Web enabled enhanced Electronic Service and Privacy Breach

Sandra J. Leonetti
Lakehead University, Thunder Bay, Canada
sjleonet@lakeheadu.ca

ABSTRACT: *The web based electonic service over the years have scaled the technology to reach the sections of the society and Government. The enhanced Electronic Service Delivery (ESD) has proved to reduce the cost and at the same time ensure effective service to the society. There remains a concern that the use of web technology increases one's risk to breach of privacy. A privacy breach, where information may be improperly released, can be catastrophic to an individual's identify and to the government's image of trust. This study reviewed that the critical web based defences designed by the government to fend off web attacks that may threaten the privacy of citizens when they use web enabled services. Hence to address this issue we have iniated discussion on strategies where users can deploy in order to ensure they protect their own privacy.*

Keywords: Web services, Electronic Government, Electronic Service Deilvery

Received: 19 October 2010, Revised 27 November 2010, Accepted 3 December 2010

1. Introduction

Since the inception of the computer, the internet has served the growing appetite of Ontarians access to public services. Ontarians now demand access to government services in a convenient and effective manner.

The value of public sector online sales increased over 30% from $3.4 billion to over $4.5 billion in 2007 [14]. Growth has been rapid over the past decade, which can be attributed to a major federal initiative that began in over a decade ago in 1999, called the "Canadian Government Online", which worked with the objective to provide common government services online [5].

This report will elaborate on what is meant by ESD and privacy, and will highlight the importance the government has placed on ensuring privacy in an electronic environment. This requires a discussion of six key critical privacy defences utilized by the Ontario government, which demonstrates the government's prudence toward privacy protection. Finally, a brief discussion will elaborate on two strategies that ESD *users* can adopt to ensure that they too protect their privacy.

1.1. What is Electronic Service Delivery (ESD)?

ESD involves the use of one or more electronic services channels (i.e. automated telephone, kiosk service, and internet or public access terminals) to provide simultaneous single window access to a variety of government services. The following discussion will focus on ESD through the internet.

As an example of how Ontario leaders have embraced technology, in 2005 the first ever "service guarantee" for birth certificate services online was introduced. Under some conditions, this service promises delivery of a birth certificate within 15 days – or your money back. This online service request requires customers to provide personal information such as the

names, date of birth, place of birth, and other sensitive identifying personal information, in order to issue a correct document to the entitled person [11].

Since 2005, Ontario has expanded its electronic service offering to residents, which include renewal of driver licence stickers, applications for death or marriage certificates, registration for a newborn, access to property assessment information or the ability to update one's home address [11].

ESD is important because it has served as the catalyst to enhanced government services. It underpins the Ontario Public Sector (OPS) service directive, set a decade ago, where modernization has refocused the attention towards efficient, effective and high quality public service [8].

1.2. What is privacy?

Privacy is important because as humans, we tend to define ourselves by information about us. For example, our age, hair colour, income, parental history, place of work, or number of siblings. As humans, we value this information differently and privacy is something we all need at some level and to some degree [4]. We choose when we want to share personal information with others, understanding there may be consequences by doing so. Within an electronic service delivery environment, privacy is one's willingness to disclose personal information online. Such information may include personal family details, which may suggest or indicate information about personal behaviour, thus, privacy appeals to one's individuality and it is understood that certain information is to be kept private [7].

The web may increase one's fear and anxiety with respect to the potential consequences when providing personal information. To protect the citizens of Ontario, all government services and programs must comply with the access to information and privacy requirements of the Freedom of Information and Protection of Privacy Act (FIPPA). This act regulates how government manages personal information that is collected [7].

1.3. Why privacy is so important

One can appreciate that ESD transactions over time will collect a great deal of personal information that must be managed and protected. If the government is unable to protect information collected through electronic channels there will be a loss in public confidence towards government and worse yet, could contribute to crimes related to identity fraud. Privacy protection must explore a balance between privacy and service delivery.

