The ISC Int'l Journal of Information Security
ISeCure

August 2019, Volume 11, Number 3 (pp. 19–27)
http://www.isecure-journal.org

SELECTED PAPER AT THE ICCMIT'19 IN VIENNA, AUSTRIA

A Sudy on Information Privacy Issue on Social Networks☆

Soran Ibrahim [1], and Qing Tan [2,*]
[1] *Master of Science in Information Systems (MSc IS), School of Computing and Information Systems, Athabasca University, Canada*
[2] *Associate Professor, School of Computing and Information Systems, Athabasca University, Canada*

ARTICLE INFO.

Keywords:
Social Networks, Social Media,
Personal Privacy, PIPEDA
Privacy Laws

Abstract

In the recent years, social networks (SN) are now employed for communication and networking, socializing, marketing, as well as one's daily life. Billions of people in the world are connected though various SN platforms and applications, which results in generating massive amount of data online. This includes personal data or Personally Identifiable Information (PII). While more and more data are collected about users by different organizations and companies, privacy concerns on the SNs have become more and more prominent. In this paper, we present a study on information privacy in SNs through exploring the general laws and regulations on collecting, using and disclosure of information from Canadian perspectives based on the Personal Information Protection and Electronic Document Act (PIPEDA). The main focus of this paper is to present results from a survey and the findings of the survey.

1 Introduction

In the resent years, SNs have been grown tremendously and have attracted many users including individuals, businesses, organizations, and governments. According to the statistic by Statista, the number of users who will be using different SNs such as Facebook, LinkedIn, Google+ is globally expected to rise from the 2.62 billion in 2018 to around 2.77 billion users in 2019, and to over 3 billion users by 2021 [2]. The report indicates that SNs are highly popular in North America in which about 66% of entire SN users in the world are located in North America [4]. As a result, SN has forever changed the way that people communicate, share ideas, express their beliefs and political views. Today, various governments and businesses are using SN for public relation management; client's interaction and targeting; product promotions; advertisements; and in expanding business and service operations both locally and globally [17]. Because of the easy usage of the public nature, and the social environment, SNs provide users a comfortable way to disclose considerable amount of information about themselves and about their connections with other users, which may include Personally Identifiable Information (PII). This information can be used to identify a user by his location, date of birth, personal photos, work place etc [13].

However, many users of SNs may not be fully aware

☆ The ICCMIT'19 program committee effort is highly acknowledged for reviewing this paper.
* Corresponding author.
Email addresses: Soran.ibr@gmail.com, qingt@athabascau.ca

ISSN: 2008-2045 © 2019 ISC. All rights reserved.

of how public sharing of their personal information may negatively impact their personal privacy. In addition, as more and more data are collected about massive SN users by different organizations and companies, the violation or compromise of information privacy and personal privacy becomes more serious[20]. Under other conditions, government and law enforcement can also add negative impact on the privacy issues as they may request users' information from SN companies [22]. As a result, more people than ever are concerned about their privacy today, especially people with proper educational background, recognize the damaging nature of sharing PII and the data collection. Earlier research in this area have underlined the following threats to information privacy [15];

- Sharing personal information by users that is completely accessible without any access restriction.
- User's unawareness of privacy boundaries, SNs' privacy policies and government privacy laws.
- SN system design and framework flaws, installing and granting third-party applications access to personal information without knowing the extent of the permission being granted.

Protecting information privacy of SN users has become a necessity from users' perspective and a key requirement for SNs since vast amount of personal information is exchanged and shared between uses over SN platforms This is due to the fact that information can easily be shared beyond intended audience. The recent incident of Facebook- Cambridge Analytica data hijacking clearly shows the importance of personal information protection on SNs. Almost all SNs provide privacy setting tools and control mechanisms that can be used to protect personal information and manage the level of user's information disclosure to other. It is important for users to be aware of the availability of privacy setting tools, to understand the meaning of all those settings and to be able to utilize them to protect their privacy. However, an earlier research indicates that most people and organizations are still unaware of the potential privacy risks to their private information [19]. Other research has shown that most users would take the privacy issue seriously only after they realize that their personal privacy is breached[11]. While other users are "aware of privacy features and know how to use them, but they do not take initiative actions to protect their information" [13].

