How Technology Affected Our Privacy

Sehnaz Ahmetoglu[1], Akram Khedher[2]

Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia, Kuala Lumpur, Malaysia

Abstract: *After the recent spread of the Internet, many technology terms appeared like Smartphone, social media and cloud computing. Flexibility in use this technology encourage people to communicate and share their information in all kinds: photos, videos, documents and sometimes sensitive information like bank account. Annually we note the increased number of users of this technology to be arrived over billions of users. Most of these users are public which they do not realize ambiguity of technology and therefore easier to access their information. The abundance of information and poor knowledge of users about privacy led to the emergence of numerous threats and fears under this term. Thus, the importance of educating people about privacy issues and related risk factors become essential. This paper views the definition of privacy and what level of awareness should be applied. With try to understand some security issues and related laws. And compare between two different privacy laws.*

Keywords: Privacy, Security Issues, Privacy Law, Privacy Awareness, Laws.

1. Introduction

Internet and its related technology have changed our lives to the better. It has made access to information, businesses and communication with people much easier and convenient. It is a means of communication with anyone anywhere, sharing all kinds of information. However, the benefits from this technology does not devoid it from risks. The popularity of using social technologies has grown to 1.96 billion active users in 2015 and it is expected that to be 2.44 billion users in 2018.[1] This increasing number has led to the increase of number of reports regarding hacking and identity violations.[2] Over the past few years, technology users have been aware about security and privacy. Understanding the value that individuals assign to the protection of their personal data is of great importance for business, law and public policy.[3]

The challenge here is how the public users understand the privacy policy in several of network application and how they can benefits from technology without exposing their information to danger. Furthermore, the level of responsibility in the organizations in defending their policies [4].

2. Literature Review

Technology is impacting the world today. It will soon become very easy for businesses, governments and other institutions to watch and store all the significant information of an individual, be it whereabouts, salaries, interests, activities etc. . Not only will they be tracking convicts, felons and terrorist, they will be tracing everyone. Even at this moment, information about us are being discovered, recorded, arranged and analyzed by super machines and on a massive scale.[5]

Steve Rambam, CEO of a successful private investigation company provide a slide show with the title ―Privacy is Dead – Get Over It.‖. He discusses great proof and cases of how easy it is to find and gather thorough information of the private life of practically any random individual in the United States by using a computer and accessing to open public databases. In 2006, he made a case study called ―mystery man‖ to support his statements. He took the name, email address and phone number from volunteer. With four and one-half hours in front of his computer he recovered elaborate and detailed profile relating to the many parts of the mystery man's private life from many different databases [5]. Furthermore, Gehrke and his colleagues founds that in today's information age, data privacy is a fundamental problem. Huge amounts of data are stored in databases that are collected by government agencies, search engines, social networks, hospitals, financial institutions, and other organizations. As there are enormous social benefits in analyzing this data; it is important that sensitive information about individuals who have given the data should not be leaked to others [6]. Information is given away every time consumers browse the internet, log on and post to a social media site, or shop online, voluntarily — and sometimes involuntarily. Organizations happily collect these bits of information to keep track, market and sell to their customers. However, both consumers and organizations leave themselves open to vulnerabilities to dishonest individuals that collect this data for themselves [7]. unfortunately, people who share sensitive information through the internet are not aware of the privacy risk associated with it [8]. So that people whose personal information has been shared to other people, their privacy concerns will be raised [9][10].

From here, laws against violators has been issued in order to lessen the amount of privacy invasion.

