Trans-Border E-Commerce: The Perspectives from Canada and the UK

Dragana Martinovic
Faculty of Education
University of Windsor
Windsor, Ontario, Canada

Victor Ralevich
ACES
Sheridan Institute of Technology and Advanced Learning
Oakville, Ontario, Canada

***ABSTRACT*:** *In this paper the authors compare Canadian and the United Kingdom practices in the management of electronic information on the Internet. The focus is primarily on policies and practices of electronic data storage and transfer, protection of privacy, and electronic business data transfer. The authors examined the impact that national personal data protection legislation and regulations have on electronic data transfers between and within Canada and the UK by organizing consultations with security and privacy experts in both countries, as well as with Canadian and international legislators. The findings are situated within the Access Rainbow framework suitable for obtaining a global view on the roles of different stakeholders in the adoption of e-commerce. This study represents the first stage of a larger project that will encompass several geographic regions*[1]**.**

Keywords: e-commerce, Access Rainbow, Outsourcing, Privacy, Cloud computing, Ubiquitous computing, Consumer trust, Cross-border data transfer

Received: 2 September 2009, Revised 18 October 2009, Accepted 29 October 2009

1. Introduction

This paper encompasses issues that are closely related to societal changes introduced with new technologies, and in particular the Internet, especially those that enable processes, based on transfers of data, that are time and distance independent. Furthermore, these technological advances allow for easy collection, inexpensive storage, and indiscriminate data mining. However, even though so far the Internet has been broadly used for more than two decades, there are economic, social, legal, and cultural issues that limit and/or otherwise make problematic the use, management, and handling of business and personal information across and within geopolitical borders.

In order to examine the challenges to e-commerce[2], the authors have organized their research around the most prominent ones: (a) consumer trust, (b) privacy concerns, and (c) practices in personal data management; with special interest in how they are addressed differently by business segments in two prominent technologically developed countries, Canada and the UK.

2. Theoretical Framework

This research was conceptualized to reflect the 'Access Rainbow,' a seven-layer model of access to the information and communication infrastructure introduced by Clement and Shade (1998):

[1] *This study was supported by the grant from SSHRC 861-2007-3017*

[2] *E-commerce includes online buying or selling, either from business-to-business or business-to-consumer (OECD, 2005).*

1. From the perspective of this project, the Internet is the first layer of Access Rainbow, as conveyer of digital information.

2. The next layer consists of devices/hardware used in managing digital information, including its storage, transfer and operation.

3. The third in the hierarchy are software tools that make equipment operational (e.g., browsers and search engines).

4. The next layer consists of utilities that satisfy users' needs in digital information management (e.g., PayPal, ordering forms, databases).

5. At the fifth layer are Internet service providers (ISPs, i.e., organizations that facilitate transfer of information on the Internet), accountable to their governments and clients.

6. The sixth layer is related to education of the public in, for example, proper use of technologies, issues of accountability and rights.

7. The seventh layer covers governance and policy-making (see Figure 1).

While for this investigation the sixth and seventh layer of the Access Rainbow model were most relevant, specifically the status of business accountability, consumer rights and public governance in relation to e-commerce across Canada and the UK, it was determined important to examine the other layers too, as the enablers and facilitators of the top two.

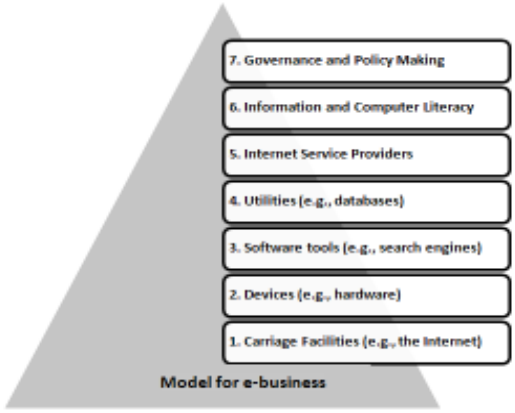

Figure 1. Access Rainbow model (based on Clement & Shade, 1998) of access to the information and communication infrastructure

3. Preliminary Findings

In the process of conducting preliminary research the authors first examined existing documents on e-commerce in order to (a) provide a map of current Internet laws and regulations in Canada and the UK; (b) compare their utility by looking at the cases that they have resolved; and (c) identify social and cultural issues that affect general public understanding of existing legal and privacy protection regulations in e-commerce.