Federal privacy laws and regulations in Canada such as PIPEDA and digital privacy acts do not protect information privacy at personal level as they govern the collection, use and disclosure of information privacy in both private sectors and federal government agencies respectively. Although our findings show that these laws and regulations have no specific guidelines that clearly and directly protect personal information on the SNs, users should be aware of the existence of these laws and how to use them when privacy violation occurs.

In this paper, we highlight two privacy perspectives: information protection laws in Canada and privacy awareness. These two topics are analyzed and assessed as we try to understand whether the current in effect rules and regulations protect and enforce the information privacy of users on SNs. We also investigate what impact SN has on users' privacy awareness, and how the awareness affects users' information sharing, online behaviour and trust. The reminder of the paper is organized as follows: in section 2, we briefly review related literature and research related to our study, especially research related to information protection laws and privacy awareness. We then present our empirical study on the privacy laws and regulations in section 3. Next, we discuss the findings of the study in section 4, and finally we will provide the conclusion in section 5.

2 Relared Work

Li and Qian [17], studied the relationship between users' actual behaviour and their perception of security risks on SNs. When it comes privacy, they argued that if SN's users are not careful when disclosing personal information on the sites, their privacy can easily be violated. They proposed to develop a system that can aware users when there is a security risk and recommend the users to mitigate the risk of negative behaviors on SNs.

Cherie and Responds [8], reminded SN users to be aware of privacy policy and terms of use. They advised users to continuously manage their privacy setting and have some sort of control over their publicly or privately shared contents in terms of who, what or when the contents are viewed since users don't really own any of their information saved on SN space.

K. Li, Lin, and Wang [16], investigated the effect of users' different profile features on privacy disclosure behaviours and patterns on SNs based on users' age and gender. The scholars collected the data from SN sites. Then analyzed the data based on breath and depth of privacy disclosure, less sensitive and highly sensitive privacy disclosures. Their findings indicated that age has a negative impact on privacy disclosure. Moreover, age has significant impact on both breath and depth of privacy disclosure. However, their results didn't find any significant relationships between SN site experience or personal SN size and users' privacy disclosure. However, significant relationships were found among specific female and old user groups.

Hagai, Leon, and Zurbriggen [12], added other factors to users' information disclosure behaviour on SNs such as enhancing user's interpersonal relationships and social communication. They concluded that disclosing personal information publicly on SNs without having privacy concerns may drag users to personal and professional issues in workplaces with employers and clients, or within relationships, friendships and families. Their results showed that the threat to information privacy is a serious issue which require real changes to the current information protection laws, the used technologies and users' behaviours to achieve better information privacy for users on SNs.

Zhao and Zhao [23], used web content analytic and network system information auditing for evaluating of 50 SN sites with respect to privacy and security. Their study found that most of the sites have privacy and child-protection policies. In addition, the social sites have identifiable, easy to use guidelines for users on their home page sites.

Hovi *et al.* [13], examined users' privacy awareness based on information protection and information sharing. They carried out a survey research on a group of 210 Facebook users. Their findings showed that most of Facebook users disclose a significant amount of information. This mainly because the users were not aware of the visibility and accessibility of their information to other users. The findings also showed that users did not know or understand privacy policy and terms of use of the SN.

Townsend and Wallace [21], questioned whether SN user's approval to a set of terms and conditions is good enough for SNs, third-party companies and organizations to collect, use and disclose a piece or pieces of user's information? They interviewed a number of researchers about gathering user's data from SNs, their ethical concerns about reuse the data. The study found that most of the researchers were not following any clear ethical framework when they gather data and they freely would reuse publicly shared data on SNs. The researchers indicted that since the data is accessible,the SN users have signed up for the service, and already agreed to terms of conditions of the SN, then they have minimal to zero ethical concerns about their collection, analysis and reuse of users' data. In addition to privacy awareness, there are also studies of information protection laws for SN platforms.

