Rise of the Canadian Network Society

Data Privacy and Security of Canadian Residents

Cassandra Evelyn Wiltshire

Master's thesis
April 2021
International Business Management
School of Business

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Wiltshire, Cassandra Evelyn

Rise of the Canadian Network Society – Data Privacy and Security of Canadian Residents

Jyväskylä: JAMK University of Applied Sciences, April 2021, 80 pages.

School of Business. Degree Program in International Business Management. Master's Thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

Current protection acts and legislations set in place for Canadian residents regarding their privacy and securities online are not adequate and must be reviewed. It was investigated whether Canadian residents are aware of how much data is being collected about them while operating in online spheres. Moreover, the lack of protection for Canadian residents regarding data collection and information sharing in the marketing and advertising sphere. The scope of research highlighted this gap and shed light on the importance of consumers' privacy and security.

Through mixed methods of both quantitative and qualitative research, a survey was administrated to Canadian residents to examine their knowledge on current legislation regarding data privacy and their overall knowledge of how organizations surveil, collect, and distribute their personal data.

It was discovered that Canadian residents are informed of the scope in which their data is being collected, however, are not informed on the full implications of this collection. More importantly, a majority of Canadian resident respondents are ill informed on the current legislations and regulations set in place to protect them. Canadian residents showed immense interest in requesting more information on how they can stop this invasion of privacy in collection practices and voiced that more stringent protocols should be put in place to better regulate this industry.

Current laws and regulations regarding the collection of personal data in online sphere are outdated. Furthermore, call the need to be reexamined, updated, changed, and quantified. Although Canadian residents are aware of the data collection being conducted, Canadian residents feel organizations are being misleading and therefore do not feel implicit consent is valid in such cases.

Keywords/tags (subjects)

privacy, security, data, legislation, consent, Canadian, PIPEDA, CASL

Miscellaneous (Confidential information)

All survey respondents remained anonymous. Therefore, responses are not confidential

Contents

Figures

Tables

1 Introduction

“Nothing vast enters the world of mortals without a curse” - Sophacies. Since the rise of the Internet, globalization and the spread of information has changed the way we consume, socialize, interact and live. The information age can be referred to as an informational economy. Manual Castells, a Spanish born professor of sociology and planning and chair of the Centre for Western European Studies, University of California, Berkley, simply states “it is an economy in which sources of productivity and competitiveness for firms, regions, countries depend, more than ever, on knowledge, information, and the technology of their processing...” (Castells, 1997). Thus, the digital age has begun to transcend past any perceived or believed originally thought potential.

However, underestimation seems to be a trend in the world of technology. For instance, in 1876 at the Western Union Internal Memo, it was said that the “’telephone’, [had] too many shortcomings to be seriously considered as a means of communication” (Vaynerchuk, 2014). However, today the telephone and its many digitalized advancements serves as the #1 most used method of communication around the world, connecting the world through a vast and intricate communication system at the touch of a button. Thus, this idea of underestimating technology has been positively flouted by some of the biggest and greatest inventors, investors, and members of society. For instance, Amazon founder Jeff Bezos told an interviewer “If I had a nickel for every time an investor told me this wouldn’t work...” (Vaynerchuk, 2014). Amazon valued at $1.7 Trillion USD as of 2020 (three hundred forty billion nickels if you are curious).

The underestimation of Internet technologies has brought about the imperative need for paralleled protocols and regulations in parliaments to protect societies and its members. With the advancement of technologies that connect us, gather information, and robotically and intellectually think for us, it is apparent that two crucial elements were not adequately considered during the successes throughout the years: privacy and security. Thus, privacy is the most sought out commodity in a modern age where it seems your privacy is for sale.

1.1 Society And Its Technologies – The Bigger Picture

The purpose of this thesis is to critically analyze and study the topic of data collection on consumers in Canada. More importantly of the data collected, who it belongs to legally and the

implications of this regarding consumers' safety, privacy, security, and the business marketing sphere. Spanish sociologist Manual Castells' *Rise of the Network Society* thoroughly explores the accelerating pace of innovation and applications of technologies. He promotes the idea that society has become technology focused because society cannot be understood without its technological tools (Castells, 1996). However, societies globally now face the threat of their rights regarding their privacy and security with their behaviours being monitored both online and offline.