2. Literature Review

A study performed by Anton *et al*., (2002) [3] proposed a framework for implementing privacy policies and practices. The framework offers five perspectives to consider:

2.1. Legal perspective must be respected, thus privacy must comply with laws and current legislation [3].

2.1.1. Technical perspectives determined that application access points must only be provided within a secure environment to protect consumer privacy. A secure a web environment protects individual privacy, thus, invites a high level of perceived trust among users [3].

2.1.2. Business perspectives determined that rules must exist around how data is collected and transformed. Importantly, users feel that privacy is respected when a web site indicates the reasons for information collection and how information is used [3].

2.1.3. Contractual perspectives consider increased vulnerabilities with applications that are developed by third parties because development can only occur by a selected group of people who hold certain expertise. These contractual networks may be perceived as a loss of control for some organizations and an increase in risk for users at the same time [3].

2.1.4. Social perspectives determine that the relationship between the web user and the organization is vital towards supporting user privacy. In many cases, organizations do understand the importance of user privacy [3].

The study concludes that all five perspectives underpin privacy concerns of web users and reflect a framework for privacy

issues and concerns in a web environment. Using this framework, the is a review of the critical defence strategies undertaken by the Ontario government designed to protect web applications from threats and attacks.

3. Critical web defence strategies designed to protect privacy

3.1. Informed Consent

The first critical element protecting privacy is known as *informed consent*, which requires that the user be given the opportunity to agree to obtain services via the web technology. This has relevance to the user, as it is designed to enhance their awareness to the sensitivities of data sharing over the web [5]. Privacy management from a business perspective, including informed consent, may lead to a clear understanding of online privacy risks for the web user [3]. Informed consent builds trust in ESD, educating the user of risks so that they are empowered to make appropriate decisions [5].

3.2. Limit collection, use and provide disclosure of information

Critical elements that protect fundamental privacy principles *limit the collection, use and disclosure of information* [5]. "The purpose for which personal information is collected shall be identified at or before the time information is collected. The collection of personal information shall be limited to that which is necessary for the purposes identified. Information shall be collected by fair and lawful means" [5].

Statutory authority for the collection of personal information by the government is identified when collecting information, therefore, users know under what authority, information is being collected. Once gathered, the information cannot be copied or disclosed for subsequent use in a non-government transaction unless explicit consent has been provided [7].

This provides relevance because the user is informed that data collected is only for the specified purpose, further enhancing the trust of web technology in government services. Through the legal framework, the review of the above literature supports this defence strategy and provides evidence that it is a successful online activity resulting from a clear understanding of online privacy [3].

3.3 Privacy Impact Assessment

A *Privacy Impact Assessment (PIA)* must be completed prior to the development of any government program where personal information may be exchanged. PIA guidelines are included in the planning process for information and technology development, enterprise architecture planning and follow architecture review board protocols [7].

The government undertakes a PIA to determine if newly proposed uses of technology will meet privacy requirements. The Freedom of Information and Protection of Privacy Act (FIPPA) legislation underpins the PIA. The PIA process examines the business rationale of the ESD initiative and reviews\analyses the hardware and system design to ensure compliance with privacy requirements. Ultimately, the PIA process ensures privacy is considered from project inception, design, implementation through to the audit and review stage. The Management Board of Cabinet (MBC) requires that a PIA be completed on all information technology projects that involve the exchange of personal information [7]. This process also prevents costs from escalating and projects from failing, as cost of failures has been evaluated as being either human, organization or technically focused [1].

Mandatory PIA guidelines implemented early during the planning stage for all ESD deliverables ensure that a privacy framework is considered. Success comes from raising concerns over privacy early in a project so that corrective action can be taken. A PIA supports the legal perspective, which has a positive reinforcement towards privacy enhancing technologies [3].

3.4 Architectural Review Board

The *Architectural Review Board (ARB)* reviews projects to ensure that there is compliance with the criteria noted within the scope of the project. The PIA, as discussed, supports the decision making of the ARB [7].