According to Benaroche [6] study, the general use of SNs remains mostly unregulated in Canada even though the information protection and related human right legislation are having positive impact on SNs and employment. The study concluded that PIPEDA, and the personal information protecting acts in Alberta, British Colombia, Manitoba and Quebec prohibit the collection, use or disclosure of personal information by employers without the employees' consent. These laws also prohibit collecting information without clear purpose at the time of collection.

3 A Brief Review of Information Protection Laws vs. Social Networks

Today, as the use of SN is growing among people in Canada and globally, so do the threats to user' information privacy which need government attention and intervention by placing powerful regulations and enforcing the privacy laws to protect information privacy. In Canada, the right of privacy is recognized in constitution and introduced in Canadian Charter of Rights and Freedom in1982. According to James [14], unlike the USA laws, individuals' privacy right in Canada, is protected through multiple of mechanisms in form of constitutional or regulatory approach. From legal perspective, information privacy in the online environment like SNs should be predominantly protected by general people and constitutional rights, especially by data protection rules. in Canada, there are two federal and several provincial laws that are in effect to protect information privacy. These laws consist of a set of rules that provide direction and guidance for both government and organizations on how to handle people personal information which can be applied to SN operators and providers [1].

The Personal Information Protection and Electronic Documents Act (PIPEDA) which is a federal law, governs the privacy practices of private sector companies including SN companies that are involved in inter-provincial and cross-border activities in Canada as long as these activities have some kinds of commercial nature [5, 10]. For example, PIPEDA's 10 basic principles regulate privacy issues in respect to consent, transparency, security measures, and data retention [5].

Canadian and International based SN companies operating or providing services in Canada must also comply with PIPEDA's legal obligations and must meet PIPEDA 's privacy requirement with respect to protecting information privacy [7, 10]. Although PIPEDA has specific rules for regulating the SNs and protecting information privacy, it still can cover the SN companies adequately. However, some of SN companies have failed to adhere to Canadian privacy laws such as PIPEDA due to the lack of enforcement power within the Canadian privacy laws [18]. Generally, PIPEDA prohibits SN companies to collect, process or disclose users' personal information in commercial nature transactions unless the process is controlled under PIPEDA principles [3]. While the laws at their current state, are seen by many for not being very sufficient in protecting information privacy especially in online SN environment, the laws still effectively govern federal and provincial jurisdictions, public and private sectors to some extent [7]. However, the general use of SNs still largely remains unregulated in Canada [6].

The use of the public SNs at workplaces is mostly regulated under private sector regulations. These rules provide employers with legal power to monitor public SNs used by employees, enforce appropriate actions whenever is needed within the context of local policies and guidelines [6]. In addition, using user's information on SNs for employment is indirectly impacted by information protection and human right laws in Canada since employees' personal information are protected by PIPEDA [6, 9].

4 The Study of Privacy Issue on Social Networks

4.1 Research Design

4.1.1 Survey Questions

For the survey, we designed 2 sets of questions (see Table 1 and Table 2). From the first set of questions, we collected demographics information of the respondents. From the second set of questions (10 questions), we collected several important types of information regarding privacy matters from our respondents. The goal is to examine respondents' perspectives about privacy related matters on SNs such as privacy setting tools, privacy control mechanisms and their general viewpoints about privacy awareness. From Table 2, questions 1 and 2 aimed to collect general information about types of SNs and hours users spend on SNs daily. Questions 3 and 4 ask about users' attitude and practice towards information disclosure and information privacy control. Questions 5 and 6 ask about users' awareness and understanding of terms of use and privacy policy of SNs. Questions 7, 8, 9 and 10 ask about user opinion concerning the collection, safety and control over their SN personal and private information. Regarding the survey answers, we provided our participants with a fixed number of responses to our 10 closed-ended questions and the other four demographic questions. We asked the users to select one or more answer(s), based on the type of the question, within limited frame of options (see Table 1 and Table 2).