It is important to understand there are many benefits to vast amounts of information. The Canadian government for instance, uses the framework of infodemiology and infoveillance "to track online health information and cyber behaviour for public health" (Eysenbach, 2011). This is emerging area of research that can be defined as "the science of distribution and determinants of information in an electronic medium, specifically the Internet, with the aim to inform public health and public policy" (Eysenbach, 2011).

With the use of textual, unstructured, and openly accessible information both consumed and on the internet such as website, blogs, social media etc., data can be collected and analyzed in real time and developed to identify health related information on individuals. According to Gunther Eysenbach, MD, MPH, Centre for Global eHealth Innovation, Consumer & Public Health Informatics Lab, University Health Network, this system was specifically designed to "measure public attention, attitudes, behaviour, knowledge, and information consumption, as well as syndromic surveillance, health communications and knowledge translation research" (Eysenbach, 2011).

1.2 The Benefits Of Disruption For The Businesses Sphere

As much as data collection can be intended for good, there are equally pressing issues that arise in the business private sector. As of 2019, Canadian internet users is estimated to be 34.56 million, with online services reaching almost 96% of the population (Statista, 2021). To protect the privacy and security of Canadians online, the Canadian government created the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA is a Canadian legislation aimed to regulate data privacy and to govern how private sector enterprises collect, disclose, and use personal information in the course of commercial business (Office of the Privacy Commissioner of Canada, 2021).

Higher than any time in history, more Canadian's are shopping online and with the use of targeting technologies, business and organizations are learning more than ever about their consumers. As PIPEDA aims to regulated data privacy, other organizations such as Google, third party sellers and organizations, and social media platforms use the legal information collected to target consumers resulting in future financial transactions. This is achieved through various means such as targeted ads through cookie tracking, email communications and newsletters, and telecommunication. As a result, the rise of communications and information gathering beget the rise and emergence of spam and other related issues.

Between April 1 and September 30, 2018 more than 137,000 Canadians made complaints to the Canadian Spam Reporting Centre—the main issue being emails communications without consent. The country itself homed 7 of the world's top 100 spamming organizations and as of 2009, 90% of all national email traffic constituted as spam (Branch, 2021). Thus, in 2014, the Canada's anti-spam legislation (CASL) was created to reinforce and strengthen best practices in email marketing and to combat spam, fraud, and related issues. Ultimately, CASL provided a new space to ensure enterprises acted more disciplined and diligent in managing their commercial messages to consumers within electronic marketing programs (Affairs, 2021).

This has resulted in positive marketing metrics for businesses including increased open and click-through rates for marketing messages and a reduction in bounce rates (Affairs, 2021). Consequently, both Canadian's and enterprises benefit from the regulation of unsolicited commercial electronic communication (CEMs), "as trust in electronic means of communications and those who use them for commercial purposes is essential to the prosperity of the Canadian economy" (Branch, 2021). To gain a full comprehensive understanding of both PIPEDA and CASL, a literature review with be explored later in this thesis.

1.3 Canadian Data, Privacy And Security

Though it seems the current protections implemented by the Canadian government is beneficial to both business and citizens, there is evidence to suggest more stringent protocols should be implemented in this sector. When visiting a website for information, it is probable that your technological medium (computer, ipad, mobile etc.) will be offered "cookies". These cookies help web developers provide more personalized and convenient website sessions. Moreover a cookie is

“a small file that is passed from a website to an end user’s computer, often without their knowledge or consent” (Office of the Privacy Commissioner of Canada, 2011).

Essentially, cookies let website remember you. Moreover, they allow website to recall your log in credentials, shopping carts, history and more. They are the digital “crumbs” you leave behind, ergo: “cookies”. This allows those websites to track you and your online activity. Although cookies are indispensable to today’s modern internet, they are a major vulnerability to one’s privacy (What are Cookies?, 2021). Today, almost all websites and business organizations use cookies for various reasons. As a result, the information collected is stored, mined and traded with third party companies and third-party companies overseas.

