

Hope is Waning: Linking Debates on Privacy of On-line Information to Distance Education Online Delivery

Seitebaleng Susan Dintoe

INTRODUCTION

Technology has brought with it new ways of securing information. Such information ranges from confidentiality, authenticity, integrity and availability. These types of information can now be stored and shared through the Internet, i.e., websites, emails and e-books. All of these electronic formats can be accessed without restrictions. However, issues of privacy, personal or confidential information still have to be assured. Thus, people utilize user-names and passwords as a means of protecting their personal information. As time passed, the hope that people had for these security measures waned out with evidence indicating that they can be penetrated through hijacking, phishing, pharming, data theft, malware, spyware, adware, spam, denial-of-service (DoS) attacks and scanning.¹ These cases necessitated some interventions like legal protection, technological tools and awareness-training programs. The legal protection, among other things, refers to government policies, regulations, legislation, international organizations actions and public education.

Public education mainly refers to the contributions of private and non-private organizations in the fight against insecurity of information with emphasis on personal information, whereas, technology refers to tools or software hijacking and the protection of online privacy. The interventions mentioned above indicate that people in different areas were concerned about unauthorized access and many are now losing hope about the security of information disseminated through technology. This paper, thus, uses evidences and cases of hijacking to illustrate its claim that it is hopeless to still believe that online privacy can be fully achieved.

The paper starts by describing what online privacy entails and the nature of challenges affecting it and then moves to discussing the online privacy with implications for distance education (DE). The paper concludes with a summary and recommendations for future research and practice.

BACKGROUND

As technology has advanced, the way in which privacy is protected has changed along with this advancement. Online privacy on the “Internet is a major concern to users thus divided into the following concerns:

- Information that can or cannot be shared
- Whether messages can be exchanged without anyone else seeing them

¹ McMillan, R. (2008). “17 arrested in Canadian hacking bust” *PCWorld >> Security* (21 February 2008).

http://www.pcworld.com/article/142711/17_arrested_in_canadian_hacking_bust.html [McMillan, “17 arrested”]. Assessed on July, 21, 2011.

- Whether and how one can send messages anonymously.²

There is a concern about privacy on personal information because technology is prone to hijacking even if protected for example through passwords. It was noted in a survey conducted by the Graphics, Visualization and Usability Center of the Georgia Institute of technology that 70% of Web users were concerned about privacy as the main reason for not registering; it was further noted that 86% wanted to control their personal information and 78% users in a study surveyed by TRUSTe (Online trust and safety) would be more likely to provide information to sites that offered privacy assurance.³ The information privacy is thus protected with a username and password. However, the user name and passwords are said to be prone to hijacking.⁴

Hijacking as a means of stealing information online, can be linked and associated with fraud. For example, it is an attempt to fraudulently acquire sensitive information, like usernames and passwords by masquerading as a trustworthy person or business through emails or phishing websites. Hijacking is a type of network security attack in which the attacker takes control of a communication.⁵ Therefore, hijacking occurs when a third party gains unauthorized access to a user's service account breaking into user-names and passwords. For instance, usernames and passwords are used to authenticate an account when completing online forms. These forms could be an application for admission into higher education or buying books online or responding to an advertisement about schools or jobs, or as a student accessing online materials. Once an individual completes personal information online, the authenticated activities can now be easily hijacked and redirected to a different site. Once in the hands of a hijacker, the user names and passwords could be hijacked through phishing. Therefore, user names and passwords protecting personal information is not safe as hijackers can easily manipulate the technological tools used for safety of online privacy.

SAFETIES TO ONLINE PRIVACY

Safety refers to the state and condition of securing by protecting personal information with a username and password against actions that threaten and deprive it of its intended purpose.⁶ The username and passwords are technological tools used as safety tools to protect online privacy. For example, when the owner authorizes his/her username, his/her personal information cannot be accessed with a username without the password. Therefore, usernames and passwords are very important technological tools protecting online privacy unless hijacked.

² Search Data Management.com (n.d.). *Privacy*. Retrieved from <http://searchdatamanagement.techtarget.com/definition/privacy> Accessed on July 29, 2011.

³ Ibid #2.

⁴ Dignan, L. (2008). *The Gmail password hijacking incident: When so-called helpful apps hurt*. Retrieved from http://www.zdnet.com/blog/security/the-gmail-password-hijacking-incident-when-so-called-helpful-apps-hurt/936?tag=mantle_skin;content Assessed on July 29, 2011.

⁵ SearchSecurity.com (n.d.). *Hijacking*. Retrieved from www.serchsecurity.com/definition/hijacking Accessed on August 5, 2011.

⁶ Charles, G.O. (2009). *Safety versus Security in Fire Protection Planning*. The American Institute of Architects: Knowledge Communities, Retrieved from <http://www.aia.org/practicing/groups/kc/A1AB079791> Accessed on August 3, 2011.

Technological Tools

Technological tools refer to communications and mobility. These tools have since been developed and used with the hope of protecting personal information.⁷ For example, first to check your online information, you enter your username, once the website identifies you, then it will request for your password to authenticate your account. Then, once the websites accepts and identifies you with the username and password, you then can access your personal information. However, Peltier (2002) further noted that for the past years, the technological tools for Internet users and for safe computer using have greatly expanded. There are various software tools, for example, user name and password for securing information and these can still be hijacked as an indication of how online privacy can vanish or be dispersed online.⁸

A username is a name you create or want to be identified with for online privacy.⁹ Firstly, a username is created online in such a way not to be easily cracked by malicious codes or hijacked. For instance, the online sessions will identify you with your username. You enter your username for the system to identify you with. Then once identified, you can easily access your online material. The user-name is used to identify the owner and thus has to be confidential. Confidentiality implies that the name cannot be easily known and copied by unauthorized hijackers. However, the hijackers can attack the username and its password.

One of the important factors of online protection is the password that tells who the user is and how the system is protected.¹⁰ It becomes very important to safeguard the usernames and passwords as they are a key to accessing online activities. Anyone who has or can guess a password can easily access personal information and can damage the entire system. For instance, if a password is shared and or created with words that can easily be manipulated, the password can be used by anyone to access personal information. However, phishing or scams as a means of hijacking can use usernames and passwords without the owner's knowledge. The hijacking usually takes place online when filling out forms for applications for a job, school or buying online products or responding to anonymous scam or phishing emails. There is a high risk associated with using usernames and passwords on online activities.

⁷ Peltier, T., R. (2002). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.

⁸ Lohr, K. (2010). How privacy can vanish online, a bit at a time, *The New York Times*.

⁹ Sharpened.net, (n.d.). *Glossary: Username*. Retrieved from www.sharpened.net/glossary/definition/username Accessed on August 5, 2011.

¹⁰ Password. (n.d.). In *Wikipedia, The Free Encyclopedia online*. Retrieved from <http://en.wikipedia.org/wiki/Password> Accessed on July 26, 2011.

RISKS TO ONLINE PRIVACY

Individuals in today's technological world are subject to privacy threats.¹¹ Risk refers to threats or means of hijacking a username and password. For instance, an individual responding to an advertisement or applying for a job or admission into school will fill out a form online. The online activity involves personal information like usernames, passwords and other sensitive information. Once the personal information is online and usernames and passwords authenticated, it can easily be stolen and spread to more malicious acts like hijacking through phishing.¹² Hijacking is discussed as one of the risks to online privacy.