Table 1. Respondents Demographic Questions and Answers; Age, Education and Employment Status vs Gender

Survey Questions about	**User to Select 1 Answer**	**Female Answers 54.3%**	**Male Answers 45.7%**
Age	18-25	6	1
	26-30	4	2
	31-35	5	4
	36-50	7	11
	Over 50	3	3
Education	High School	5	2
	Degree-Diploma	15	12
	Masters	4	5
	PhD	1	1
	Bachelors	0	1
EmploymentStatus	Student	7	1
	Working Student	3	1
	Employed	10	16
	Other	5	3

4.1.2 Data Collection

The data was collected from one random group of SN users. In total, we invited 73 users via direct email, Facebook or Twitter to complete this survey. The survey invitation receivers were also able to invite more people to complete the survey by forwarding the invitation emails. We noticed that although they could invite more of their friends to answer the survey questions, our respondents did not invite anyone for unknown reasons.

By default, we allowed only one response per a user as we turned the multiple response option off. As a result, our respondents could only take the survey once per email or browser. The survey was available for 14 days from the day it was sent out to the respondents. A total number of 46 responses from different anonymous individuals were received. The participation success rate was about 63% as 46 responses were received (see Table 1).

4.1.3 Data Analysis

We use Microsoft Excel charts and tables to summarize and analyze the collected data. Data visualization was used to find patterns in the data for the data variables. We used Frequency distribution and Pivot tables, Pie and Bar charts to arrange, summarize, represent the distribution and compare data results.

Basic summary statistics were used (see Table 3) to scale questions 7, 8 and 9 of the survey to identify the significant data patterns for these questions in the data. We used cross-tabulations test, frequency analysis and descriptive statistics to examine relationships within the data with respect of respondents' age, gender, educational background and employment, and with other survey variables.

Table 2. Questions and Answers used in the Survey with the Answer Types

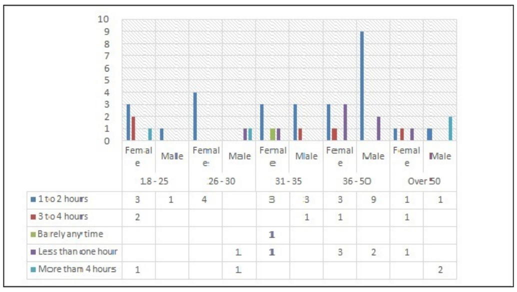
Survey Questions	Answers Options
1. What social network(s) respondents use?	Facebook, Twitter, Instagram Skype, Snapchat, WhatsApp Google+, other
2. On Average, how many hours per day is spent on social network(s)?	A. Barely any time B. Less than 1 hour C. 1 to 2 hours D. 3 to 4 hours E. More than 4 hours
3. How often user post share or comment publicly on own and/or other SN pages?	A. Never B. Occasionally C. Sometimes D. Often E. Frequently
4. Which of the following privacy control mechanism user is currently using?	A. Control how others can find me B. Block spam users C. Control who can message D. Restrict visibility of my profile E. Restrict photo tagging F. Set alarm if login occurs from unknown
5. When join a social network which answer best describes user?	A. Never read the terms of service but agree to join B. Only sometimes read the terms yet still agree to join C. Always read the terms still agree to join D. Always read the terms but do not join if disagree
6. Regarding social network privacy policy. Which answer best describes user?	A. Not aware, don't read and can't find them B. Aware but never read them C. Aware, sometimes read them but have no concern with privacy D. Aware, read and take info. privacy seriously and act adequately
7. If others try to uncover user's private information from the user's social network pages, how difficult would be?	A. Very difficult B. Somewhat difficult C. Not too difficult D. Not at all difficult
8. What's user's opinion about social network's targeted advertisements	A. Don't click Ads, invade users' privacy B. Ads provides uncomfortable and false info C. Sometimes click ads, trust their info. and offer D. Often click ads ads have no threat to privacy
9. What's user's opinion about the level of control user has over collected private data by others?	A. High level of control over collected data B. Somewhat limited level of control over collected private data C. Little level of control over the collected data D. No control over collected private data at all
10. What's user opinion about personal data on social network collection by governments and other companies ?	A. Without consent, data shouldn't be collected B. It's Ok without my knowledge but only for legitimate use by law only C. Users' personal data shouldn't be collected or used in circumstances by anyone D. Not aware of users' data collection by others