Online cookies can be classified as either HTTP cookies or Magic Cookies. The HTTP cookie is a repurposed and modernized version of the “magic cookie” built for the purpose of internet browsing ("What are Cookies?", 2021). Additionally, they can be a treasure trove of private information for organizations to collect and criminals to spy. In a survey of 1,005 Canadians conducted in the Canadian Journal of Administrative Science, it was found that many respondents were ill informed about how their data is being collected and used. Marshall David Rice and Ekaterina Bogdanov (2018), authors of an Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices: Canadian Journal Of Administrative Sciences, York University, Toronto, suggest the need of further research into “alternative methods of informing Canadians about corporate data practices and of enhancing individuals' control of private data in today's increasingly connected and mobile world”.

Search Engines such as Google, Bing, Yahoo etc., and other websites, use cookies to store, mine, trade data to provide other companies and businesses information on how to better interact and engage with consumers. Through these marketing sales tactics, businesses are now able to target and cater advertisements specifically to consumers as individuals. The data collected that is owned and distributed by these mediums include: age, gender, interests, addresses, biometric facial data etc. without users’ explicit “opt-in” consent. Additionally, not only is data stored and collected on one particular platform, but data is also used to track you to other sites, other applications on your phone, and other physical locations you have visited in real life.

In a 2016 Pew Research Centre study, researchers found that more than 50% of respondents cannot identify the cookies as a primary website browsing hacking tool (Pew Research Center, 2014). Jeff Seibert, Former executive at Twitter, Serial Tech Entrepreneur and Co-founder of Digits wants people to know that "everything they're doing online is being watched, is being tracked, is being measured. Every single action you take is carefully monitored and recorded." (Orlowski, 2020).

Tim Kendall, Former Facebook Executive (2006-2010) and Director of Monetization, Former Pinterest President and current CEO of Moment, a mobile device application that tracks screen-time, stated how everyone had a "total admiration for Google and what Google had built, which was this incredibly useful service that did, far as we could tell, lots of goodness for the world, and they built this parallel money machine." (Orlowski, 2020). As companies continue to use the data, they collect to aid in their transformation of becoming digital economies to scale, we see a paradigm shift for the intended purposes and the well-being of this data. Shoshana Zuboff Ph.D., Professor Emeritus at Harvard Business School and Author of *The Age of Surveillance Capitalism*, explains that this shift "is what every business has always dreamt of: to have a guarantee that if it places an ad, it will be successful. That is their business. They sell certainty. To be successful in that business...you need a lot of data" (Orlowski, 2020).

Rice and Bogdanov (2018), highlight how companies today are collecting data in ways that would have been unimageable a few years ago. Furthermore, Zuboff highlights that "they have more information about us than has ever been imagined in human history. It is unprecedented." (Orlowski, 2020). Furthermore, prominent digital methods of tracking users internet browsing patterns, has been met with newer methods that include voice and facial recognition, emotional recognition, and location tracking via GPS or Wi-Fi pinging (Rice & Bogdanov, 2018). Gary Vaynerchuk's*, The Thank You Economy* highlights that these technologies have "allowed us to become more aware of the minutiae in each other's lives, of what was going on, of what people were thinking and doing, than ever before" (Vaynerchuk, 2011).

Additionally, the number of data collection points have also increased with the proliferation of smartphones, wearable devices, and the emerging Internet of Things. Zuboff highlights that we have "a new kind of marketplace now" (Orlowski, 2020). Moreover, that it is "a marketplace that

never existed before. And it is a marketplace that trades exclusively in human futures...We now have markets that trade in human futures at scale, and those markets have produced the trillions of dollars that have made the Internet companies the richest companies in the history of humanity." (Orlowski, 2020).