Hijacking

The intruders use ill-gotten privileges as a means of hijacking to tap into a system's software accessing or controlling the behavior of the local TCP (Transmission Control Protocol).¹³ Ill-gotten privileges are ways and means of using technology to unlawfully access information without owners' knowledge or concern. In the case of *R. v. Cole* (2009)¹⁴, the teacher's laptop was accessed through user-name and a protected password. As a teacher with additional roles to monitor school network, the teacher accessed students' accounts, which were protected with their usernames and passwords. In addition to unauthorized access, UK government protested that Egypt hijacked their text network, which means that their usernames and passwords were used for texting.¹⁵

Usernames

The username as an identity into an account protects all online activities though can easily be vulnerable to hijacking through phishing.¹⁶ For example, an email can be sent by a familiar name, or can be an advertisement to respond to or can be an email informing you of some danger or money that you have won, like the prize or money scams. For instance, an anonymous email will be sent with a message stating that you have won a prize or that money is in the account with no identity. Therefore, by receiving an email and authorizing them to deposit the lump sum of money into your account is risky. Once you respond to one of these threats, you send out all

¹¹ Peltier, T.R. (2001). *Information security risk analysis*. Boca Raton, FL: Auerbach Publications. ISBN 0-8493-0880-1.

¹² See Appendix A: Pearson Education Canada (2008). How Computer Virus is Spread. Computer Crimes – Destructive Code.

¹³ Anti-Spyware Coalition, (ASC) (2007). "Definitions and Supporting Documents". <http://www.antispywarecoalition.org/documents/2007definitions.htm>> [ASC, "Definitions and Supporting Documents"]. Assessed on July 23, 2011.

¹⁴ *R. v. Cole* (2009). Ontario Superior Court of Justice, Toronto Region. Case Can LII72331 (On SC). Retrieved from <http://www.canlii.org/en/on/osc/doc/2009/2009canlii72331> Accessed on July 28, 2011.

¹⁵ Sonne, P. (2011). U.K. *Protests Egypt Hijacking Text Network*. Retrieved from www.online.wsj.com/article/SB1000142052748704709304576123971737287928.html Accessed on August 4, 2011.

¹⁶ Ibid #9.

your personal information. Your personal information like your username will be exposed to these scams and thus your information easily hijacked and redirected it to another website. In this case all your personal information will be hijacked and can be openly accessed by anyone, thus exposing your personal information to risk and automatically affecting your password too.

Passwords

A successful hijacking enables an attacker to borrow or steal an open connection (say, a telnet session) to a remote host for his/her own purposes. Hijacking is associated with fraud that occurs when a third party gains unauthorized access to a user's service account into the username and password. The unauthorized access may occur through a phishing attack, used by someone close to the victim or who is able to find out his or her username and password, or some other illicit tactic. In the likely event that the sincere user has already (been) authenticated to the remote host, any keystrokes sent by the attacker are received and processed as if typed by the user.¹⁷ Virus spreading through the computer can attack the false processing.¹⁸ A study was conducted where a keylogging hijacking software was installed on rental computers at 14 Kinko's stores in New York. In the store, the software monitored keyboard input and recorded it to a log file. However, login information was captured from 450 people and unauthorized access was liable for hijacking passwords.¹⁹ This proved that passwords could easily be hijacked through new technological tools.

The Internet space where all types of hijacking takes place occurs mostly on websites and through emails. However, email hijacking is very common and easy for unauthorized access on personal information. For example, listing email addresses publicly or posting it on social networking sites like Facebook opens it to hijacking threats. The other thing is, one password for all your online activity is susceptible to these online threats. You are also vulnerable to threats whenever you respond to spam messages or offers for deals sent to your email. This type of spam constitutes a phishing hijack attack in which hijackers attempt to gain your personal information.²⁰

It is not safe to back up your Gmail account to G-Archiver for your personal information.²¹ For example, your personal information once backed into a saver like G-Archiver, will swipe your username and password hard coding it into a source code. Then every time you add your account to the program to back up data, an email will automatically be sent with your username and password to your personal email box. Once you are in your inbox, you will receive emails from

¹⁷ Jones, L. (2003). Kinkos's password hijacking case: Why you need RSA SecurIDs. Retrieved from <http://www.lesjones.com/2003/07/29/kinkos-password-hijacking-case-why-you-need-rsa-securids-3/> Assessed on July 29, 2011. Hughes, L.J., Jr. (1995). *Actually Useful Internet Security Techniques*. New Riders Publishing (Indianapolis, IN).

¹⁸ *Information Systems Today, 2/C/e, 2008 Pearson Education Canada*. Unauthorized Access - Survey by Computer Security Institute.

¹⁹ Ibid #17.

²⁰ Ibid #13.

²¹ Ibid #4.

everyone who has used this software.²² This is hopeless and risky for online privacy as Gmail hijacks usernames and passwords without the owners' knowledge. However, unauthorized access into all online activities has been proposed as a mandate for Internet service providers (ISPs) with police to track secured information due to surveillance issues.²³

Tracking of online activities

Tracking is the process of policing online activities.²⁴ It was noted (Schmidt, n.d.) that Canadians are not aware of how closely they are tracked by companies. For example, global policing of all online activities are accessed freely without the owner's consent, due to unknown killings through bombs or commercial advertisements sent to consumers. What this implies is that the usernames and passwords of everyone, even innocent victims, will be hijacked. The victims or online users will not be aware of this unauthorized access racking into their accounts. However, the trade-offs for this free policing of online users accounts had been authorized collaboratively by international organizations due to increasing surveillance issues, to protect the people at large.²⁵

However, some complications arose on authorized access intercepted without a warrant by police, which led to a complex intended use. For instance, the police intercepted without a warrant accessing students and teachers' personal information not permitted.²⁶ It was held in a court case where Electronic Frontier Foundation (EFF) sued the giant telecommunications for violating privacy laws by collaborating with National Security Association (NSA) for illegal

²² Ibid #4.

²³ Geist, M. (2009). *Government introduces Bill to require surveillance capabilities, mandated subscriber disclosure*, (July 18, 2009). Retrieved from www.michaelgeist.ca/content/view/4069/125 Accessed on August 3, 2011. Corbin, K. (2011). *House Panel Presses for ISP Data Retention Mandate*. Data Retention Tag Index. Datamation. Internet.com. Retrieved from www.datamation.com/tag/data-retention-69040.html Accessed August 4, 2011.

²⁴ Schmidt, S. (n.d.). Most Canadians unaware of online tracking: privacy watchdog, *Postmedia News*, (May 5, 2011) Retrieved from <http://www.canada.com/technology/Most+Canadians+unaware+online+tracking+privacy+watchdog/4735324/story.html> Accessed on August 3, 2011.

²⁵ Lyon, D. (2007). *Surveillance Studies: An overview*. Cambridge: Polity Press. ISBN 978-0745635910. Flaherty, D. (1989). *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill, U.S.: The University of North Carolina Press. CBC NEWS, (n.d.). ISPs must help police snoop on Internet under new bill. *Technology & Science*. Quirks & Quirks Blog, Retrieved from (June 8, 2009). <http://www.cbc.ca/news/technology/story/2009/06/18/tech-internet-police-bill-intercept-electronic-communications.html> Accessed on August 3, 2011. USA Patriot Act, 2001 (H.R. 3162) RDS, Focusing public attention on emerging privacy and civil liberties issues. Epc.org. *Electronic Privacy Information Centre*. Retrieved from <http://epic.org/privacy/terrorism/hr3162.html> Accessed on August 3, 2011.