Table 3. Summary of Respondents' Scaled answer to questions 7, 8 and 9

Answers Measurement Scale 1 to 4	Average	Mode	standard deviation	Sample Size
Question7 answers scaling: 1=Very difficult 2= Somewhat difficult 3= Not too difficult 4=Not at all difficult	2.4	2	0.8	46
Questions 8 answers scaling: 1=Often click on Ads 2= Sometimes click on Ads 3= More likely not to click on Ads 4=Don't click on Ads	3	3	0.9	46
Question 9 answers scaling: 1=High control level 2=Somewhat limited control 3= Low control level 4= No control at all	2.3	2	0.9	46

4.2 Summary of the Participants Demographics

Based on summarized demographics data of respondents in Table 1, 54.3% of respondents are female and 45.7% are male. Majority of respondents (58.7%) are in age between 30 and 50, and 58.7% of them having either diploma or degree. More than half of respondents (56.5%) are employed. Interestingly, the results show the respondents belonged to 30 to 50 age groups and mostly employed with high educational background are the ones who using SNs more than other age groups and other employment status. This finding is very similar among female and male respondents.



	18 - 25 Female	18 - 25 Male	26 - 30 Female	26 - 30 Male	31 - 35 Female	31 - 35 Male	36 - 50 Female	36 - 50 Male	Over 50 Female	Over 50 Male
■ 1 to 2 hours	3	1	4		3	3	3	9	1	1
■ 3 to 4 hours	2					1	1		1	
■ Barely any time					1					
■ Less than one hour				1	1		3	2	1	
■ More than 4 hours	1			1						2

Figure 1. Users Average Time Spent on SNs

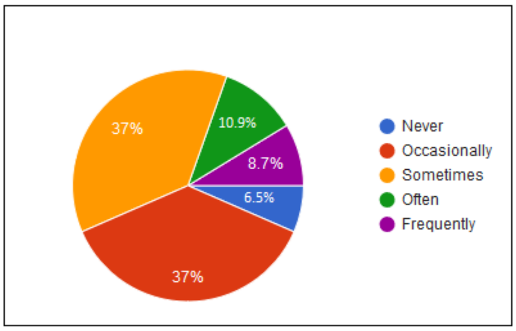


Figure 2. How Often Users Share Information Publicly

4.3 Respondents' Average Time Spent on SNs and Respondents' Attitude toward Information Sharing

Figure 1 shows the answers to question 2. It indicates that majority of respondents (60.9%) are spending 1 to 2 hours per day Social Networking, and 64% of them within the age of 30 to 50. Significantly, these results are less than the daily average use of SNs in the world in 2017. Further study is needed to determine what factors affecting users spending time on SNs.

Figure 2 shows the answers to question 3. It indicates that a significant minority of respondents (3%) only are not posting any information publicly, and 74% of respondents doing so 'Occasionally' and 'Sometimes'. However, 27% of respondents are 'Often' and 'Frequently' posting and sharing publicly. The results show that the respondents are somehow cautious about their information in the first place since they are not willing to share publicly.

4.4 Respondents' Use of Privacy Control Mechanism

Most of SNs provide mechanisms to control user privacy. Figure 3 shows respondents' answers to question 4. The results indicate that most of the respondents are using at least on these mechanisms to manage their personal privacy. The findings show that except 6% of the respondents, the others are utilizing available privacy tools for managing their information privacy on SNs.