Identifying privacy risk and requirements early, before actual development work begins, is critical to the integrity of an ESD product and is a major force in guiding government decisions. This crucial background work provides evidence that ESD products are developed utilizing sound principles and overall arching privacy legislation [7]. There is adequate focus and attention placed on privacy when developing ESD products, thus, citizens can place a comfortable level of trust in the web

products offered. The ARB process places importance interweaving privacy policy with the technical requirements to reduce user privacy concerns and increase their level of trust with the organization [3].

3.5 Application Development and Testing

The fifth element to reduce the privacy concerns of a web application is *sound application development and testing policies and protocols*. Rigorous penetration testing is conducted throughout the web application and environment, identifying risks in advance of launching ESD products to the public [7].

Penetration testing attempts to simulate an attack on a web application, searching for system vulnerabilities in application code or other software flaws. These tests are part of a risk mitigation strategy that attempts to keep one-step ahead of those who attempt to hack into a system for nefarious purposes. While costs are incurred to perform this function, it is vital in the process of developing trusted ESD services and products.

Another part of application testing includes code reviews that assist in the identification of vulnerabilities in applications, as well as the identification of design and coding errors. This process is important in order to ensure that tax dollars are not spent on non-beneficial events such as code re-writing [7].

Testing ensures reduced online privacy invasions. Application testing supports that the framework for privacy concerns could be properly addressed through a technical perspective, where public trust in the protection of private information collected by the government becomes vital to the success of web technology [3].

3.6 Secure Environment

Finally, *security features* protect web applications. For instance, robust firewalls work to make web application software 'invisible' and protect applications against attacks such as theft or unauthorized access [16].

Security features include portals that do not leave personal information behind on a user's computer. This is extremely important, as ESD services can be easily accessed from any computer located in a public facility, such as in a public library. Therefore, security features should ensure that when a session is terminated, no information is stored in the cookies or is cached. Inability for the web service to store information protects personal and confidential information from getting into the wrong hands [7].

Trust and confidence in government web service is maintained with the solid safeguard of robust firewalls that include the inability for browsers to cache information. This supports past research, which considered that access points must only be provided within a secure environment to protect consumer privacy [3]. A secure web environment protects individual privacy, thus, invites a high level of perceived trust among users.

4. Summary

Ontario has been on the forefront of ESD development, paving the path towards protecting one's privacy and excellent customer service. Recall that the government's position with respect to privacy protection does not start at the development stage of an IT product; rather, it begins many months earlier, during the privacy assessment review and architecture review stages. IT development can only begin once these functions are completed. Web development is well managed, strategic and considered an investment for Ontarians.

Some may suggest that there are a relatively small number of reported privacy concerns to the Information and Privacy Commissioner of Ontario (IPC). In the IPC 2008 Annual Report, there are a reported 223 privacy complaints. Of all the complaints closed during that same year, individual members of the public initiated 154 (66%) of all complaints. The Commissioner initiated 34 (15%). Another 35 complaints (19%) were self-reported by institutions [6].

5. Users obligations to protect their own privacy

Knowing that the government advocates very strongly for the privacy of personal information, users too, must act wisely to mitigate their exposure to risk by being aware and verifying the authenticity of websites. Each provides relevant privacy protection strategies.

5.1 Become aware

Ontarians need to understand what misperceptions and realities exist to actively play a role in protecting their privacy. For instance, ensure that you have logged off a public computer and that you have cleared any personal data on any forms completed. Cautiously use home computers, shared workspaces, considering access to workspace by others.

5.2 Verify authenticity of websites

Trust in an electronic environment is important and beware of non-government websites that will promise access to government services for additional fees. Ensure websites have government symbols and literature.

6. Conclusion

The Ontario government can safely intake private and confidential information while acting as an honourable custodian of the information its in collects. There has been a demonstration in its transparency towards ESD products and privacy protection through informed consent, data collection mandates, rigid planning through a privacy impact assessment and the architectural review board along with consistent backroom testing. Web enabled access to government services has provided enhanced products to the citizens of Ontario while maintaining their right to privacy.