²⁶ Ibid #14.

wiretapping and data mining of American's communication.²⁷ This was emphasized by incidences that were tracked due to September 11 US terrorist attacks.²⁸ The terrorist tracking led to the US introducing the mandate of Internet service providers (ISPs) to police by tracking and accessing personal information and giving it to police without the individual's knowledge due to surveillance issues.²⁹

Surveillance Mandates

In the above discussions, there were exemplary cases cited to indicate that online security is waning out and people are losing hope in it or is being hopeless. This hopelessness is mainly due to many attempts and success to gain unauthorized access by surveillance. Surveillance refers to monitoring the behavior, activities, or other changing information, usually of people often in a surreptitious manner: watching over,³⁰ hijacking usernames and passwords. According to Geist's blog, Investigative Powers for the 21st Century (IP21C) would allow lawful access for mandated surveillance of Canadian Internet service providers (ISPs) that would force them to disclose user information to authoritative sources.³¹ In other words, the ISPs were obliged to freely access all online activities and pass it to the police. It was evidenced by Geist (2009) that a bill was proposed for surveillance mandate in Canada, allowing the ISPs to freely access personal information of all online users and giving it to the police without the owner's knowledge.

The U.S. are said to be the great supporters of surveillance since the September 11 terrorist attack.³² The US Patriot Act, (2001) enhances more on surveillance provisions so that authorities need not go through proper protocol to gather intelligence via electronic devices. The worst case is the surveillance of Radio Frequency Identification (RFID) in US Elementary Schools policing the students' personal information like the GPS (Global Positioning System) systems monitoring cell phone activities. The schools in Japan and England implemented the RFID (Radio Frequency Identification).³³ The FRA Act of Sweden proposed to hook all phones

²⁷ Hepting v. AT & T, EFF, 2006, WL 2038464 (N.D. Cal. 2006). US 145997.

²⁸ Stanley, J. & Stenhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*. Americas Liberties Union (ACLU). Technology and Liberty Program. New York, NY.

²⁹ Isenberg, D. (n.d.). House, Senate leaders back online surveillance. GigaLaw.com daily News (January 27, 2011). Retrieved from <http://www.gigalaw.com/2011/01/27/house-senate-leaders-back-online-surveillance/> Accessed on August 3, 2011, and Ibid #23.

³⁰ Lyon, D. (2007). *Surveillance Studies: An overview*. Cambridge: Polity Press. ISBN 978-0745635910.

³¹ Ibid #23.

³² Ibid #30.

³³ Best, J. (2004). School children to be RFID-chipped. Silicon.com, Technology, Networks. (July 8, 2004). Retrieved from <http://www.silicon.com/technology/networks/2004/07/08/schoolchildren-to-be-rfid-chipped-39122042/> Accessed on August 3, 2011.

and Internet together to police and track all cross border online activities.³⁴ This surveillance mandates led to another loophole of hijacking usernames and passwords. In this case, surveillance openly accessed all online activities as discussed above. Online activities are username and password protected. The technological tools used by surveillance to hijack online activities are tools developed in another version to protect personal information with usernames and passwords. This provided stronger evidence for the hopelessness of online privacy due to surveillance acts being supported collaboratively by governments and international bodies. However, having evidenced the waning out of online privacy, the government and international organizations intervened, establishing, legislations, regulations and public education hoping to help in responding to the online privacy risks.

RESPONSES TO RISKS

Hijacking demonstrated as discussed and evidenced above that people can penetrate usernames and passwords. There came a need to attack methods, therefore, a number of means were proposed or devised like national and international strategies as noted above with the hope of protecting online privacy with usernames and passwords.

Government legislation/Regulations

The government regulations are the first to be considered when it comes to taking actions on making changes to information security. Online privacy laws are developed and proposed at government level. In a 2004 study published by the Federal Deposit Insurance Corporation, it was estimated that almost two million American Internet users experienced unauthorized access.³⁵

The unauthorized access refers to hijacking of personal information as noted in Appendix B with the highest cost. In this article it shows that no matter how secured the information is it can still be hijacked. As noted by Lennon, a new online “Ad hijacking scheme” was discovered.³⁶ The author said that ad hijacking is a new highly sophisticated advertising fraud scheme targeting online video, display and search ads. The question one would ask is, is there hope on online privacy and security information? As new hijacking tools have been discovered, there is a need for global cooperation on securing information. For example, the Organization for Economic Co-operation and Development (OECD) published the “OECD Recommendation on Cross-Boarder

³⁴ Falkvinge, R. (n.d.). Who’s The police and who’s The crook, Anyway? *Torrent-Freak*. (12/06/2011). Retrieved from <http://torrenfreak.com/whos-the-police-and-whos-the-crook-anyway-110612> Accessed on August 3, 2011.

³⁵ Federal Deposit Insurance Corporation FDIC) (n.d.). *Putting an End to Account-Hijacking Identity Theft*. Retrieved from <http://www.fdic.gov/consumers/consumer/idtheftstudy/> Accessed July 16, 2011.

³⁶ Lennon, M. (2011). *New Online Ad Hijacking Scheme Discovered*. Security Week, Internet and Enterprise Security News, Insights & Analysis. Entrust, Securing Digital Identities & Information (June 6, 2011). Retrieved from: [_www.securityweek.com/new-online-ad-hijacking-scheme-discovered](http://www.securityweek.com/new-online-ad-hijacking-scheme-discovered). Accessed on August 6, 2011.

Co-operation in the Enforcement of Laws against Spam” in 2006.³⁷ Even though international organizations are co-operatively working together for securing information, it was stated in “the News of the World that a phone hacking scandal had catapulted the former volley ball player in spotlight”.³⁸ Is there hope as new technology tools to protect online privacy face risks of being freely hijacked?

In Canada, the Privacy Act of 1980³⁹ first attempted to legislate protection of citizen’s data. Currently data in Canada is protected under the Personal Information Protection and Electronic Documents Act (PIPEDA) supervised by the Privacy Commissioner of Canada, focusing on commercial activities exploiting consumers.⁴⁰ The Access to Information & Protection of Privacy Act (ATIPPA) protects personal privacy by preventing the unauthorized collection, use or disclosure of personal information by public bodies in Canada.⁴¹ The U.S. Family Educational Rights and Privacy Act (FERPA) required that student account information be private and protected. To meet this requirement, Peirce College in U.S. needed SSL encryption for all registration activities.⁴² Therefore, in the US, distance education (DE) and colleges encrypt to protect students’ personal information in compliance with the U.S. Privacy Acts. However, data privacy in the European Union (EU) governed by the Data Protection Directive states that the individuals collecting the personal information must give consent to the owners as to the collection and purpose of accessing their data.⁴³ Although, all measures are taken with the hope of securing information, there are still ways and means of going around the security measures. The Children’s Online Privacy Protection Act (COPPA) was passed by U.S. Congress in 1998, and came into effect in 2000.⁴⁴ The act states that personal information cannot be collected from children younger than 13 years without parents’ or legal guardians’ permission and sites must post clear privacy policy. A case in U.S. court held that Foreign Intelligence Surveillance Act (FISA) was violated against warrantless wiretapping because it was abusing personal privacy.⁴⁵ However, with government legislations and regulations, the information security was not coping

³⁷ Organization of Economic Co-operation and Development (OECD) (n.d.). Retrieved from <http://www.oecd.org/sti/security-privacy.pdf> Assessed on July 21, 2011.