3. Privacy: Definition and Awareness

Privacy in general is the state or condition of being free from being observed or disturbed by other people. And it is defined as ―the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others‖. Another definition is ―A fundamental human right‖ as defined in the 1950 European Convention of Human Rights. And in this information evolving age, privacy has been one of the most important human right issues. Users should have a clear differentiate between Privacy and Security they are not synonymous. Informational privacy has two main points: 1. The right to be left alone; 2. The right to decide oneself what to reveal about oneself [11]

Paper ID: NOV151933

406

This definition and Description consider the importance of privacy to the users in their life and business. In recent time, the use of technology was in the form of expanding the number of one's business and relationships, it can be used in different fields.[1] User should be awake about their privacy they need to be careful when they provide their personal information in online sites.[4]

Privacy is not just a personal issues, it is a common matter between public, organizations and governments. Figure 1 demonstrate that our information in different area.
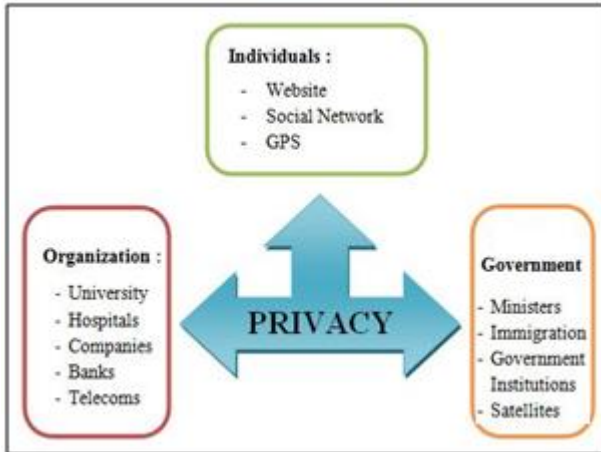

Figure 1: Privacy and Information sector.

In an attempt to emphasize privacy protection it should be a top priority:

- To Providing courses and raising awareness on security using social networks.
- User should be self-aware about privacy when using the internet.
- Users need to be familiar in read privacy conditions which is provided by the website, social network or organizations and make sure about their default privacy.
- Create a culture that understands the fundamental importance of privacy beyond reciting the organization's policies.[7]
- Organizations should focus on privacy accountability on an ethical path as well as adhere to aligning with suggestions from regulators, and instilling the importance of privacy within their employees [7]
- The governments need to apply a strategic approach with organizational demands for personal information in order to make balance between them and privacy for program management and service delivery.[12]
- Privacy Laws should be known to the public in order to educate them about their rights.

In 2013, the Office of the Privacy Commissioner of Canada made a Survey of Canadians on Privacy-Related Issues. They asked people: How would they rate their knowledge of their privacy rights under the various laws protecting their personal information they found people have limited knowledge about privacy laws and the rate of their good knowledge was increase slowly between 2001 and 2012. Figure 2 shows the different rate in Canadians knowledge about privacy rights. [13]
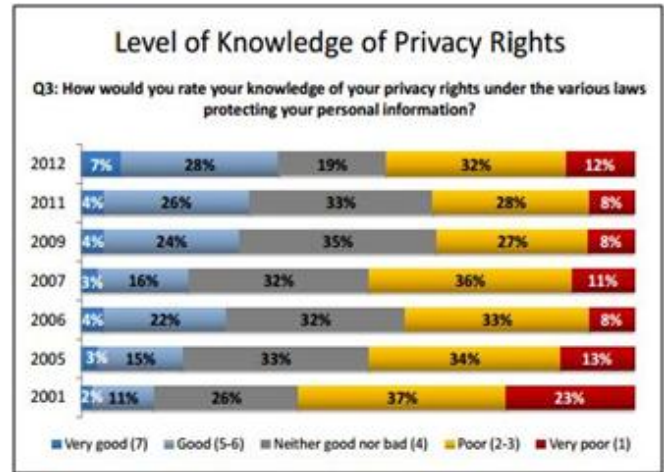

Figure 2: Level of Knowledge of Privacy Rights.[15]

4. Security Issues and Privacy

The use of computer technology allowed to increase the security issues related to privacy in electronically transmitted and stored information. The most important issue is about the use of this information only in a particular purpose without any being exposed or accessed.[14] Privacy focusing on the individual's capability to manage the collection, use, and dissemination of their personal information, while security presents the method to ensure confidentiality and integrity of information, and the availability of information technology systems. To avoid this kind of issues organizations and governments need to apply a high level of security guiding which includes: Confidentiality, Integrity and availability (see figure 3). However, privacy and security are not interchangeable, but privacy is a field of security. For instance IT controls ensure the confidentiality and integrity from a security perspective which support privacy objectives.[15]