Statistics on trends in the Internet use are revealing. According to the Internet World Stats (2010), in 2010 there were more than 1.9 billion Internet users (28.7% of population) in the world compared to about 1.2 billion Internet users in 2007 (Internet World Stats, 2007). Of all geographic areas, Asia contributed the most to this rapid growth having more than 825 million users with penetration of 21.5%. Second is Europe with 475 million Internet users (58.4% of population), followed by North America with 266 million users (77.4% of population). Canada accounts for 26 million Internet users (77.7% of population), compared to UK with 51 million Internet users (82.5% of overall population). Although these statistics reveal that the issues of primary access to the Internet are diminishing worldwide, other statistics elicit new questions. For example, using the, so called, *Internet Activity Index*, the Online Publishers Association (OPA) points to a steady decrease in the amount of time the Internet users spend on e-commerce sites (i.e., 16% in 2003, 15% in 2007, 13% in 2009, and 11% in 2010), compared to percentage of time spent on other activities like, communications, community, content and search (OPA News, 2010; 2008). At the same time, Canadian statistics show decrease in average online purchase from $183 in 2007, to $158 in 2009 (Statistics Canada, 2010).

There may be different explanations for these findings. The first trend may be the consequence of online buyers becoming more experienced and informed so that they need less time to do the online business transaction; also, the decrease in purchase may mean that buyers use the Internet to find better deals and cheaper alternatives among the most popular purchases (i.e., travel and entertainment). However, both findings raise certain concerns. The main players in international commerce find these statistics disturbing as they may underline the shifts in public interests as well as a probable lack of trust in doing business online. One of the key obstacles in developing further trust among the general population for e-commerce may be caused by the activities of organized international cybercrime groups. According to the latest studies and media coverage, identity theft is on the rise in most of the developed countries, primarily the U.S., Canada, and the EU. Based on the Norton Cybercrime Report (2010), which states that the most common types of cybercrime are related to: malware (51%), online scams (10%), phishing (9%), social network hacking (7%), and online credit card fraud (7%), it could be concluded that one of the main targets of cybercrime is e-commerce, with a likely purpose of achieving financial gains.

To provide wider context for this study, the authors looked closely at the following three aspects of the Internet-based business communication: (a) economic; (b) legal; and (c) socio-political and cultural.

Economic aspect. From a financial perspective, businesses are looking for technologies that are geared towards more efficient and less costly access for customers. The governments of both Canada (Industry Canada, 2000) and the UK (HM Treasury, 2000) aim to be at the forefront of e-government and e-commerce movements internationally; however, both countries struggle with finding a balance between the two opposing ideologies of supporting a non-regulated Internet or tightening control over it. These matters become even more complex in view of outsourcing tendencies in both countries, where even small on-line businesses can be registered locally, but have employees and customers spread internationally.

Legal aspect. It is a known fact that legislation has been slow to follow technological advancements (Holtzman, 2006). In other words, "[r]egulation has tended to be reactive: response had been made to technological development, implementation and practice after the fact" (Surveillance Studies Network, 2006, p.77). In many countries, including Canada and the UK, work on legislation is initiated by disruptions and public outcries rather than as a product of a continuous forward-looking process. In the absence of legislation, a number of business associations and other public entities have developed their own data management and privacy-related policies and codes of professional conduct. These codes are followed on a voluntary basis since they are *not required by law; rather, they exist to guide, educate and discipline members*. In addition, it is observed that "European customers have poorer protection against the online banking scams […], than in the US" (McGraw, 2007, p. 11) or Canada.

Socio-political and cultural aspect. What further compounds issues of privacy, trust and security in the international context is the terminology used in many information networks scenarios. Internet-related legal terminology is not universally agreed upon and concepts are "prone to different interpretations which may be largely politically and culturally determined" (Martinovic & Ralevich, 2007, p. 4).

The different ways of interpreting what 'privacy' is has resulted in a divergence of Internet legislation in UK and Canada. In Canada, the *Personal Information Protection and Electronic Documents Act*, PIPEDA (Department of Justice Canada, 2000) provides guidelines for collection, use and disclosure of personal information in the course of commercial activity. In the EU, *Data Protection Directive*[3] describes strict limitations in such cases and "bars transmission of this personal data to countries that don't have parallel privacy safeguards" (Industry Canada, 2007, Europe).

As it was noted in Martinovic and Ralevich (2007, p.9-10), similar difficulties exist in implementing security measures because users are either not knowledgeable enough or are careless, inconsistent and not persistent enough. Acquisti and Grossklags (2005) pointed to discrepancy between what theory suggests, which is that "consumers should be able to manage their privacy" and what one can find in practice, which is that "consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits" (p.26). In other words, individuals are often willing to trade privacy for convenience or bargain the release of personal information in exchange for relatively small rewards and are reluctant to adopt privacy protective technologies.