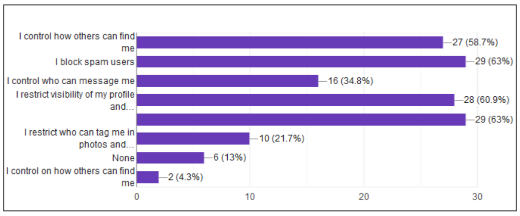


Figure 3. SN Privacy Control Mechanism Used by the Respondents

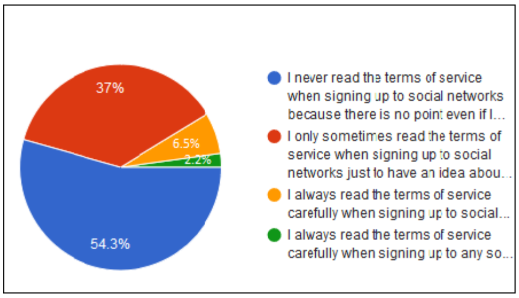


Figure 4. Respondents Attitude toward Social Network Terms of Service

4.5 Respondents' Knowledge, Understanding and Attitude toward SN's Terms of Services and Privacy Policies

Figure 4 and 5 present respondents' responses to questions 5 and 6. The results show that54.3% and 61% of the respondents, respectively, do not put any effort to actually read SNs' terms of use and privacy policies. The majority (97.8%) of the respondents accept terms of service just to be able to use the services regardless of their reading or understanding the contents of the terms. This may result into the biggest risk to information privacy as SNs can use these agreed contracts to bypass privacy obligations. Regarding privacy policy, although 13% of the respondents indicated that sometimes read the privacy policies, they have no concern with their information privacy. Moreover, only 26.1% of respondents are familiar with privacy policies, read and understand them, and take serious initiatives to protect their information privacy. Surprisingly, 15.2% of the respondents are not even aware of the existence of privacy policies. These results show that not all of the respondents read privacy policies of their SNs, while only a quarter of them are concerned about their privacy and act accordingly to protect their information.

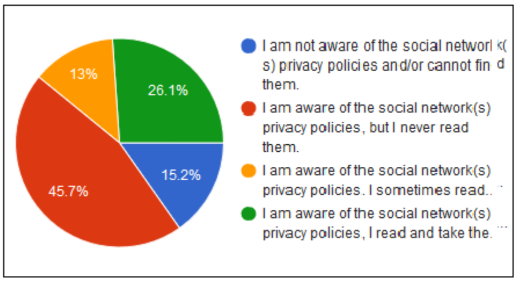


Figure 5. Respondents Attitude toward Social Network Privacy Policies

4.6 Summary of Respondents' Viewpoints toward the Safety and the Level of Control over Their Collected Data by SN

For this section, the observational data from respondents' answers to questions 7, 8 and 9 are scaled into counted categories (see Table 3).Then we applied simple statistics functions on the data sample (N) such as Average to find answers' central tendency, Mode to find the answer with greatest occurrence, and Standard deviation (SD) to find how far the answers are spread out from the calculated average number. The aim is to determine the respondents' overall answers to the questions 7, 8 and 9. The respondents' answers to question 7 indicate that they generally think it would not be difficult for others to invade their information privacy on SNs. The respondents think that their information on SNs is not too safe. Respondents' answers to 8 shows that more likely they don't click on targeted advertisements. This signifies that the respondents have concerns about advertisements on SNs related to their privacy. The answers to question 9 indicate that the respondents have concerns about the level of control that they have over their collected data. The overall answers show the respondents are somewhat concerned about their information safety on SNs, worried about their real access and control over their information once collected by SN companies Figure 6 shows the answer to question 10.A small percentage (8.7%) only are not aware of the data collection by governments and other companies. The majority of the respondents (78.3%) are concerned about their personal information knowing that various entities continuously harvesting users' SNs data. The results show that most of the respondents believe that governments and SN companies should not collect or disclose any of users' data under no circumstances (28.3% of respondents), while 50% of respondents are okay with their data collection or use only with their consents, and for only 'legitimate' business or government purposes only.