Consequently, Rice and Bogdanov (2018), have conceived that such a low awareness of data practices is partially explained by the shortcomings of the privacy notice. Further, Tristan Harris, former Google Design Ethicist (2013-2016), Co-Founder and CEO of Apture (2007), Co-Founder of Centre for Humane Technology and Co-Host of Your Undivided Attention with Aza Raskin, highlights that regarding data collection and security, he "[wishes] more people could understand how this works because it shouldn't be something that only the tech industry knows. It should be something that everybody knows." (Orlowski, 2020).

1.4 The Privacy Notice

Over the past 50 years, consumer privacy worldwide has been governed by a framework called Fair Information Practice Principles (FIPP). The goal of FIPP is to essentially oblige businesses to disclose information about their data practices to allow consumer to make informed decisions. This legislation was proposed in 1973 as a response to the upward trend and use of automated data systems containing data about individuals by the United States Secretary's Advisory Committee on Automated Personal Data systems. The FIPPs model of privacy regulation rests on a theory of informational self-determination (Rice & Bogdanov, 2018). This theory being the idea that "an individual ought to have control over his or her information" and includes five areas of data privacy (Mulligan & King, 2012):

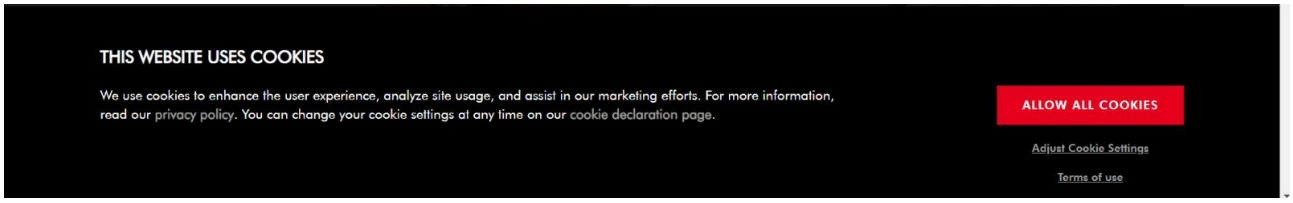
<u>5 Areas Of Data Privacy:</u>

1. Companies must disclose their data practices to individuals.
2. Consumers must provide their consent.
3. Individuals should be able to view their data and correct it if needed.
4. Organizations should protect the integrity and security of private data.
5. Mechanisms should be put in place to enforce the principles and provide redress where they are violated.

In Canada, the five core FIPPs tenets give rise to the 10 principles that underpin the PIPEDA. However, FIPP and PIPEDA does not significantly restrict the means of cooperate rate collection and the use of consumer data. Furthermore, that in order to obtain consumers consent and to comply with FIPP and PIPEDA, cooperation's developed the privacy notice.

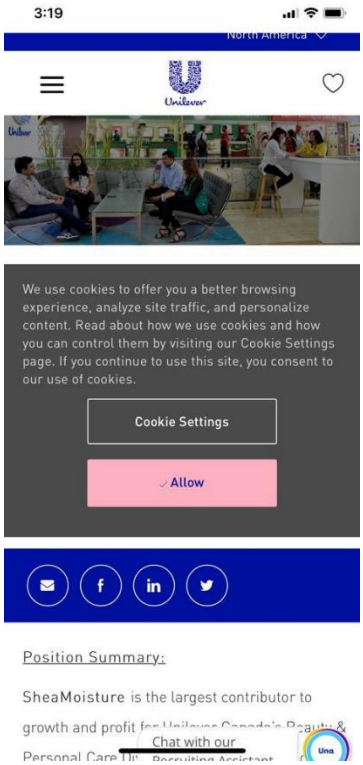
The privacy notice “is a statement or document [that discloses] a company’s data-related practices” (Rice & Bogdanov, 2018). These statements or documents are presented to the consumer, and the user must usually consent to the terms of data collection before being permitted to use the company’s services. Thus, through these terms and conditions disclaimers, companies can legally collect and store information. Furthermore, that if information regarding corporate data practices is in fact contained in a privacy notice that which the users agrees to, then the user has provided the collector (business or organization) consent to data practices. Further, that the corporation is abiding to FIPPS, PIPEDA and CASL. However, in a Deloitte survey of 2,000 consumers, 91% of respondents consented to legal terms and service conditions without reading them and a higher 97% of people aged 18-32 agreeing to terms without reading them (Business Insider, 2021). Rice and Bogdanov (2018) highlight broadly that “research suggests that consumers believe that laws protect their privacy more than it actually does”.