Through the methods of social engineering which exploit "users as the weakest link" one can be persuaded to reveal

[3] *The Data Protection Act turns the stipulations of the EU Data Protection Directive into the UK law.*

sensitive information even before any real security attack on their computer is attempted. This was exactly the case with Acquisti and Grossklags'(2005) sample, where over 70% of the participants (N = 119) did not know how to browse the Internet anonymously to prevent others from identifying their IP address; more than 75% could not compare a Web site's privacy policy with their privacy preferences; over 80% could not remain anonymous when completing online payments; and for over 65% it was problematic how to protect e-mail so that only the intended recipient can read it. The same study revealed that some individuals equated security to privacy and had other misconceptions in that area as well.

Research findings reveal that privacy is a sensitive concept prone to different interpretations which are largely politically and culturally determined. For example, Levin and Nicholson (2005) conclude that the concepts on which understanding of privacy is based in US, EU and Canada play a significant role in their legal protection of privacy. In the US, they claim, privacy protection is primarily motivated by the protection of liberty. In the EU, the protection of privacy is mainly the protection of one's dignity (to avoid humiliation); while Canadians occupy the middle ground, thus "sharing US concerns about 'Big Brother' Government, while also having deep concerns about private sector abuse of their personal information. […] Privacy to them is about control – the right to control one's personal information and the right to choose to remain anonymous" (Levin & Nicholson, 2005, p.360). Furthermore, some individuals may understand privacy as "a data attribute: some data are private and some are public. To others, privacy is not a property of particular data but a right to control when and on what terms personal attributes can be disclosed" (Landwehr, 2006, p.4).

To conclude this section, the authors found that there is no firm and internationally accepted officially binding and legal framework regarding potential consequences of data mining, personal and business data storage, retention, ownership and conditions of use. According to MEMO/07/159 (Europa, 2007), Data Protection Directive and the ePrivacy Directive impose obligations on the EU data controller, which in turn recognize rights of the individual that the data are about. Still, this scheme is difficult to implement due to "data processing by different actors in different locations, and with the hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries" (p.1, italics added). In many instances the Internet appears to be borderless, while closer inspection shows that boundaries and limitations do exist. However, there is a lack of sustainable international agreements on how to resolve the border issues in information transfer and "to align domestic and local law and regulation with international human rights laws, norms and standards" (Internet Governance Forum, 2006, p.2). In other words, there exists a whole plethora of issues at different levels of 'Access Rainbow' model (Clement & Shade, 1998) that the authors of this paper used as starting points in their investigation of trans-border e-commerce.

4. Methods

Methodologically, for a broad consultation process the authors organized workshops in Canada, the UK, and Ireland with a number of experts. In these workshops the authors presented statistics and comprehensive information on Internet laws, social and cultural factors and privacy regulations in e-commerce that they have gathered and analyzed.

In addition, there were organized meetings with individuals associated to the Canadian government, who provided their input into the current aspects of cross-border business data transfer.

One of the exercises that the research team did during the workshops in Toronto and in Dublin was to ask those in the audience where their interest lies among the provided topics (see Table 1).

The Toronto audience (N = 7), which consisted of security practitioners, a lawyer, and a government official, was mostly interested in (1) International data transfers; data processors in other countries; issues of liability and control; followed by (2) Internal codes of practice in various domains; impact assessments procedures and (3) three other topics were equally ranked. The Dublin audience (N = 13), which consisted of academics (some of whom are from the UK) and two security practitioners (one of whom also works for the government), was interested in (1) International electronic data exchange: cases, incidents (e.g., business disruptions, network congestions, delays, disaster recovery); (2) Dilemmas of privacy and surveillance; and (3) Internet service providers (ISP)—handling of data, jurisdictions.

The data in this project were collected through the questionnaires, workshops—focus group meetings, interviews and observational notes taken. In addition, the researchers attended four conferences: (1) Industry Canada: Participatory Web, Ottawa, ON, October 15, 2007; (2) ITAC's Who's Who in ICT, held in conjunction with Toronto Tech Week, Toronto, ON,

How Interested are You in the Following Topic?	TorontoWorkshop	DublinWorkshop
Specifics of data management in international setting in your area of expertise	2	5
Relations of Canada/UK with US and EU that may influence data management regulations-Living besides a mighty neighbor	3	6
International electronic data exchange: cases, incidents (e.g., business disruptions, network congestions, delays, disaster recovery)	n/i	1
Problems encountered by small to medium enterprises	n/i	6
Specifics of customers' populations in various international settings	n/i	n/i
Dilemmas of privacy and surveillance	3	2
Internal codes of practice in various domains; impact assessments procedures	2	6
International data transfers; data processors in other countries; issues of liability and control	1	4
Relation of industries/sectors with legislators in your country	n/i	n/i
Internet service providers (ISP)-handling of data, jurisdictions	3	3

Table 1. Ranked Interest of the Workshop Audiences

Note: 1 is the highest rank; n/i stands for not having interest in the topic.