³⁸ Watson, T. (2011). *Murdoch’s wife leaps to his defense during pie assault*. Deseret News, (July, 20, 2011). Retrieved from www.deseretnews.com/article/700164733/Mudochs-wife-leaps-to-his-defense-during-pie-assault.html Accessed on August 2, 2011. USA Today.

³⁹ Privacy Act, Canada (1980-81-82-83), c. 111, Sch, II “1”.

⁴⁰ Personal Information Protection and Electronic Documents Acts (PIPEDA) (S.C. 2000, c. 5).

⁴¹ Access to Information and Protection of Privacy Act (ATIPPA) (2002). *An Act to Provide the Public with Access to Information and Protection of Privacy*. SNL 2002 Chapter A-1.1.

⁴² Family Educational Rights and Privacy Act (FERPA) of 1974, US Law, retrieved from www.en.wikipedia.org/wiki/Family_Educational_Rights_andPrivacy_Act Accessed August 4, 2011.

⁴³ Data Protection Act 1998, Office of Public Sector Information, Retrieved from www.legislation.gov.uk/ukpga/1998/contents Accessed August 4, 2011.

⁴⁴ *The Child Online Privacy Protection Act (COPPA)*, 15 U.S.C. SS 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728.

⁴⁵ *Al-Haramain Islamic Found., Inc. v. Obama*, (2010). *District Court Limits the use of state secrets privilege in warrantless wiretapping*. No. 07-109 (N.D. Cal., Mar. 31, 2010).

with the fastest advancement of technological tools that led to hijacking and thus international organizations actions were established.

International Organizations actions

The international organizations, as explained above, collaboratively worked together to come up with common rules and laws to be applied globally for online privacy. The collaborative actions mandates for example, naming the few like the privacy international (PI) in UK, OECD, APEC, to aim for securing online privacy.

Privacy International (PI) “is a UK-based non-profit organization formed in 1990, as a watchdog on surveillance and privacy invasions by governments and corporations”.⁴⁶ PI aims and mandates have remained largely unchanged since its inception. Its objectives were to defend personal privacy and protection from intruders. PI works at national and international levels monitoring and finding ways through which IT can be used to protect privacy.⁴⁷

Organization for Economic Co-operation and Development (OECD’s) main focus was on collaborative co-operation forums for online privacy threats. It helped develop guidelines and policies on privacy issues.⁴⁸ Also, the Asian-Pacific Economic Cooperation (APEC) was also active in addressing privacy issues.⁴⁹ It encourages international co-operation with Canada, U.S., UK and other countries in addressing issues on online privacy risks. Online privacy was discussed at all levels to educate the public at large.⁵⁰ I observe that countries through collaboration, as noted by researchers above, were able to trace individuals causing problems like accessing information from computers and, for example, killing innocent people. On the other hand, as noted by the research above, since technology is non-neutral, there is no privacy.

Public Education attempts

Public education refers to means and ways of educating the public to be aware of online privacy laws.⁵¹ For example, the Office of the Privacy Commissioner of Canadian (OPC) mandate provides educational materials online to the public at large. They develop an awareness on online privacy issues for understanding risks and making choices about whom and how to share

⁴⁶ Privacy International (PI) (n.d.). In Wikipedia, The Free Encyclopedia. Retrieved from www.en.wikipedia.org/wiki/Privacy_International Accessed on August 5, 2011.

⁴⁷ Ibid #46.

⁴⁸ Ibid #37.

⁴⁹ Asia-Pacific Economic Cooperation (n.d.). In Wikipedia, The Free Encyclopedia. Retrieved from www.en.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation Accessed on August 5, 2011.

⁵⁰ Privacy International (PI), 2007, www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007 Accessed August 4, 2011. See Appendix C Leading Surveillance Societies in the EU and the World 2007: The 2007 International Privacy Ranking.

⁵¹ Office of the Privacy Commissioner of Canada (OPC) (n.d.). *Commissioner’s Message*. Retrieved from www.priv.gc.ca/aboutUs/message_e.cfm Accessed on August 5, 2011.

personal information.⁵² For instance, one of the US Electronic Privacy Information Centre's (EPIC) focuses on educating the public on information privacy issues.⁵³ The EDRI-gram in Europe also provides bi-weekly updates for the ongoing Internet and online laws and legislations that impact the European populace.⁵⁴ The majority of information provided include items for anonymous use, privacy policies, online tracking, protection levels for social networking sites (especially for minors), rights and freedoms for users, action recommendations, accountability and liability measures, copyright infringements and issues surrounding basic human rights and the parameters to protect all from harm while online.⁵⁵ Although there had been a lot of attempts at different levels, online privacy is still waning out. It thus becomes important to look at it (on-line privacy) in the context of distance education.

LESSONS LEARNED AND IMPLICATIONS FOR DISTANCE EDUCATION (DE)

DE refers to flexible on-line learning delivered to individuals accessing materials online and submitting their completed work on-line to instructors. It is a mode that surpasses all other educational delivery arrangement with its use of on-line with secured information using usernames and passwords.⁵⁶ For example, the tutor communicates online with the students sending them assignments, instructions, course outlines and examination results. The students access all online materials with their usernames and passwords. For example, at Memorial University (MUN) in Newfoundland and Labrador, the DE (Distance Education) students use their usernames and passwords to access online courses and register for courses online.⁵⁷ They login to MUN with their student numbers to create usernames and passwords. The DE tutor or instructor of the course sends assignments and assessments online to students. Students, can, however, reset their passwords if they had forgotten them. The question is how secure is their personal information? Who gives them a temporary number?

There is ample evidence in the literature suggesting that passwords and usernames are hijacked. A case in point is that of R. v. Cole (2009),⁵⁸ where the teacher and students' personal

⁵² Ibid #51 and Loukidelis, D. (2002). Information and Privacy Commissioner (June 27, 2002). Retrieved From <http://www.canlii.org/en/bc/bcipc/doc/2002/2002canlii42463.html> Accessed on July 27, 2011.

⁵³ EPIC, (n.d.). Focusing public attention on emerging privacy and civil liberties issues. Epic.org. *Electronic Privacy Information Centre* (August 3, 2011). Retrieved from <http://epic.org> Accessed on August 3, 2011.

⁵⁴ European Digital Rights, (2010). *Digital Rights in Europe: About European Digital Rights. EDRI-gram*. Retrieved from www.edri.org/about Accessed on August 5, 2011.

⁵⁵ Ibid #54.

⁵⁶ Moore, M., G. & Kearsley, G. (2005). *Distance Education: A Systems View* (Second ed.). Blemont, CA: Wadsworth. ISBN 0-534-50688-7. Allen, I.E. & Seaman, J. (2006). *Making the Grade: Online Education in the United States*. Needham, MA: The Sloan Consortium. ISBN 0987654321.

⁵⁷ Memorial University of Newfoundland (MUN) (n.d). *Appropriate use of computing resources*. Retrieved from <http://www.mun.ca/policy/site/policy.php?id=164> Accessed on August 3, 2011.

⁵⁸ Ibid #14.

information was accessed without their concern and police intervention without a warrant. Students too can commit technology crime to reverse mathematics equations during assessments.⁵⁹ The question is how students are able to hijack a system that has been encrypted and which can only be authenticated by the authorized owner? As is evidenced by the case⁶⁰ where a student accessed confidential information at the University of Alberta, there is clear evidence that usernames and passwords can be easily hijacked. The student in this case can change his/her marks or even access other sensitive personal information without the consent of the owner, in this case, other students.