Figure 1 – Desktop



(Zwilling J.A. Henckels Ltd., 2021)

Figure 2 — Mobile



(Unilever, 2021)

Social media platforms such as Facebook, Instagram and Snapchat are infamous for collecting data. These platforms also feature applications available on mobile devices enhancing the use of GPS location tracking information. Facebooks terms and conditions policy clearly state:

“We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera... Our systems automatically process content and communications you and others provide to analyze context... We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of...” (Facebook, 2021).

The Facebook Pixel in particular, enables websites and online retailers the means to collect information about users as the social network analyzes aggregated user behaviour. In a 2020 interview, Tim Kendall highlighted that “there were meaningful, systemic changes happening

around the world because of these planforms that were positive! But they grew naïve about the flip side of the coin" (Orlowski, 2020).

Further to Rice and Bogdanov's point, it remains evident that one crucial area remains understudied: "how much do people actually know about the ways in which companies collect their data?". More importantly, in their study, they highlight that because consumers do not know enough and the extend of the information and that the data collection is taking place, then they can neither engage in privacy-protecting actions, make informed decisions, request their data, or file any complaints regarding the collection with the regulator. Therefore, is it really legitimized explicit informed consent? Rather, that with this surface level of understanding and incentivizing consumers to "accept" by withholding access to the provided services, products, and information, we see a phenomenon that raises the question of ethicality. Thus, if the ethicality is questioned then legitimacy of the consent should also be questioned.

In Canada, research regarding consumers' knowledge on privacy-impacting business practice is extremely limited. In a 2016 study conducted by the Office of the Privacy Commissioner of Canada to investigate the awareness of Canadian consumers, 32% of Canadians "did not feel confident that they had enough information to know how new technologies may affect their privacy" (Rice & Bogdanov, 2018). Additionally, in a study by Kezer et al, only 5.8% of respondents knew "that popular search engine sites such as Google, track the sites you come and go to" (Kezer et al, 2016).

Currently the American multinational technology giant Google, faces a proposed class action lawsuit in the Supreme Court of British Columbia for allegedly collecting and profiting from Canadians personal information collected without explicit consent. The said lawsuit alleges that "Google has turned Canadians' electronics into tracking devices" (Canada's National Observer, 2021). A team of lawyers across the nation are seeking compensation for "the invasion of privacy, trespass, and consumer protection violations with the intention of getting Google to stop these alleged invasive practices" (Canada's National Observer, 2021).

Additionally, these allegations incriminate internationally renowned programs. Programs such as Google Analytics and Google Ads which have become industry standards for website globally. Google further postulates that these programs are installed on more than half of global website

(Canada's National Observer, 2021). Further, the lawsuit claims "Google creates "profiles" on users based on websites visited, and further uses this data for practices such as ad targeting without the user's consent" (Canada's National Observer, 2021).

A recent 2014 study by Yong Jin Park and S. Mo Jang, found similarly on the low awareness of companies' data practices as a third of respondents was not aware that "companies today have the ability to place an ad that targets you based on information collected...". While quantitative research conducted by Park and Jang (2014), reported that "while interviews knew that they access the Internet on their computers, they incorrectly believed that they do not access the Internet when they use mobile applications such as Facebook, which led them to mistakenly believe that mobile activities are more private than those on the computer".

In a study on the widespread concern about the surveillance by government and businesses, 91% of adults in the survey "agree" or "strongly agree" that "consumers have lost control over how personal information is collected and used by companies", while 80% of "those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites" (Pew Research Center, 2014). Thus, regardless of the disclosure of information and cooperate data practices in privacy notices, evidence concludes that consumers and Canadian consumers are in fact ignorant to the collection and use of their personal data by private for-profit enterprises.