September 22–26, 2008; (3) 3rd International Conference for Internet Technology and Secured Transactions (ICITST-2008), Dublin Institute of Technology, Dublin, Ireland, June 23–28, 2008; and, (4) 10th Annual Privacy and Security Conference, Empress Hotel, Victoria, BC, February 1–4, 2009, where they made contacts and organized interviews. Participants in this research are also considered to be its contributors, as their input was valuable in answering research questions and achieving the research goals.

5. Integrated Findings

This section contains selected findings based on data collected in the Dublin and Toronto workshops, individuals connected to the Canadian government, as well as the literature review on the topic. These findings are grouped according to the level of Access Rainbow model they apply to.

A. Recent trends

1) Level 1 of Access Rainbow—the Internet: In terms of supply chain (B2B) businesses may be moving off the Internet to their proprietary networks. Given that the companies are concerned about privacy and security, they are setting their private networks away from the challenges of the Internet.

The most recent novelty that may have a serious impact on e-commerce is the introduction of cloud computing, which presents a shift from a corporate IT to an Internet-centric model. With cloud computing, many of the old concepts and practices may

become obsolete, like storing data locally. As one of the participants said, "Everything about [cloud] is in stealth. You have no knowledge of it. It is just there. And you just hope because there are just these massive arrays of server farms globally, that your privacy and your data are OK." The problem is that one does not know where the processing is happening? boundaries are based on routers and nodes and not necessarily national borders. As a consequence, geographic legislative boundaries cannot easily apply to processing on the cloud and use of cloud computing for business purposes may fall into domain of cross-border outsourcing.

2) Level 4 of Access Rainbow—Utilities for Information Management: It was mentioned that regardless of the proliferation of the Internet and a plethora of online businesses, consumers do not use the Internet for large payments. It seems that some sort of saturation point was reached in that there are no new incentives on the big purchase items like cars and real estate to draw more Internet commerce users. For smaller items (e.g., booking hotels, airline tickets) the businesses are pushing customers towards Internet purchases (e.g., Delta Airlines charges $25 more for on site booking compared to online booking). While savings on hotels and airfares provide good examples of incentives that successfully attract online customers, presently the public awaits a new business model to emerge for stimulus of e-commerce growth.

The participants pointed to a fact that is often overlooked, namely that in the Internet era there is much e-commerce that is non traditional. 'There is always revenue somewhere on the Internet.' Thus, online businesses are finding other ways (e.g., by using advertising) to gain revenue without directly charging customers.

With government liaisons, the authors discussed a difference between the utilities for surveillance used by different governments. For example, the UK government has utilities such as, the identity card, DNA databases, and finger print scanning. They are all separate programs and they extensively serve different purposes. But when put together and considered concurrently, they end up covering most of population. Canada has some similar, but watered down versions of all of these programs, such as a DNA database (but not a significant part of Canadian population in the database) and ID card systems (which is not mandatory on the national level).

The difference in social, political systems as wells as cultural and ethical systems of values in Canada and the UK is one of the reasons that these surveillance systems are implemented on different scales. This makes a lot of difference in the allocation of government resources and economics.

3) Level 7 of Access Rainbow—Governance and Policy Making: Governments and municipalities digitize their services, and feel more or less confident in knowing what they need to do to properly organize business with the citizenry. But when this knowledge is extrapolated to geographies and countries, the whole issue becomes obtuse in terms of what laws apply, how data are transferred across borders, and the disposition of data that fall into a foreign jurisdiction. So then it becomes questionable as to how C2B or B2B practices could be organized in a meaningful fashion to be sustainable, so that consumers are attracted rather than discouraged.

The recent report from the Public Interest Advocacy Centre (PIAC) suggests that governance issues regarding online payments in Canada should be considered carefully, particularly in view of current developments in Australia and the UK (PIAC, 2007). The UK and Australia currently use a regulatory framework for electronic payments that is in many ways superior to Canada's, and both countries are striving, through broad public consultation, to improve on those schemes in order to face the new and upcoming realities of the market. For example, the UK's Banking Code applies to all types of electronic funds transfers, with specific provisions for particular mechanisms, such as banking machines, clearing cycle, direct debits, electronic purses, cards and PINs, credit cards or aggregation services as required.

Privacy legislation in general is porous—it is the origin of tremendous problems for security professionals when they try to apply it in their own particular context. Privacy laws are written by legislators without sufficient input from information systems security experts and practitioners, so the law is purposely vague in terms of the actual security countermeasures that are required to protect something or somebody. The participants concluded that the strongest method of enforcement of privacy protection is one of public perception. This is because the companies are more concerned about public perception than about obeying the law. In other words, the court of public opinion has a stronger impact on how companies behave than any particular regulator or any particular law.