In distance education (DE), students constantly come up with new ways to hijack into their Facebook/Myspace accounts at school, bypassing the school network's firewall even though protected with authenticated encryption (AE) for online privacy.⁶¹ This enables unauthorized access and or modifications to suit their needs without teachers' knowledge. The students are able to modify and also intrude Facebook personal information of others due to the way a virus is transmitted into the computer;⁶² this can be referred to as part of the dark side of the computer/Internet. Kim, Ok-Flan, Kim & So (2011)⁶³ described the dark side of the Internet attacks, costs and responses as the bad things the Internet has brought about – elements... that are illegal or unethical or at least reprehensible and prone to hijacking through phishing usernames and passwords.

It was argued that in the current online environment due to phishing and hijacking attacks even when best security practices are met, like user-names and passwords, there is no guarantee that online users like distance learners (students) would enjoy a safe online privacy environment.⁶⁴ Instead of us requiring users like students to maintain a malware-free, like from Trojan Horse viruses in their personal computers (PCs), and be able to detect complex phishing scams, we designed a technique that will largely protect user's information security even when the user performs sensitive Internet tasks from a compromised PC, and is uninformed regarding semantic attacks.⁶⁵ For example at MUN, Distance Education and Learning Technologies (DELT) uses McAfee software tool to protect students' online personal information. The McAfee is a software tool that automatically detects any malicious unacceptable activities into MUN's network.⁶⁶ However, technology tools like McAfee in MUN have been used to secure information from hijackers. Therefore, government, legislations and regulations with international organizations and public education played a part to collaboratively develop a means of hoping to protect

⁵⁹ Callow, R. (2010). *Students using technology to cheat: Is this a problem*. Sync.ca, (June 10, 2010). Retrieved from www.sync-blog.com/sync/2010/06/students-using-technology-to-cheat-is-it-a-problem.html Accessed on August 6, 2011.

⁶⁰ R. v. McLaughlin, (1980), 18 C.R. (3d) 339 S.C.C.).

⁶¹ Ibid # 12 and see Appendix B.

⁶² Ibid #12.

⁶³ Kim, W., Ok-Flan, J., Kim, C. & So J. (2011). The dark side of the Internet: Attacks, costs and responses, Computer and Information Science. *Information Systems Journal*, Vol. 36(3), p. 675-705.

⁶⁴ Ibid #36.

⁶⁵ Ibid #61.

⁶⁶ Ibid #57.

privacy, but there was an evidence that it was waning out. As noted by *Kyllo v. United States* (2001),⁶⁷ devices that can reveal unknown information without warrant violate privacy.

This paper has emphasized that people who use technology such as e-books, etc., are concerned with issues of personal privacy. In this context, issues of privacy, personal or confidential information still have to be properly addressed. People hope to be assured that their privacy is protected. This paper has provided evidence that this hope is waning out. This is so because private information can be hijacked due the following policy initiatives that are being taken in many countries. This paper points out that such initiatives will have serious implications for Distance Education (DE).

The legislations and regulations authorized online activities to be tracked.⁶⁸

- International organizations with different jurisdictions allow surveillance mandates to freely police all online activities.⁶⁹
- New ways of technological tools like ad hijacking were discovered and used to hijack online activities.⁷⁰
- For example, the way usernames and passwords are created leads to hijacking.⁷¹

Therefore, there is no hope for the security of on-line DE information, since what is considered secured information can now be accessed without owners' concern as far as the global surveillance laws are concerned. As noted by Geist, (2009), the proposed Canadian Bill on surveillance laws, allows ISPs free access on users' personal information, and to pass it to the police. As also noted by, US, RFIDs and Europe, the Sweden FRA Act on surveillance mandates to freely access all online activities.⁷² The surprising thing is that in spite of all the attempts with strategies collaboratively made by different jurisdictions and awareness mandates, some do not comply with the Human Rights Acts of Canadian Charter and European Human Rights Acts as discussed above.⁷³ The free access of users' personal information, due to surveillance issues, increases scamming thus, watering down the hope for online privacy. In addition to that, new technological tools are advancing very fast, thus leading to hijacking of online activities. For example, the new sophisticated technological ad-hijacking tools for attacking online activities was recently discovered as noted above.

No software program is perfect; errors are made, even if the errors have a low probability of occurring. Software manufacturers knowingly ship buggy products. These buggy products involve users who commit computer crimes and or abuses.⁷⁴ The abuses could be in the form of

⁶⁷ *Kyllo v. United States*, (2001). (533 U.S. 27).

⁶⁸ *Ibid.*

⁶⁹ *Ibid.*

⁷⁰ *Ibid.*

⁷¹ *Ibid.*

⁷² *Ibid.*

⁷³ Ovey, C., White, R.C.A. (2006). *Jacobs & White: The European Convention on Human Rights* (4th ed.). Oxford University Press. ISBN 0-19-928810-0.

⁷⁴ *Ibid.*

a hijacking like spam. Spam is unsolicited emails and leads to hijacking. While spam is a tool for identifying thieves, phishers, malware distributors and other fraudsters, it is also a tool for marketers.⁷⁵ For instance, in a study, it was estimated that unsolicited email comprised 90% of all email sent in 2007 – up from 50% in 2003 and only 10% in 2000 (Industry Canada, 2004).⁷⁶ Unsolicited commercial email spams everything from pharmaceuticals to directories. The economics of spam provide a strong incentive to spammers to continue the behavior. The cost of distributing spam is negligible; accordingly, it only takes a tiny number of email views to make the venture worthwhile. All these processes, decreases out online privacy and the question is, what next can be done?

SUMMARY AND RECOMMENDATIONS

The above discussion provided evidence that hope for online privacy has waned out. The technological tools used to protect online privacy like usernames and passwords are prone to hijacking. The main problem is that, as security measures on software tools are developed, at the same time the malicious hijacking tools are developed. In addition to that fact, the law enforcements, government regulations and legislations with public education, at the same time come up with laws that threaten online privacy. The question now is what next can be done?

Therefore, based on the discussions and evidences from case, the following recommendations were suggested:

- The surveillance mandates need to be addressed again because this was found to be one of the loopholes leading to username and password hijacking.
- Technological tools are developed by commercial organizations to attract consumers into buying their products. It is therefore of high importance for the different organizations and jurisdictions to collaboratively monitor and access the way the software is developed and used.
- Collaborative attempts to deal with the growing number of reported hijackings need to be continued. These could include legislation, user training and technical measures.
- There is need for ongoing training, assessment, protection, monitoring and detection, incident response and repair, documentation and review.
- The username and password creation needs to be looked into, because information protection with them is still prone to hijacking.

REFERENCES

Access to Information and Protection of Privacy Act (ATIPPA), (2002). *An Act to Provide the Public with Access to Information and Protection of Privacy*. SNL 2002 Chapter A-1.1

Al-Haramain Islamic Found., Inc. v. Obama, (2010). *District Court Limits the use of state secrets privilege in warrantless wiretapping*. No. 07-109 (N.D. Cal., Mar. 31, 2010).

⁷⁵ Ibid.

⁷⁶ Industry Canada, “An Anti-Spam Action Plan for Canada” (May 2004) [Industry Canada, “Anti-Spam Action Plan”]. Industry Canada, “Anti-Spam Action Plan”, note 109 *supra*. 60.