In an individual's level there are other security issues that rise in terms of privacy. Extortion cases, Impersonation and Theft of bank accounts are common issues related to privacy which depends on personal information. In a Canadians privacy survey they found that Financial information (bank fraud), Computer privacy (internet security), Identity theft (identity fraud) and Personal information being accessed (general) are the top four risks in privacy that concerns the people the most [13]. The increasing amount of these kind of issues, led privacy regulators, governments and international corporations to keep pace with this matters by upgrade the privacy laws to be in line with the technology and the issues related to. [7]
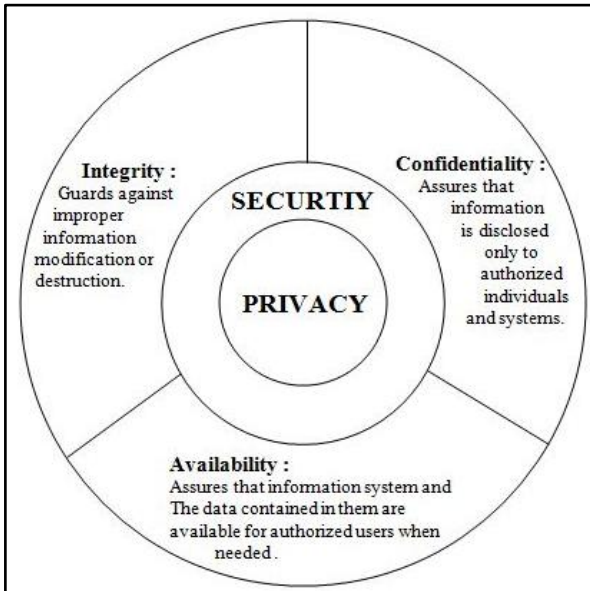
Figure 3: Privacy and Security guiding.

5. Privacy Laws

First we start with privacy law definition ─it is the act to protects a person's right to be left alone, and governs collection, storage, and release of the financial, medical, and other personal information".[16] This act handled by the government Information Commissioner regulations and it shall be applied in the Penal Law of the State. The protection of personal data contain [17]:

- Personal information include information or an opinion (forming part of a database). it does not include any sensitive data.

- Sensitive information consist of personal information or an opinion about an individual's such as name, address, political opinions and health information.

In this section we will make a comparison between privacy law in Australia and Canada in terms of:
- Data Collecting and Processing
- Data Transfer
- Data Security

Australia, data privacy is ruled at the federal level by the Privacy Act of 1988 (the ─Act"). The Act ─applied to Commonwealth, Australian Capital Territory government entities, and credit reporting organizations and private sector organizations and businesses that earn more than $3 million annually"[17][18]. Table 1 will introduces the privacy law applied for Data (Collecting, Transfer and Security) in Australia.

In Canada, they used federal law called Personal Information Protection and Electronic Documents Act, S.C 2000, c. 5 (─PIPEDA") which is focus on how private sector organizations are allowed to collect, use or disclose personal information in the course of commercial activities. PIPEDA also applies to federal works, in regards of undertakings and businesses in respect of employee personal information [17][19]. We can see how this law applied in data sector from table 2.

Table 1: Privacy Law in Australia.