For the most part, in Canada there is such huge diffuseness of privacy regulations, that security experts "do not know … how

to help privacy." Canada has Privacy Impact Assessments (PIA-s) which are a powerful privacy tool, but they only go so far. As one of the participants commented, "There is no detail as an addendum or as an adjunct to that privacy body for practitioners to say 'this is the refutable baseline counter-measure that you need to apply.' It is always 'it depends'." As the level of privacy is always case-dependent (i.e., public health is regulated differently than accounting), it is difficult for municipalities to answer to the cry from the local businesses asking "what is enough, what is just enough?". Companies have to have the trust model built into their design and there has to be substance behind it. However, it is questionable whether legislation is precise enough to induce confidence in today's consumers. The participants noted that Canadian legislation is too ambiguous, that it is based on a 'reasonableness factor' (which different individuals may understand differently), and that it still does not provide enough guidance to be helpful to organizations. What complicates this situation even more is that the present prevalent business and social models are such that they support partnerships and information sharing, rather than isolation and information protection.Among Canadian research participants, it was often reiterated that 'Canada needs harmonizing laws'. It seems that Canada is doing a better job with harmonizing its laws with external partners than by doing so internally between jurisdictions and governments within Canada. For example,

Canada and the UK are both partners in the OECD; consequently, the OECD requirements affect documents like PIPEDA.

B. Recommendations from the workshops

1) Level 5 of Access Rainbow*—The Role of Internet Service Providers*: In both workshops, the topic of role of ISPs was ranked as third most interesting. The reason for such interest is that they handle data. To increase the overall public trust in these transactions, ISPs need to make clearer what their security requirements are with respect to protecting customers' data. However, ISPs are usually first to be asked to cooperate with governments and law enforcement agencies. In Canada, there is a push that ISPs should ensure that certain data that violate, for example, copyright laws do not get through. "This is a bit troubling—where does it stop?" It was maintained among participants that *the ISPs are facilitators of traffic and not traffic shapers*. They are part of critical infrastructure and should remain impartial in their operation.

An example of *Society for Worldwide* Interbank Financial Telecommunication (supplies secure messaging services and interface software to wholesale financial entities) was brought up in the discussion. Apparently, there was a complaint launched because the Patriot Act allowed for a subpoena due to the release of Canadian information to United States Treasury. The Office of Privacy Commissioner of Canada concluded in this case that: "the [Privacy] Act cannot prevent foreign authorities from lawfully accessing the personal information of Canadians held by organizations within their jurisdiction. Likewise, the *Act* cannot force Canadian companies to stop outsourcing to foreign-based service providers" (OPCC, 2006, Media Release). The participants unanimously stated that the data originating in Canada are not Canadian data, but *they belong to individuals* who most often are not aware that their privacy was breached: "Privacy is a personal thing. When you talk about corporations and governments, then it is a [matter of] secrecy and confidentiality. That is not privacy. Privacy is protoplasm of an individual." The element of consent is crucial for privacy. The *California 1386*[4] model is mushrooming in many states in the US and raising interest in Canada too. Is that the model to follow in the area of country to country e-commerce?

***2) Level 6 of Access Rainbow—Social Factors*:** During the workshops the participants exposed some of the barriers to the adoption of solid Information Management practices in the Canadian context—the notions of demographics and regionalism. People in the large metropolitan areas are more sophisticated, and may be more interested in this kind of uptake, whereas individuals living in more depressed areas may not. Such a distinction defines some sort of microcosm, which can be extrapolated to a much bigger international arena, where there are blatant cultural differences. The issues of privacy in identity management and personal identification across jurisdictions cannot be divorced from the study. The participants concluded that, "These issues are tightly coupled to any kind of discussion around e-commerce and a bi-lateral agreement between countries. You can't ignore them."

In conclusion, it was noted that the whole concept of personal identifiable information is evolving: "In 1965 you only had a credit card, a VISA card—today you have a credit card and a mobile phone. So, mobile computing is going to provide new

[1] *In the United States , the California Security Breach Information Act (SB-1386) is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. The Act stipulates that if there is a security breach of a database containing personal data, the responsible organization must notify each individual for whom it maintained information.*

processes whereby you protect the data in a different fashion." It seems that for some "the issue is not whether this unit of data is protected. The issue is whether I am protected." With mobile computing that is adding more and more features, protection of entity becomes a liability. It was noted that while in many cases that involve new technologies it is natural to apply legacy solutions and processes, in case of electronic data management that is not true:

"A plane from Toronto that crashes in the UK is still under the ownership of Canada. Why is that, on the international stage, it is a simple matter that the plane belongs to the Canadian government, but if data originate from Canada similar laws do not hold?" The reason was found in the slow maturation of the security field—the process of standardization takes time, as a lot of complexity needs to be agreed upon to create the needed infrastructure. However, "we are now in prehistoric Internet times and the population is 6 billion people."