Allen, I.E. & Seaman, J. (2006). *Making the Grade: Online Education in the United States*. Needham, MA: The Sloan Consortium. ISBN 0987654321.

Anti-Spyware Coalition, (ASC) (2007). "Definitions and Supporting Documents"
<http://www.antispywarecoalition.org/documents/2007definitions.htm>> [ASC, "Definitions and Supporting Documents"]. Assessed on July 23, 2011.

Asia-Pacific Economic Cooperation, (n.d.). In *Wikipedia, The Free Encyclopedia*. Retrieved from www.en.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation Accessed on August 5, 2011.

Best, J. (2004). School children to be RFID-chipped. Silicon.com, Technology, Networks. (July 8, 2004). Retrieved from <http://www.silicon.com/technology/networks/2004/07/08/schoolchildren-to-be-rfid-chipped-39122042/> Accessed on August 3, 2011.

Callow, R. (2010). *Students using technology to cheat: Is this a problem*. Sync.ca, (June 10, 2010). Retrieved from www.sync-blog.com/sync/2010/06/students-using-technology-to-cheat-is-it-a-problem.html Accessed on August 6, 2011.

CBC NEWS, (n.d.). ISPs must help police snoop on Internet under new bill. *Technology & Science*. Quirks & Quirks Blog, Retrieved from (June 8, 2009).
<http://www.cbc.ca/news/technology/story/2009/06/18/tech-internet-police-bill-intercept-electronic-communications.html> Accessed on August 3, 2011.

Charles, G.O. (2009). *Safety versus Security in Fire Protection Planning*, The American Institute of Architects: Knowledge Communities, Retrieved from <http://www.aia.org/practicing/groups/kc/A1AB079791> Accessed on August 3, 2011.

The Child Online Privacy Protection Act (COPPA), 15 U.S.C. SS 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728.

Corbin, K. (2011). *House Panel Presses for ISP Data Retention Mandate*. Data Retention Tag Index. Datamation. Internet.com. Retrieved from www.datamation.com/tag/data-retention-69040.html Accessed August 4, 2011.

Data Protection Act 1998, Office of Public Sector Information, Retrieved from www.legislation.gov.uk/ukpga/1998/contents Accessed August 4, 2011.

Dignan, L. (2008). *The Gmail password hijacking incident: When so-called helpful apps hurt*. Retrieved from http://www.zdnet.com/blog/security/the-gmail-password-hijacking-incident-when-so-called-helpful-apps-hurt/936?tag=mantle_skin;content. Assessed on July 29, 2011.

European Digital Rights (2010). *Digital Rights in Europe: About European Digital Rights. EDRI-gram*. Retrieved from www.edri.org/about Accessed on August 5, 2011.

EPIC, (n.d.). Focusing public attention on emerging privacy and civil liberties issues. Epic.org. *Electronic Privacy Information Centre* (August 3, 2011). Retrieved from <http://epic.org> Accessed on August 3, 2011.

Family Educational Rights and Privacy Act (FERPA) of 1974, US Law, retrieved from www.en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act Accessed August 4, 2011.

Falkvinge, R. (n.d.). Who's The police and who's The crook, Anyway? *Torrent-Freak*. (12/06/2011). Retrieved from <http://torrenfreak.com/whos-the-police-and-whos-the-crook-anyway-110612> Accessed on August 3, 2011.

Federal Deposit Insurance Corporation FDIC), (n.d.). *Putting an End to Account-Hijacking Identity Theft*. Retrieved from <http://www.fdic.gov/consumers/consumer/idtheftstudy/> Accessed July 16, 2011.

Flaherty, D. (1989). *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill, U.S.: The University of North Carolina Press.

Geist, M. (2009). *Government introduces Bill to require surveillance capabilities, mandated subscriber disclosure*, (July 18, 2009). Retrieved from www.michaelgeist.ca/content/view/4069/125 Accessed on August 3, 2011.

Hepting v. AT & T, EFF, 2006, WL 2038464 (N.D. Cal. 2006). US 145997.

Hughes, L.J., Jr. (1995). *Actually Useful Internet Security Techniques*. New Riders Publishing (Indianapolis, IN).

Industry Canada, "An Anti-Spam Action Plan for Canada" (May 2004) [Industry Canada, "Anti-Spam Action Plan"]. Industry Canada, "Anti-Spam Action Plan", note 109 *supra*. 60.

Isenberg, D. (n.d.). House, Senate leaders back online surveillance. GigaLaw.com daily News. (January 27, 2011). Retrieved from <http://www.gigalaw.com/2011/01/27/house-senate-leaders-back-online-surveillance/> Accessed on August 3, 2011.

Jones, L. (2003). Kinkos's password hijacking case: Why you need RSA SecurIDs. Retrieved from <http://www.lesjones.com/2003/07/29/kinkos-password-hijacking-case-why-you-need-rsa-securids-3/> Assessed on July 29, 2011.

Kim, W., Ok-Flan, J., Kim, C. & So J. (2011). The dark side of the Internet: Attacks, costs and responses, Computer and Information Science. *Information Systems Journal*, Vol. 36(3), p. 675-705.

Kyllo v. United States, (2001). (533 U.S. 27).

Lennon, M. (2011). *New Online Ad Hijacking Scheme Discovered*. Security Week, Internet and Enterprise Security News, Insights & Analysis. Entrust, Securing Digital Identities & Information (June 6, 2011). Retrieved from www.securityweek.com/new-online-ad-hijacking-scheme-discovered. Accessed on August 6, 2011.

Lohr, K. (2010). How privacy can vanish online, a bit at a time, *The New York Times*.

Loukidelis, D. (2002). Information and Privacy Commissioner (June 27, 2002). Retrieved From <http://www.canlii.org/en/bc/bcipc/doc/2002/2002canlii42463.html> Accessed on July 27, 2011.

Lyon, D. (2007). *Surveillance Studies: An overview*. Cambridge: Polity Press. ISBN 978-0745635910.

Memorial University of Newfoundland (MUN) (n.d). *Appropriate use of computing resources*. Retrieved from <http://www.mun.ca/policy/site/policy.php?id=164> Accessed on August 3, 2011.

McMillan, R. (2008). "17 arrested in Canadian hacking bust" *PCWorld* >> Security (21 February 2008), http://www.pcworld.com/article/142711/17_arrested_in_canadian_hacking_bust.html [McMillan, "17 arrested"]. Assessed on July, 21, 2011.

Moore, M.G. & Kearsley, G. (2005). *Distance Education: A Systems View* (Second Ed.). Blemont, CA: Wadsworth. ISBN 0-534-50688-7.

Office of the Privacy Commissioner of Canada (OPC) (n.d.). *Commissioner's Message*. Retrieved from www.priv.gc.ca/aboutUs/message_e.cfm Accessed on August 5, 2011.

Organization of Economic Co-operation and Development (OECD) (n.d.). Retrieved from <http://www.oecd.org/sti/security-privacy.pdf> Assessed on July 21, 2011.

Ovey, C., White, R.C.A. (2006). *Jacobs & White: The European Convention on Human Rights* (4th ed.). Oxford University Press. ISBN 0-19-928810-0.

Password, (n.d.). In *Wikipedia, The Free Encyclopedia online*. Retrieved from <http://en.wikipedia.org/wiki/Password> Assessed on July 26, 2011.

