol. 17, No. 1, pp. 13-21.

National Archives (2002) 'E-Government Act of 2002', Available online at: http://www.archives.gov/about/laws/egov-act-section-207.html (accessed on 25 February 2009).

Office of Management and Budget (1999) 'Memorandum for the Heads of Executive Departments and Agencies, Privacy Policies on Federal Web Sites,' Available online at: http://georgewbush-whitehouse.archives.gov/omb/memoranda/m99-18.html (accessed on 26 February 2009).

Rose, E. (2000, June). 'Balancing Internet marketing needs with consumer concerns: A property rights framework', *ACM SIGCAS Computers and Society*, *30*(2), 20-24.

Sheng, H. & Trimi, S. (2008) 'M-government:technologies, applications and challenges', *Electronic Government, An International Journal'*, Vol 5, No. 1, pp. 1-18.

Tang, H., Chung, S., Weng Se, C. (2009) 'Examining the impact of possible antecedents on service usage: an empirical study on Macao e-government', *Electronic Government, An International Journal'*, Vol 6, No. 1, pp. 97-109.

Tsai, W., Purkbokusumo, Y., Cheng, J., Duc Tuan, N. (2009) 'E-government evaluation: the case of Vietnam's provincial websites', *Electronic Government, An International Journal'*, Vol 6, No. 1, pp. 41-53.

Turow, J. (2003) 'Americans and Online Privacy: The System is Broken', Report of the Annenberg Public Policy Center, Available online at: http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf (accessed on 9 February 2009).

U.S. Federal Trade Commission (2000). 'Privacy online: Fair information practices in the electronic marketplace: A report to Congress', *Washington: The Commission*. Available online at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (accessed on 9 February 2009).

West, D. (2001) 'State and Federal E-Government in the United States, 2001', *Inside Politics*, Available online at: http://www.insidepolitics.org/policyreports.html (accessed on 13 February 2009).

Wu, M. (2008) How Accessible is Government of Saskatchewan Website, *Presentation to CMPT 480 Accessible Computing*. Available online at:

http://www.cs.usask.ca/classes/480/t2/Shawn%20presentation.ppt (accessed on 27 February 2009).

W3C: (2007) 'Enabling smarter Privacy Tools for the Web'. Available online at: http://www.w3.org/P3P/ (accessed on 1 February 2009).