References

[1] Al-Sebie, M., Elliman, T., Zahir, I. (2006). *Transaction stage of e-government systems: identification of its location and importance*. Hawaii International Conference on System Sciences (HICSS-39), Hawaii, USA.

[2] Aljawarneh, S., Alkhateeb, F. (2009). Design and implementation of new data validation service (NDVS) using semantic web technologies in web applications. *World Congress on Engineering*. Retrieved January 2, 1010 from, http://www.iaeng.org/publication/WCE2009/WCE2009 _pp179-184.pdf

[3] Anton, A., Earp, J., Jarvinen, O. (2002). *A social, technical and legal framework for privacy management and polices*. AMCIS2002 Proceedings. Paper 89. Retrieved December 30, 2009 from http://www4.ncsu.edu/~jbearp/amcis02_final.pdf

[4] Bennett, C.J. (2003). What government should know about privacy : A foundation paper. Retrieved December 30, 2009 from, http://www.accessandprivacy.gov.on.ca/english/pub/wgskap.html

[5] Electronic Service Delivery Privacy Standard. (2000). Retrieved December 30, 2009 from, http://www.accessandprivacy.gov.on.ca/english/pub/esd 1.html

[6] Information and Privacy Commissioner of Ontario (2009). 2008 Annual report. Retrieved December 30, 2009 from http:/www.ipc.on.ca/images.resources.ar-08e.pdf

[7] Information and Privacy Office, I&IT Strategy, Policy, Planning and Management Branch, Office of the Corporate Chief Strategist, Management Board Secretariat, Government of Ontario (2001). Privacy Impact Assessment – A user's guide. Retrieved on December 31, 2009 from, www. accessandprivacy.gov.on.ca/english/pia/pia1.pdf

[8] Office of the Corporate Chief Information Officer, Management Board Secretariat, Government of Ontario (2003). Discussion paper on identity authentication and authorization in electronic service delivery- An Ontario perspective. Retrieved December 19, 2009 from, www.accessandprivacy.gov.on.ca/english/pub/iaa.pdf

[9] Proctor, R., Ali, M.A., Vu, K.P. (2008). Examining usability of web privacy policies. *International Journal of Human – Computer Interaction*. 24 (3) 307-328. Retrieved November 19, 2008 from ABI/INFORM Global.

[10] Reiner, R. Dr. (2007). *Identity management and information protection in the digital world. Can we meet the challenge? Electronic service delivery – Security risks, challenges, & solutions.* 8th Annual Privacy and Security Conference, British Columbia, Canada. Retrieved December 17, 2009 from, http://www.mser.gov.bc.ca/privacyaccess/Conferences/Feb2007ConfPresentations/Reiner-Richard.pdf

[11] ServiceOntario. (2009). Services for residents. Retrieved December 15, 2009 from, http://www.serviceontario.ca

[12] Statistics Canada (2006). Canadian firms connect with government on-line. *Innovation Analysis Bulletin*. 8 (3) 21-23.

[13] Statistics Canada (2007). Electronic commerce and technology. The Daily. April 20, 2007. Retrieved November 5, 2009 from, www.statcan.ca/daily/english/070420/d070420b.htm

[14] Statistics Canada (2008). Electronic commerce and technology. The Daily. April 24, 2008. Retrieved January 1, 2010, www.statcan.ca/dailyquotidien/ 080424a-eng.htm

[15] Stoecklin-Serino, C., Paradice, D.B. (2009). An examination of the impacts of brand equity, security, and personalization on trust processes in an e-commerce environment, *Journal of Organizational and End User Computing*. (2) 11-36. Retrieved January 1, 2010 from ABI/INFORM Global.

[16] Zviran, M. (2008). User's perspectives on privacy in web-based applications. *The Journal of Computer Information Systems*. 48(4) 97-105. Retrieved December 30, 2009 from ABI/INFORM Global.