Peltier, T.R. (2001). *Information security risk analysis*. Boca Raton, FL: Auerbach Publications. ISBN 0-8493-0880-1.

Peltier, T.R. (2002). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.

Personal Information Protection and Electronic Documents Acts (PIPEDA) (S.C. 2000, c. 5).

Privacy Act, Canada (1980-81-82-83), c. 111, Sch, II “1”.

Privacy International (PI), (n.d.). In Wikipedia, The Free Encyclopedia. Retrieved from www.en.wikipedia.org/wiki/Privacy_International Accessed on August 5, 2011.

R. v. Cole (2009). Ontario Superior Court of Justice, Toronto Region. Case Can LII 72331 (On SC). Retrieved from <http://www.canlii.org/en/on/osc/doc/2009/2009canlii72331> Accessed on July 28, 2011.

R. v. McLaughlin (1980), 18 C.R. (3d) 339 S.C.C.)

Schmidt, S. (n.d.). Most Canadians unaware of online tracking: privacy watchdog, *Postmedia News*, (May 5, 2011). Retrieved from <http://www.canada.com/technology/Most+Canadians+unaware+online+tracking+privacy+watchdog/4735324/story.html> Accessed on August 3, 2011.

SearchSecurity.com, (n.d.). *Hijacking*. Retrieved from www.serchsecurity.com/definition/hijacking Accessed on August 5, 2011.

SearchDataManagement.com, (n.d.). *Privacy*. Retrieved from <http://searchdatamanagement.techtarget.com/definition/privacy> Accessed on July 29, 2011.

Sharpened.net, (n.d.). *Glossary: Username*. Retrieved from www.sharpened.net/glossary/definition/username Accessed on August 5, 2011.

Sonne, P. (2011). U.K. *Protests Egypt Hijacking Text Network*. Retrieved from www.online.wsj.com/article/SB1000142052748704709304576123971737287928.html Accessed on August 4, 2011.

Stanley, J. & Stenhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*. Americas Liberties Union (ACLU). Technology and Liberty Program. New York, NY.

USA Patriot Act, 2001 (H.R. 3162) RDS, Focusing public attention on emerging privacy and civil liberties issues. Epc.org. *Electronic Privacy Information Centre*. Retrieved from <http://epic.org/privacy/terrorism/hr3162.html> Accessed on August 3, 2011.

Watson, T. (2011). *Murdoch's wife leaps to his defense during pie assault*. Deseret News (July, 20, 2011). Retrieved from www.deseretnews.com/article/700164733/Mudochs-wife-leaps-to-his-defense-during-pie-assault.html Accessed on August 2, 2011. USA Today.

BIBLIOGRAPHY

Anti-Phishing Best Practices for ISPs and Mailbox Providers” (Version 1.01, July 2006). http://www.maawg.org/about/publishedDocuments/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf Assessed on July 22, 2011.

Bellovin, S. Problem areas for the IP security protocols. In Proceedings of the Sixth USENIX Security Symposium (July 1996), pp. 1–16.

Bernstein v. U.S. Department of State 945 F. Supp. 1279 (N.D. Cal 1996).

Cai, X., & Gantz, W. (2000). Online privacy issues associated with Web sites for children, *Journal of Broadcasting and Electronic Media*, Vol. 44(2), 197-214.

Cai, X., & Gantz, W., Sshwartz, N., & Wang, X. (2003). Children's website adherence to the FTC's online privacy protection rule. *Journal of Applied Communication Research*, 31(4), 346-362.

CALEA Archive -- Electronic Frontier Foundation. Electronic Frontier Foundation (website). Retrieved 2011-06-29.

Criminal Code of Canada, R.S.C. 1985, c. C-46 (as amended) [*Criminal Code*].

Criminal Intelligence Service Canada, (n.d.). Retrieved from <http://online.mun.ca/d21/lms/discussions/messageLists/frame.d21?isShared=False&fid=36086&tid=100320&ou=80741> Assessed on July 21, 2011.

Data Protection, University Administration and Services (UAS). The Data Protection Act 1998, University of Oxford, UK.
<http://online.mun.ca/d21/lms/discussions/messageLists/frame.d21?isShared=False&fid=36086&tid=100320&ou=80741> Assessed on July 21, 2011.

Etzioni, A. (2000). Are new technologies the enemy of privacy? *Knowledge, Technology & Policy*, Vol. 20, 115-119.

European Data protection Servisor (EDPS), (n.d.). *The European guardian of personal data protection. What are my rights as a data subject?* Retrieved from <http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA5#rights> on July 9, 2011.

Friedlos, D. (2007). Online fraud to soar to £1.5bn. *Computing* (15 May 2007). Retrieved from <http://www.computing.co.uk/computing/news/2189932/online-fraud-soar-5bn> Assessed on July 23, 2011.

Government of Ontario, "Freedom of Information and Protection of Privacy act," Queen's Printer for Ontario, (2007). Retrieved from http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm.

Griffiths v. Nova Scotia (education), 2007 NSSC 178 (Can LII). The Supreme Court of Nova Scotia. Retrieved from <http://www.canlii.org/en/ns/nssc/doc/2007/2007nssc178/2007nssc178.html> Accessed on July 28, 2011.

Ha, Thanh, T., (2008). "Ring invaded computers in 100 countries, police say", *The Globe and Mail* (21 February 2008).

Katz, R.N. (2002). "The ICT infrastructure: A driver of change." *EDUCAUSE*, 52-60. Memorial University of Newfoundland (MUN) (n.d). Retrieved from <http://www.mun.ca/distance.mun.ca/forms/support/step1.php> Accessed on July 24, 2011.

Michigan Department of Technology, Management & Budget, DTMB, (n.d.). <http://online.mun.ca/d21/lms/discussions/messageLists/frame.d21?isShared=False&fid=36086&tid=100320&ou=80741> Accessed on July 21, 2011.

Nova Scotia Freedom of Information and protection of Privacy Review Office (n.d.). Retrieved from <http://www.foipop.ns.ca/> on July 9, 2011.

Privacy in Research Ethics & Law, Canada: data protection, (n.d.). Retrieved from <http://www.privereal.org/content/dp/canada.php> on July 9, 2011.

Schiffman, N. (2007). "Metamorphic malware sets new standard in antivirus evasion" *SearchSecurity.com* (8 February 2007), http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1264968,00.html>. Assessed on July 23, 2011.

Shade, L.R. (2008). Reconsidering the right to privacy in Canada. *Bulletin of Science, Technology & Society*, Vol. 28(1), 80-91.

Shou, C. (1996). Handbook of INFOSEC Terms, version 2.0. CD-ROM (Idaho State University & Information systems Security Organization).

Symantec, "Security Update - July 2005: Worldwide and Americas" (July 2005), http://www.symantec.com/avcenter/reference/SSU_AMS_07_2005.pdf Assessed on July 23, 2011.

University of Victoria, Re, 2002 CanLII 42463 (BC IPC).

University of Tennessee: Unauthorized access. Retrieved from https://my.tennessee.edu/portal/page?_pageid=40,614533&_dad=portal&_schema=PORTAL, on July 9, 2011.

Wilson, C. (2008). Congressional Research Services, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" (29 January 2008).

Zhang, Y. & Egelman, S., Cranor, L.F. and Hong, J. (2007). Phishing phish: An evaluation of anti-phishing toolbars. *In Network and Distributed Systems Security Symposium (NDSS'07)*, San Diego, CA, USA, Feb. 2007.