1.5 Research Questions

The focus of this thesis is to emphasize and investigate Canadian residents' knowledge or lack thereof of current data collection practices. Analysis on current regulations for Canadians regarding their online privacy will also be explored to provide critical analysis on whether Canadian laws a regulation regarding data privacy and security are sufficient. Ultimately, this thesis aims to adhere to the undeniable fact that there is a need for more stringent laws and regulations regarding Canadians and their data security.

The research question is:

1. Are Canadians residents aware of how much digital data is being collected about them while participating in online spheres?

Other secondary objectives that will be explored are:

1. What does this plethora of digital data mean for Canadian's privacy and security online? And who does this data legally belong to?

2. Furthermore, is there a need for more stringent protocols and regulations to be reexamined, updated, and/or implemented regarding Canadian residents' online data? And if so, what will this mean for future advertising and the business sphere?

The objective of this research is to analyze the knowledge, awareness, and opinions of Canadians regarding their online privacy and security. This research is expected to be of interest to active Canadians participating in the online sphere. It is hoped that this study will highlight the issues related to the challenges and ignorance faced by online Canadians. Additionally, this research can be used in aid of establishing action in Canadians to increase their knowledge, their awareness, to provide a deeper understanding on the topic, to serve as a platform for further thoughts, and to entice action for possible intervention by the Canadian government.

This thesis will first examine the Personal Information Protection and Electronic Documents Act (PIPEDA) as well as the Canadian Anti-Spam Legislation (CASL) through literature review. This thesis will then address and discuss the theoretical framework utilized, followed by the methodology. Finally, after clearly answering the research question and secondary objectives, the research process is critically evaluated, results are examined, key recommendations derived from the research are discussed, and suggestions for further research are presented. The following hypotheses were made in conjunction to the research question and secondary objectives:

1. Canadians residents have considerably low knowledge when it comes to data collection practices in Canada and have further low awareness of the legislations and acts put in place to protect them.
2. There is a current crisis regarding the privacy and security of Canadian residents surrounding upon ethicality.

3. There is an immense need for more stringent protocols and regulations regarding Canadian residents' online data. Furthermore, that this need will effectively change the advertising and the business spheres.

2 Privacy And Digital Technological Advancements

2.1 Personal Information Protection And Electronic Documents Act

Following expansive consultations across multiple stakeholders regarding the topic of data and privacy protection in Canada, a set of guidelines were approved as the national standard by the Standards Council of Canada. These guidelines came to be known at the Model Code for the Protection of Personal Information. Out of this PIPEDA was born and passed into law in 2000.

PIPEDA, which officially came into effect following a three-stage integration process over four years on January 1st, 2004, is the Canadian Law protecting the rights and privacy of consumers in Canada from the emerging e-commerce world. Specifically, the Law focuses on establishing a framework in our increasingly technologically driven lives while governing how private organizations and federally regulated organizations carrying out commercial activities are allowed to collect, store, utilize and distribute any personal information and data they collect from consumers.

2.2 Valid Consent

"The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." (Personal Information Protection and Electronic Documents Act, 2000).

PIPEDA in its current form, governs a wide range of commercial activity and has continued to slowly evolve in the near twenty years since its introduction. There are 10 interrelated privacy

principles which guide organizations on how to handle collected consumer data. Simply highlighted by Rice & Bogdanov, (2018), there principles are as follows:

- Accountability – the collector of the personal information and data is accountable for it.
- Identifying Purposes – before data can be collected the purpose of the collection must be disclosed.
- Consent – the individual must provide consent.
- Limiting Collection – data collected must be done in a lawful manner and should not exceed what is required for the identified purpose.
- Limiting Use – data collected can only be used for the identified purpose, except in cases where the individual gives consent.
- Accuracy – data collected must be accurate and up to date for its required purpose. Safeguards – data collected must be securely safeguarded.
- Openness – information about the collectors polices regarding data collection must be readily available.
- Individual Access – consumers should be able to upon request be informed of the existence, use and disclosure of his/her collection information and be given access to it.
- Challenging Compliance – a individual should be able to challenge any practice.