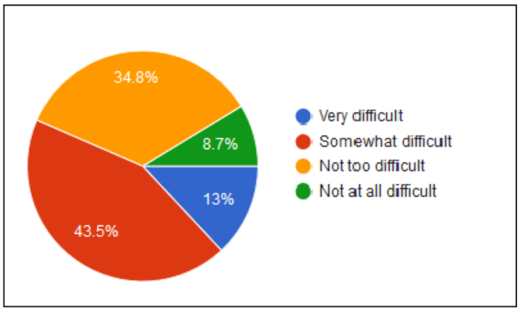


Figure 6. Respondents Opinion toward the Collection of their Information by Government and Commercial Companies

5 Conclusion

In this paper, we have reviewed earlier research on privacy issues related to SNs and explored information privacy protection from perspectives of main Canadian legislation like PEPIDA. We also presented the questions, methodology and results of our survey research about privacy awareness. Currently federal privacy laws in Canada such as PIPEDA and Digital Privacy Act do not tend to protect information privacy of individuals at personal level. Instead, the laws regulate privacy practices of private sectors and government agencies. The general use of SNs mostly remains unregulated in Canada, nevertheless SN companies must comply with privacy laws. We designed 2 sets of questions to learn about users' demographics and users' opinions and practice about information sharing, privacy control mechanism, SNs' terms of use and privacy, safety and level of control over their information. We collected answers from 46SN users via emails. The results show 76% and 54% of the respondents, respectively, lack knowledge about privacy and terms of service. However, majority of them (94%) are using one or more of privacy control mechanism, and 78.3% are concern about the safety and level of control over their information.

References

[1] Your privacy rights, 2016. URL https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/.

[2] Number of social media users worldwide 2010-2021, 2017. URL https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[3] Personal Information Protection and Electronic Documents Act, 2017. URL http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.

[4] Global social media ranking 2018 | Statistic, 2019. URL https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[5] Tariq Ahmad. Online Privacy Law: Canada, 2012. URL https://www.loc.gov/law/help/online-privacy-law/canada.php{#}Current.

[6] Patrick L. Benaroche. Social Media and Employment Law An International Survey |Chapter 5 Canada. In *Social Media and Employment Law An International Survey*, page 26. 2015. ISBN 978-90-411-4768-4. URL http://www.stikeman.com/pdf/Social-media-employment-law-survey{_}Walters-Kluwer.pdf?utm{_}source=Mondaq{&}utm{_}medium=syndication{&}utm{_}campaign=View-Original.

[7] Colin J. Bennett, Christopher A. Parsons, and Adam Molnar. Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice. Technical report, 2013. URL http://ssrn.com/abstract=2208098.

[8] Sohnen Cherie and Moe Responds. How can I become more confident in using social media? *MASSAGE Magazine*, pages 32–36, 2017. URL www.massagemagazine.com.

[9] Pierre-Luc Dusseault. PRIVACY AND SOCIAL MEDIA IN THE AGE OF BIG DATA. Technical report, House Of Commons - Canada, Canada, 2013. URL https://www.ourcommons.ca/Content/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf.

[10] Lisa Feinberg. Social Networking, 2012. URL https://cippic.ca/en/FAQ/social{_}networking{#}SN12.

[11] Enrico Franchi, Agostino Poggi, and Michele Tomaiuolo. Information and Password Attacks on Online Social Networks:: An Argument for Cryptography. *Journal of Information Technlogy Research*, 8(1):25–42, 2015. ISSN 1938-7857. doi: 10.4018/JITR.2015010103.

[12] Ella Ben Hagai, Gabrielle Leon, and Eileen L. Zurbriggen. Negotiating privacy and intimacy on social media: Review and recommendations. *Translational Issues in Psychological Science*, 2(3):248–260, 2016. ISSN 2332-2136, 2332-2136. doi: http://dx.doi.org/10.1037/tps0000078. URL https://search.proquest.com/docview/1826150550?accountid=15977{%}5Cnhttp://su3pq4eq3l.search.serialssolutions.com/?ctx{_}ver=Z39.88-2004{&}ctx{_}enc=info:ofi/enc:UTF-8{&}rfr{_}id=info:sid/ProQ{%}3Apsycinfo{&}rft{_}val{_}fmt=info:ofi/fmt:kev:mtx:journal{&}rft.genre=article{&}rft.