Zurko, M.E. (2005). User-centered security: Stepping up to the grand challenge. In *Annual Computer Security Applications Conference (ACSAC'05)*, Tucson, AZ, USA, Dec. 2005. Invited Essay.

APPENDICES

Appendix A: Computer Crimes – Destructive Code. See Fig. 9.13, How a Computer Virus is Spread, © 2008, Pearson Education Canada. Thus, this figure is not included here.

Appendix B: Unauthorized Access. Thus, see: Survey by Computer Security Institute *Information Systems Today, 2/C/e, 2008 Pearson Education Canada*

Appendix C: Leading Surveillance Societies in the EU and the World 2007: The 2007 International Privacy Ranking

Privacy International																					
National Privacy Ranking 2007 - Leading Surveillance Societies Around the World																					
	Constitutional protection	Statutory protection	Privacy Enforcement	Identity Cards and Biometrics	Data-sharing	Visual surveillance	Communication interception	Communication Data Retention	Government Access to Data	Workplace monitoring	Surveillance of Medical, Financial, and Movement	Border and Trans-border Issues	Leadership	Democratic safeguards	Total	Last Year's Ranking	This Year's Ranking	Change			
EUROPEAN UNION																					
GREECE	4	3	4	3	-	3	1	-	3	-	3	-	4	3	3.1						
ROMANIA	3	3	4	-	-	-	-	2	3	2	-	-	2	4	2.9						
HUNGARY	4	4	4	4	3	1	1	4	3	2	2	3	1	4	2.8						
SLOVENIA	4	4	4	2	3	4	2	1	2	4	2	-	2	3	2.8			Improving			
PORTUGAL	4	4	3	2	2	2	2	-	-	3	3	-	2	4	2.8						
LUXEMBOURG	2	3	3	3	2	2	2	3	-	4	4	-	1	4	2.8			Deteriorating			
GERMANY	4	4	4	2	4	2	2	1	3	2	4	2	1	4	2.8						
ITALY	4	4	4	2	-	3	1	1	2	4	2	3	3	3	2.8						
ESTONIA	3	3	4	2	-	-	2	-	3	-	3	-	2	3	2.8						
BELGIUM	4	4	4	1	1	-	2	2	3	4	3	2	1	4	2.7			Deteriorating			
CZECH REP.	4	3	4	2	1	2	1	2	2	3	2	2	3	4	2.5			Deteriorating			
FINLAND	3	3	3	2	1	-	3	3	2	2	2	2	2	4	2.5						
IRELAND	2	3	4	2	2	-	3	1	2	3	3	2	1	4	2.5						
MALTA	2	4	3	-	-	-	2	-	2	-	-	-	2	2	2.4			Deteriorating			
POLAND	3	4	3	1	3	2	1	1	2	-	2	-	3	2	2.2			Deteriorating			
SPAIN	3	4	4	1	-	2	1	2	2	3	1	-	1	4	2.3			Deteriorating			
AUSTRIA	2	3	2	2	1	2	2	4	2	-	3	2	1	4	2.3			Deteriorating			
CYPRUS	3	3	3	2	-	2	1	-	-	-	2	2	2	3	2.3			Deteriorating			
EU	3	2	3	2	2	-	-	1	2	-	3	2	2	3	2.3			Deteriorating			
LATVIA	2	4	4	1	1	2	-	2	3	2	2	2	2	3	2.2			Deteriorating			
NETHERLANDS	2	4	4	1	1	2	1	1	2	4	2	1	2	1	4	2.1					
SLOVAKIA	4	3	3	1	-	-	2	1	1	-	2	-	2	2	2.1						
SWEDEN	3	2	3	3	2	3	2	1	1	1	1	2	1	4	2.1			Deteriorating			
DENMARK	3	2	2	4	1	3	2	1	1	-	1	1	2	3	2.0			Deteriorating			
BULGARIA	3	2	3	1	-	-	1	2	2	-	2	-	2	2	2.0			Deteriorating			
LITHUANIA	3	3	2	1	-	1	1	3	2	1	-	-	2	3	2.0			Deteriorating			
FRANCE	3	2	3	2	1	2	2	1	1	-	2	1	1	4	1.9			Deteriorating			
UK	1	2	2	1	1	1	1	1	2	2	1	1	1	3	1.6						
England & Wales	1	2	2	1	1	1	1	1	2	2	1	-	1	2	1.4						
Scotland	1	2	2	3	3	2	-	-	3	-	2	-	3	4	2.5						
INTERNATIONAL																					
CANADA	4	4	2	2	2	2	3	4	3	3	2	2	3	4	2.8			Deteriorating			
ARGENTINA	4	4	2	-	-	-	2	2	-	-	2	-	4	3	2.8						
ICELAND	4	4	4	2	3	2	3	2	2	3	2	1	2	4	2.7						
SWITZERLAND	4	4	2	2	2	1	2	2	2	-	2	1	3	4	2.4						
NEWZEALAND	2	2	3	3	2	-	1	3	2	2	2	2	2	4	2.3						
SOUTH AFRICA	4	1	1	2	2	-	2	1	-	-	4	2	-	4	2.3						
JAPAN	3	1	1	2	2	2	3	4	3	-	3	1	1	3	2.2						
AUSTRALIA	1	2	2	3	2	-	2	4	2	3	1	1	2	3	2.2						
ISRAEL	4	3	3	2	2	2	2	2	1	-	1	1	2	3	2.2						
BRAZIL	3	2	1	2	2	2	2	2	2	3	1	2	3	3	2.1						
NORWAY	3	2	3	2	1	2	2	2	2	3	1	1	2	4	2.1						
INDIA	3	1	1	-	-	-	1	-	1	-	2	-	2	4	1.9						
PHILIPPINES	3	2	1	1	-	-	1	2	1	-	2	-	2	3	1.9			Deteriorating			
US	3	1	1	1	2	1	1	3	2	1	1	1	1	2	1.5			Deteriorating			
THAILAND	2	2	2	1	-	2	1	2	1	-	1	1	2	1	1.5			Deteriorating			
TAIWAN	2	2	1	1	-	-	1	3	2	-	1	1	1	2	1.5						
SINGAPORE	1	1	1	1	2	1	1	3	1	1	3	2	1	1	1.4						
RUSSIA	3	2	1	2	1	-	1	1	1	-	1	1	1	1	1.3						
CHINA	2	2	1	2	1	1	1	1	1	-	2	-	1	1	1.3						
MALAYSIA	1	2	1	1	1	1	1	3	1	-	1	1	2	1	1.3						
GRADE																					
5	no invasive policy or widespread practice/leading in best practice															FINAL SCORE	4.1-5.0	Consistently upholds human rights standards	CHANGE	Improving	Country has improved since last year
4	comprehensive efforts, protections, and safeguards for privacy															3.6-4.0	Significant protections and safeguards	Deteriorating	Country has dropped by one category		
3	some safeguards, relatively limited practice of surveillance															3.1-3.5	Adequate safeguards against abuse	Decaying	Alarming rate of fall in protections		
2	few safeguards, widespread practice of surveillance															2.6-3.0	Some safeguards but weakened protections				
1	extensive surveillance/leading in bad practice															2.1-2.5	Systemic failure to uphold safeguards				
															1.6-2.0	Extensive surveillance societies					
															1.1-1.5	Endemic surveillance societies					

Privacy International (PI), 2007, www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007 Accessed August 4, 2011.