Data Privacy	Laws
Collecting and Processing	- An organization covered by the Act is prohibited from collecting personal information unless that information is necessary for one or more of its functions or activities. - An organization must generally collect personal information about an individual only from that individual. - An organization cannot use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless it obtains the individual's consent. - Consent is not necessary where: ✓ The information is not sensitive information and the use of the information is for the secondary purpose of direct marketing. ✓ the information is health information and its use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety [17:7].
Transfer	- A record-keeper in possession of personal information is prohibited from disclosing that information unless the: ✓ individual concerned has consented to the disclosure; ✓ record-keeper reasonably believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person; ✓ disclosure is required or authorized by law; or enforcement of criminal law. - Third parties cannot use or disclose the information they have been given for a purpose other than that for which they were given the information. - International Data Transfer. An organization is prohibited from transferring personal information to another organization in another country unless for special case such as that the recipient of the information is subject to a law [17:9].
Security	An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure. An organization must also take reasonable steps to destroy or permanently de‑identify personal information if it is no longer needed for any purpose for which the information originally could be used or disclosed under the Act [17:10].

Paper ID: NOV151933

Table 2: Privacy Law in Canada.

Data Privacy	Laws
Collecting and Processing	• An organizations required that subject to the laws only collect, use and disclose personal information for ~~purposes~~ that a reasonable person would consider are appropriate in the circumstances". • The certain exceptions, require an individual's consent prior to the collection, use, and disclosure of the individual's personal information. (The exceptions are different as to each of ~~collection,"~~ ~~use,"~~ and ~~disclosure"~~ without knowledge or consent.) • There is a more flexible standard for consent under PIPEDA, and consent may be either implicit or explicit, oral, or in writing, including through electronic means . • Organizations required that identify the purposes for which personal information will be collected at or before the time of collection and make available the organization's personal information collection, use, and disclosure practices. • The Canadian Data Protection allow individuals the right to access personal information held by an organization (subject to certain exceptions) and to correct any inaccuracies or required updates concerning the personal information held by the organization . • Special Considerations Regarding Employee Data: the collection, use, and disclosure of employee personal information is generally subject to the same rules. There are, however, often more strict consent requirements in the employment context due to the nature of the employee/employer relationship [17:29].
Transfer	• When an organization transfers personal information outside of the organization, it remains responsible for the protection of the personal information and ensuring compliance with the applicable statutes. Stricter, more specific requirements under the provincial laws also may apply to data transfers, particularly if transferring outside of Canada. • PIPEDA itself does not distinguish between international and domestic transfer. Therefore, in accordance with the principles on the use of data under PIPEDA, so long as the transfer is consistent with the use for which the data was originally collected, consent to transfer the data is not required. If not, consent would be required . • Service Providers. The Canadian Data Protection Statutes generally allow organizations to transfer personal information to third-party service providers, subject to certain additional requirements. Organizations must ensure the same level of protection by a third party through contractual agreement or otherwise. These contractual agreements typically require adherence to the Canadian Data Protection Statutes and may include indemnification provisions, liquidated damages, and other relief in the event the third party fails to comply with privacy law requirements [17:31].
Security	The Canadian Data Protection Statutes require that organizations appoint a position/individual who is responsible for the organization's compliance with the requirements under the various applicable laws also they require reasonable measures to protect personal information against theft, other loss, and unauthorized collection, access, disclosure, copying, use, destruction, or modification [17:32].

From these two tables we can find, privacy has now become an embedded part of public relations, organizations and governments. Each country have their own laws, they are similar in content but differ in the way they apply according to the percentage of the issues related to the privacy appeared in a specific country.

6. Contribution to Research

This study has showed that information privacy on the internet is a subject not commonly known or spread to the public, even though a huge amount of people use it every day. And the more people not knowing about it, the more risks they put themselves into. Hence, the rise of internet privacy laws, which forces government and organizations into protecting individuals' information and not share it without their consent.

Furthermore, despite the similarities in the privacy low acts in different countries, the application of the laws are in fact dissimilar.

7. Recommendation and Conclusion

In conclusion, the increase amount of Internet and Technology users raise the importance to educate people about their information privacy to limit the security issues that appeared in this case. In this paper, we have briefly define privacy and privacy laws and what are the security

issues related to privacy. Then, we made a comparison between Australia and Canada's privacy law. This comparison explained different laws used in these countries. As they are similar in content but differ in the way they apply according to the percentage of the issues related to the privacy appeared in the country. Finally, we recommend that to increase the awareness about privacy for people, include privacy rights and policies in all computer curriculum in schools to let the awareness message reach the biggest amount of people and provide different workshops for the employees which is expands their awareness about the organization privacy policies by invite some participants to share their individual experiences.