3) Level 7 of Access Rainbow—Governance and Policy Making: Regarding the following two topics, *Internal codes of practice in various domains* and *Relation of industries/sectors with legislators*, it was suggested that some mapping exercise will help develop conclusions. For mapping exercises it is always useful to have a standard framework or model. Such a framework, in terms of structured exposition of the topic and a sufficient amount of detail, as mentioned in the discussion, is IETF3647[5]. Another useful standard that focuses on the enterprise is ISO27001[6]—a worldwide amalgam of multinational standards. Basic principle of IS codes is practice, therefore, if organization follows this practice, it shows that it is compliant. For example, ISPs can get organizations certified to be compliant with ISO27002. It seems that even the small and medium enterprises (SME) are getting increasingly interested in being certified, because ISPs, banks, and brokerages are coming to them with questions about IT security. However, one has to be careful when using standards to compare different legislations because, as one of the participants commented, "IS standard was originally developed to protect enterprise, to protect the fortress and we are beyond that now. We are [now] trying to protect information."

Another standard that was mentioned during workshops is the payment card industry (PCI) data security standard, which has certification associated with it. PCI is very dense and very prescriptive—it sets up standards on how personal information is treated, what data can be transmitted between merchants, what data can be stored openly, what data can be printed on a receipt. It was acknowledged that there exist various layers in addressing the electronic data management issues. PCI is a technical process layer, but this project should also address populations, human behavior, axiology, law, and enforcement. It was suggested that the research team may look to develop a new model that is partly prescriptive (like PCI) and partly a good practice (like ISO 27002).

Suggested research questions for the second phase of the study were:

1. What is the value proposition for engaging in e-commerce between the U

K and Canada for the average consumer, business, or government?

2. Are there industries that are better predisposed to e-commerce than others? If so, why? What sectors dominate e-commerce? For those who do not, what is the reason? Is privacy an issue?

3. How do consumers view e-commerce? What impedes their trust in engagement in e-commerce? What is the consumers' perception of risk for engaging in a $1 transaction vs. $500?

In addition, it was suggested to the research team to create a lexicon of terms—normalize conversation around what is

---

[5] This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates.

[2] The newer code of practice, ISO27002, contains 11 domains (including privacy) that the organization has to use to extend its information security program. These standards are written by the Joint Technical Council, subcommittee 27, which deals with the IS body of knowledge. 27K family has as its more mature offerings 01, 02. But there is a whole complex of INFOSEC standards under this general rubric. Uptake of these standards in North America is slow; uptake in Europe is rapid. In terms of 01 adoption, not too many financial institutions in Canada have been certified. But generally in the US and Canada there is lot of interest in 02 which has many elements that deal with privacy. These standards came from the UK (BS7799) and mutated into ISO or world wide standard, ISMS.

meant by e-commerce. Finding out what the e-commerce eco-system is about may also be important.

C. Loopholes in Governance and Policy Making

The participants expressed concern that on the Internet, no one assumes liability. It is no wonder then that the end consumers are concerned because everyone is holding them liable. In the brick and mortar businesses case, consumers know fairly well where to go and what is to be done if something goes wrong—there is redress, a predetermined scenario for consumers to get their money back. In the virtual world, however, if something goes wrong, what is the recourse for a consumer? If the consumer's privacy has been breached, what can be reasonably done? It seems that the only guideline that has "any teeth" is the one from PCI. Our participants from academia pointed out that no firm regulations exist for security professionals—there is no control over them. However, security professionals think that IT personnel need to be regulated, as "there may be one person in the company that works on security and 10 others that are IT."

Legislators, on the other hand, mentioned "lack of teeth" in the Canadian privacy protection practices. Apparently, in Canada, a Privacy Commissioner does not have any direct ruling authorities, but the Commissioner will try to resolve the matter and can take the findings to the court. The court may or may not take the case further and will then give its ruling and not the commissioner. Some of these cases relate to cross-border transfer of data, such as credit card processing, banks, telecommunication, mail carrier systems, and insurance agencies.

Another loophole was mentioned in the conjunction with the US privacy protection legislation which applies only to companies that are providing service to the public, but not to the companies that are dealing only with wholesale. The problem is that any company can outsource its shipping to one company, billing to another, and so on. These outsourced companies may only prepare invoices and bills. To such companies PATRIOT act can be applied.

D. Disagreements among participants

The workshop participants disagreed in some instances. The most heated discussion among security professionals in Toronto was related to the "Wild West" nature of e-commerce. Should consumers take justice into their hands and start creating their own rules, thus behaving in the same ad-hoc manner in which other Internet players treat them?

The Dublin audience was mostly divided as to the following question: Is the Internet state-independent? "National interests do not have a place on the Internet. Canada (or the UK) cannot influence the Internet; the Internet influences the states." Some participants feared the possibility that the Internet could become over-regulated. In such a case, data will migrate to legislation where it is easier to handle—"the Internet Liberia."