PIPEDA is enforced by the Office of the Privacy Commissioner of Canada. However, the Commissioner does not have the authority to issue final decisions on complaints. The Commissioner however is able to seek a court order from the Federal Court to achieve resolution (Office of the Privacy Commissioner of Canada, 2000).

Consent is the fundamental tenant of PIPEDA and it is implicitly stated that under PIPEDA, organizations must obtain consent from their consumers in regards to the collection and dissemination of their collected data. Furthermore, data collected from consumers is only supposed to be used for the purpose it was stated and collected for by the collector.

Section 4. 6.1 “For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.” (Personal Information Protection and Electronic Documents Act, 2000).

The current model of PIPEDA is flawed because it is based around the idea that consumers consent to trading their personal data and information in exchange for desired services. Essentially this exchange can be viewed as contract based on the informed and willing consent of consumers who agree to share their personal information and data.

Despite the above, it is argued by some that PIPEDA has not done enough to ensure proper application for its own tenants. Even with evolution in its own principles, it can be seen that PIPEDA tends to be more reactive than proactive given the rise of new entrants of business companies in the marketing sphere. The likes of MP Peter Kent, the Conservative critic for Access to Information, Privacy and Ethics, has raised this issue as recently as 2018 with the following “PIPEDA, today, is barely adequate. We’re really only scraping the surface of a very rapidly changing threat to privacy” (Global News, 2021).

Another major hindrance for PIPEDA centers around PIPEDA’s current principles in regard to data subjects ”rights to be forgotten”. Under PIPEDA, individuals have the right to withdraw consent, but companies can still retain their already collected data as long as it is essential to the stated purpose for which it was initially collected (Coos, 2019).

Further, no discussion about the rights and privacies of the Canadian consumer in the digital world would be complete without broaching the topic of the Canadian Anti-Spam Legislation (CASL). CASL is the Federal Law that came into effect on July 1st, 2014 that governs spam and other electronic threats in Canada. CASL’s, which the Commissioner shares the responsibility of enforcing with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau, introduction naturally resulted in modifications to PIPEDA.

2.3 Canadian Anti-Spam Legislation

The legislation of CASL applies to all CEMs that are transmitted through electonic sources (email, text, instant messages, social media, and voicemail). CASL came into effect as a means of protecting Canadian consumers and to prevent businesses from misusing digital technology while ensuring that Canadians could still operate and compete in a global digital market. CASL's focus can be broken down to the need to eliminate any forms of communications from businesses that would lead to the use of electronic meidums to conduct commercial activities.

Any such negative conduct would provide the following hindrances:

- "impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities;
- imposes additional costs on businesses and consumers;
- compromises privacy and the security of confidential information; and undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities in Canada and abroad." (Canadian Anti-Spam Legislation).

In short, CASL exists to create a safer online marketplace in relation to the sending of CEMs, and the installing of computer programs on systems in Canada. They achieve this goal by reducing the negative effects of spam and related threats such as phishing, identity theft, and the spreading of malicious software in the form of viruses and malware.

CASL has the power to investigate and instigate punitive actions against violators of the law and set monetary penalties when needed. It should be noted that violators of CASL could find themselves facing significant monetary penalties ($1,000,000 per individual and up to $10,000,000 for entreprises). In addition to monetary fines, there exists the possibility of director's and officer's "liability and extended liability for those involved in committing the violation" (Canadian Anti-Spam Legislation, 2010).

In fact, since CASL's introduction in 2014, violators have had to pay out nearly $1.4 million Canadian dollars of which approximately $730,000 came from administrative monetary penalties, while the remainder came from negotiated settlements (Government of Canada, 2021).