References

[1] Ahmetoglu, S. Al-Yami, N. Ibrahim, J (2015). " The Impact of Social Network Technology on Business ". International Journal of Science and Research (IJSR). Volume 4 Issue 4. Retrieved from http://www.ijsr.net/archive/v4i4/SUB153876.pdf

[2] Carolyn. B, Clare, M. Feng, J (2005). "Usable Security and Privacy: A Case Study of Developing Privacy Management Tools". Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.6437&rep=rep1&type=pdf

[3] Acquisti, A. John, L. Loewenstein, G . "What is privacy worth? ". Heinz College. Retrieved from

Paper ID: NOV151933

409

http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-worth.pdf

[4] Chewae, M. Hayikader, S. Hasan, M. Ibrahim, J (2015). " How Much Privacy We Still Have on Social Network?". International Journal of Scientific and Research Publications, Volume 5, Issue 1. Retrieved from http://www.ijsrp.org/research-paper-0115/ijsrp-p3755.pdf

[5] Gordon, M. (2012). " Do we still want privacy in the information age". American Civil Liberties Union of Oregon (ACLU). Retrieved from http://www.aclu-or.org/sites/default/files/Privacy_Digital_Age_Paper.pdf

[6] Gehrke, J. Lui, E. Pass, R. " Towards Privacy for Social Networks: A Zero-Knowledge Based Definition of Privacy". Retrieved from http://www.cs.cornell.edu/~luied/zkPrivacyFinal.pdf

[7] EY Company. (2014). "Privacy trends 2014 Privacy protection in the age of technology". Insights on governance, risk and compliance. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

[8] Srivastava, A . Geethakumari, G. (2013) "Measuring Privacy Leaks in Online Social Networks," International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100, 2013.

[9] Srivastava, A . Geethakumari, G. (2013). "A Framework to Customize Privacy Settings of Online Social Network Users," IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 187-192, 2013.

[10] Dhami, A. Agarwal, N. Chakraborty, T. Singh, B. Minj, J (2013). "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," 3rd IEEE International Advance Computing Conference (IACC), pp. 465-469, 2013.

[11] Blarkom, G. Borking, J. Olk, J. "Handbook of Privacy and Privacy-Enhancing Technologies". The case of Intelligent Software Agents. Retrieved from http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

[12] Bennett, C (2001) . " What Government Should Know about Privacy: A Foundation Paper". Retrieved from http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf

[13] The Office of the Privacy Commissioner of Canada (2013). "Survey of Canadians on Privacy-Related Issues". Retrieved from https://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.pdf

[14] Parliament of Victoria . "Security and Privacy issues relating to technology and law ". Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/lawrefrom/technology/barisic_paper.pdf

[15] MITRE Corporation. (2013). "Privacy Systems Engineering". Retrieved from http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive-enterprises/privacy-systems-engineering

[16] Business Dictionary. "Privacy Law". Retrieved from http://www.businessdictionary.com/definition/privacy-law.html

[17] Baker Hostetler. (2015). "International Compendium of Data Privacy Laws". Retrieved from http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

[18] Australian Government, Office of Australian Information Commissioner. " The Privacy Act". Retrieved from http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act

[19] Office of the Privacy Commissioner of Canada. "The Personal Information Protection and Electronic Documents Act (PIPEDA)". Retrieved from https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

[20] Office of the Privacy Commissioner of Canada. "A Guide for Individuals - PROTECTING YOUR PRIVACY ". An Overview of the Office of the Privacy Commissioner of Canada and Federal Privacy Legislation. Retrieved from https://www.priv.gc.ca/information/pub/guide_ind_e.pdf

Paper ID: NOV151933

410