[13] Marjaana Hovi, Olli Pitkänen, and Virpi Kristiina Tuunainen. In *22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety*, page 17, Slovenia, 2009.

[14] Michael C. James. A COMPARATIVE ANALYSIS OF THE RIGHT TO PRIVACY IN THE UNITED STATES, CANADA AND EUROPE Michael. *Connecticut Journal of International Law*, 29(2):257–300, 2013. ISSN 02729490. doi: 10.3366/ajicl.2011.0005.

[15] Sangeeta Kumari and Shailendra Singh. A Critical Analysis of Privacy and Security on Social Media. *2015 Fifth International Conference on Communication Systems and Network Technologies*, pages 602–608, 2015. doi: 10.1109/CSNT.2015.21. URL http://ieeexplore.ieee.org/document/7279989/.

[16] Kai Li, Zhangxi Lin, and Xiaowen Wang. An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information and Management*, 52(7):882–891, 2015. ISSN 03787206. doi: 10.1016/j.im.2015.07.006. URL http://dx.doi.org/10.1016/j.im.2015.07.006.

[17] L Li and K Qian. Using Real-Time Fear Appeals to Improve Social Media Security. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 2:610–611, 2016. ISSN 07303157. doi: 10.1109/COMPSAC.2016.217.

[18] Rob Normey. Privacy in Canada. *LawNow*, 1 (33):8, 2012.

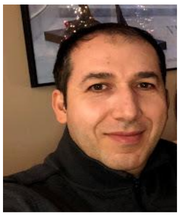
[19] RBS. Social Media âĂŞ What are your privacy risks?, 2012. URL https://www.riskbasedsecurity.com/2012/09/my-privacy-audit/.

[20] Hemamali Tennakoon. Information security and privacy in social media: The threat landscape. *Implications of social media use in personal and professional settings.*, pages 73–101, 2015. doi: 10.4018/978-1-4666-8614-4.ch085. URL http://ovidsp.ovid.com/ovidweb.cgi?T=JS{&}PAGE=reference{&}D=psyc12{&}NEWS=N{&}AN=2015-24113-004.

[21] Leanne Townsend and Claire Wallace. Social Media Research: A Guide to Ethics. *Economic and Social Research Council*, pages 1–16, 2016.

[22] J. L Williams. Privacy in The Age of The Internet of Things. *Human Rights*, 4(14):6, 2016.

[23] Jensen Zhao and Sherry Y. Zhao. Security and Vulnerability Assessment of Social Media Sites: An Exploratory Study. *Journal of Education for Business*, 90(8):458–466, 2015. ISSN 0883-2323. doi: 10.1080/08832323.2015.1095705. URL http://www.tandfonline.com/doi/full/10.1080/08832323.2015.1095705.



Soran Ibrahim is a technical support analyst and general IT manager at a local medical clinic in the province of Ontario in Canada. He graduated from University of Baghdad where he earned a bachelor's degree in computer science in 1997. He, in Canada, continued his education and received an advanced diploma with honor in computer engineering technology from Conestoga College in Kitchener, Canada. In 2007. After working in few high-tech companies as Testing Engineer, Technical Analyst and IT Data Conversion Specialist, and with his wide-ranging field expertise, he attended Athabasca University for his master's degree of science in information systems. His academic interest and primary research involve personal data privacy in the digital world, social networking, and how the privacy laws impact the personal information privacy.

Qing Tan is an associate professor in School of Computing and Information Systems at Athabasca University. He earned his PhD in Cybernetics Engineering for Robotics from the Norwegian Institute of Technology in 1993. The Japan Atomic Energy Research Institute invited him in 1994 as a foreign senior research fellow. He did his post-doctoral fellowship at University of Alberta. He joined Athabasca University in 2007 with extensive IT industrial experiences.