6. Conclusions

This project was undertaken with an awareness that Information Management is developing into a discipline that encompasses security, privacy protection and issues of data retention. By taking a data-centric perspective—with all the limitations of such an approach—this project was anchored in the paradigm of electronic business data management on an international scale.

The authors started this paper by asking if there is a shift in consumer interest and a lack of trust in e-business that may affect reported recent trends. Findings of this study present e-commerce as multi facetted phenomenon that depends on the whole range of elements in the Access Rainbow model. In 2004-05, the European Information Technology Observatory provided statistics that in e-readiness the UK holds joint third position with the Netherlands and the US, ranking ahead of the majority of its European competitors[7]. It was concluded that the UK has become the first European country to reach critical mass usage of Internet services in the area of e-commerce (in 2005, almost half the population of the UK regularly used the Internet and 91% of employees worked in an Internet-connected business). In 2007, the UK online spending was worth £46.6bn, up 54% compared to the previous year (The Guardian, 2008). These statistics place the UK high on the Access Rainbow model

[7] *E-readiness is the extent to which a country 's business environment is conducive to e-commerce. It is based on a range of factors, from telephone penetration to online security to intellectual property protection.*

[8] *The shopping search engines are designed to check prices at various online stores or locate e-commerce outlets by category [17].*

for e-business.

Other statistics point to change in the Internet users' behavior. For example, it is a well established fact that those retailers (even the big brands) who are not good in marketing themselves online are losing out to their Internet-savvy rivals. It may be that people are "trying to shop more carefully" (The Guardian, 2008). Apparently, in the UK, consumers are extensively using Shopping Comparison Engines[2] such as *Cheapflights*, *Ciao*, *Confused.com*, *Genie Group*, *Gocompare*, *Kayak*, *Kelkoo*, *Moneysupermarket*, *Motley Fool*, MSN-Shopping, *Pangora*, *PriceGrabber*, *PriceRunner*, *Shop.com*, *Shopping.com*, *Shopzilla*, *Twenga*, and *uswitch*.

Compared to the UK, Canadian on-line sales are moderately rising. According to Statistics Canada (2010; 2008), in 2009 orders for goods and services were valued at $15.1 billion, up from $12.8 billion in 2007. The increase resulted from more online shoppers and a higher volume of orders. In 2007, total private and public sector Internet sales reached $62.7bn, which is up 26% from 2006. In the private sector, B2B sales accounted for 62% of online sales (they decreased from 68% in 2006). During the same time, B2C online sales increased from 32% to 38%.

Apart from the weak presence of e-commerce in the Canadian total economic activity (in 2007, online sales in private sector accounted for under 2% of total operating revenue), there are several other alarming statistics (Statistics Canada, 2008). One is that customers outside Canada generate only one fifth of online sales in the private sector, a ratio that did not change for several years. Another is that although in 2007, 87% of private sector firms used the Internet, less than half (41%) of them reported having a website. While Canada has infrastructure in place, there is much to be done to not only increase consumers' interest in e-business, but also the awareness among businesses of the importance of their presence on the Internet, as the UK example shows.

Throughout the consultations with participants, the authors were hearing comments like "this is reality," as opposed to, "this is how it should be done." It seems that comparison with other countries as well as a wide consultation process between representatives (both practitioners and theorists) from government, e-commerce, information security, law, and consumer protection groups are necessary to make real progress in this area.

In conclusion, there are two distinct views found in the literature and confirmed in this study: Some, like Hurley (1999), say that in view of the global information infrastructure, *the rules for privacy and personal data protection must be harmonious and work as a global solution*. Others suggest that it may be appropriate for each country to establish a system in accordance with its socio-economic circumstances, local idiosyncrasies and cultural characteristics (including legal culture) (OECD/OCDE, 2007). It seems that because "we are in the infancy years of the use of Internet for commercial and other business and socially oriented purposes," it will take time and effort to develop a culture of security/privacy at all levels of the Access Rainbow framework. Looking at privacy and security issues through binary lenses, such as described here, may negatively influence the necessary discourse on these important topics. Such matters are compounded by political and economic pressures from the most influential countries[1] and by socio-cultural diversity of countries joining the e-commerce scene.

It will take a meeting of minds and much good will to overcome the notion shared by security professionals in this study, that current legislation is underpinned with rules that bring about unanticipated consequences. Measuring the real-time impact of technological innovations on the socio-economic infrastructure of Canada and the UK will determine the future direction Information Assurance in Security and Privacy will take both locally and globally.

[9] *Both the UK and Canada have mighty neighbors —the rest of the EU and the US (respectively), that cannot be underestimated in this analysis.*

References

[1] Acquisti, A., Grossklags, J. (2005). Privacy and rationality in individual decision making, IEEE Security and Privacy, January–February, 3 (1) 26–33.

[2] Clement, A., Shade, L.R. (1998). The Access Rainbow: Conceptualizing Universal Access to the Information/ Communicatioins Infrastructure, *In*: Information Policy Research Program, Faculty of Information Studies, University of

Toronto. Working Paper No. 10. Toronto: IPRP University of Toronto. Retrieved September 1, 2010 from http://www3.fis.utoronto.ca/research/iprp/publications/wp/wp10.html

[3] Department of Justice Canada (2000). Personal Information Protection and Electronic Documents Act. Retrieved September 1, 2010, from http://laws.justice.gc.ca/en/P-8.6/text.html

[4] Europa (2007). Privacy enhancing technologies (PETs). Retrieved September 1, 2010 from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/159&form

[5] Guardian, The. (2008). Internet shopping: High street stores are losing out to independents online. Retrieved September 1, 2010 from http://www.guardian.co.uk/business/2008/aug/11/retail.internet?gusrc=rss&feed=technologyfull

[6] Holtzman, D.H. (2006). Privacy Lost, Jossey-Bass.

[7] Hurley, D. (1999). A whole world in one glance: Privacy as a key enabler of individual participation in democratic governance."

21st Inl Conf on Privacy and Personal Data Protection, Hong Kong. Retrieved September 1, 2010 from http://www.pco.org.hk/english/infocentre/files/hurley-paper.doc

[8] Industry Canada (2000). Canadian E-Business Opportunities Roundtable: Industry leaders launch six-point strategy for accelerating Canada's growth in global internet economy. Retrieved September 1, 2010 from http://e-com.ic.gc.ca/eteam/release.html.

[9] HM Treasury (2000). Business strategy statement. Retrieved September 1, 2010, from http://archive.treasury.gov.uk/docs/2000/ebusiness30_11.htm

[10] Industry Canada (2007). Retrieved September 1, 2010 from http://strategis.ic.gc.ca/epic/site/direct.nsf/en/h_uw00237e.html

[11] Internet Governance Forum (2006). Statement on Internet Governance. Retrieved September 1, 2010 from http://www.igfgreece2006.gr/

[12] Internet World Stats (2010). Retrieved August 23, 2010 from http://www.internetworldstats.com/

[13] Landwehr, C.E. (2006) Speaking of privacy. *IEEE Security and Privacy*, July–August, 4 (4) 4-5.

[14] Levin, A., and Nicholson, M.J. (2005). Privacy law in the USA, the EU and Canada: The allure of the middle ground. *University of Ottawa Law and Technology Journal, University of Ottawa*, Canada, 2 (2) 357–395.

[15] Martinovic, D., Ralevich, V. (2007). Privacy issues in educational systems. *Int. J. Internet Tech and Sec Trans*, 1 (1/2) 132-150.

[16]McGraw, G. (Jul/Aug 2007). Interview: Silver Bullet Talks with Ross Anderson. *IEEE Security &Privacy*, 5 (4) 10-13.

[17] Norton (2010) Norton Cybercrime Report: The Human Impact. Retrieved October 26, 2010 from http://us.norton.com/theme.jsp?themeid=cybercrime_report

[18] OECD/OCDE (2007). The report on OECD member countries' approaches to consumer contracts." Retrieved October 26, 2010 from www.oecd.org/dataoecd/11/28/38991787.pdf

[19] OECD (2005). Guide to Measuring the Information Society 2005.

[20]Online Publishers Association (n.d.). Internet Activity Index. Retrieved October 26, 2010 from http://www.online-publishers.org/internet-activity-index#

[21] OPCC (2006). Commissioner's Findings. Retrieved April 29, 2009 from http://www.priv.gc.ca/cf-dc/2007/365_20070402_e.cfm

[22]PIAC (2007). Comments regarding the creation of a new framework for electronic fund transfers in Canada. Retrieved September 1, 2010 from http://www.piac.ca/files/piac_eft_comments_final.pdf

[23]Statistics Canada, 2008. Retrieved September 1, 2010 from http://www.statcan.gc.ca/daily-quotidien/080424/dq080424a-eng.htm

[24] Sullivan, D. (2003). Search Engine Watch. Retrieved September 1, 2010 from http://searchenginewatch.com/2156331

[25] Surveillance Studies Network (2006). *In:* D.M. Wood (Ed.). A Report on the Surveillance Society: For the Information Commissioner. Retrieved September 1, 2010, from http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

[26] Watershed Publishing (n.d.)."Users' Online Time Spent Mostly on Content - not Communications, Commerce, retrieved October 26, 2010 from http://www.marketingcharts.com/interactive/users-onlinetime-spent-mostly-on-content-not-communications-commerce-1256/opa-internet-activity-index-four-year-summary-time-spent-onlinejpg/