Despite PIPEDA and CASL both being in place and having consent as a major tenant, is enough being done to truly empower consumers right to exercise their consent to giving away their personal information and data? In an age where the access to and the obtaining of information and resources is being withheld from users to encourage the acceptance of informed consent, the phenomena of coercion can be the result. Thus, is there truly express consent in such scenarios? According to CASL under "Express consent — sections 6 to 8". there "A person who seeks express consent for the doing of an act described in any of sections 6 to 8 must, when requesting consent, set out clearly" and simply the following information (Canadian Anti-Spam Legislation, 2010):

- the purpose or purposes for which the consent is being sought;
- prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies that other person;
- any other prescribed information

2.4 Valid Consent vs. Coercion

There are many factors to consider when discussing consent. If a consumer chooses to access a website that requires that they "accept all cookies" before they are allowed the freedom to access the website's information, should that be seen as consent if refusal to accept means they are denied? Furthermore, most consumers will simply comply without giving a second thought to what it is they are allowing to be collected from them. Surely, in cases such as these, consent was more coercion and thus voidable.

If these instances can be seen as coercion of consent and as a result then be deemed voidable, this presents interesting positions for consumers who may then feel the necessity to seek reconciliation under CASLs principles:

"Section 47 of CASL: 47 (1) A person who alleges that they are affected by an act or omission that constitutes a contravention of any of sections 6 to 9 of this Act or of section 5 of the Personal Information Protection and Electronic Documents Act that relates to a collection or use described in subsection 7.1(2) or (3) of that Act — or that constitutes conduct that is reviewable under section 74.011 of the Competition Act — may apply to a court of competent jurisdiction for an

order under section 51 against one or more persons who they allege have committed the act or omission or who they allege are liable for the contravention or reviewable conduct by reason of section 52 or 53." (Canadian Anti-Spam Legislation, 2010).

Another major factor to consider in regard to the idea of consent is just how informed consumers are in relation to the methods in which organizations collect their information. Research on this topic has been limited but in the most recent study carried out in 2016 by the Office of the Privacy Commissioner of Canada (OPC) called the Phoenix Strategic Perspectives brought up worrying information. "In the 2016 study, the OPC found that 32% of Canadians did not feel confident that they had enough information to know how new technologies may affect their privacy, down from 41% in 2009 and up from 29% in 2000." (Rice & Bogdanov, 2018).

When it comes to the ideas surrounding consent Daniel Therrien, Privacy Commissioner of Canada, discussed the following regarding the topic (Canada's Anti-Spam Legislation, 2017):

- "PIPEDA allows for implicit consent and requires explicit consent based on criteria that
- generally makes sense. Does it work? It all depends on whether meaningful consent is
- obtained, and people do come to us frequently to say, "Maybe the law allows for
- implicit consent, but I never understood that I was giving implicit consent for this or that conduct by the organization.

This further illustrates that while consumers may be granting consent to the collection of their data and information, they may not be fully cognisant to what they are actually consenting to. In Rice and Bogdanov's (2019), emperical study, 75% of respondents did not know the answer to the question: "When a website has a Privacy Policy, it means that the site will not share its visitors' personal information with other companies without their permission?".

2.5 PIPEDA vs. GDPR

The European Union's General Data Protection Regulation (GDPR), is seen by many as the toughest and most stringent legislation covering privacy, data and security in the world. The GDPR came into full effect on May 25th, 2018 and while it was drafted and imposed by the European Union it tackles organizations anywhere in the world once they are engaged in the activity of

collecting data and information related to people in EU nations. PIPEDA, has been recognized by the European Union as possessing requirements that match the standards of the GDPR and received a partial adequacy decision from the European commission as a result of this.

However, it should be recongnized that the European Commission adequacy decision in regard to PIPEDA centers around and specifically applies to commercial organizations. This is a result of PIPEDA's applicability criteria. In other words, there are several organizations that fall outside the scope of PIPEDA's applicability criteria. Such as: Non-profit organizations, Political Parties, Educational Organizations, and any other organization that does not deal in the scope of commercial agendas.

The GDPR by its very design has a far greater reach than its Canadian counterpart. The laws of the GDPR are applicable and enforceable against any person, organization, agency or body that deals in the collection of data and information from EU subjects.

The major difference between PIPEDA and the GDPR comes down to the existence of the Extraterritoriality clause that exists in the GDPR. Extraterritoriality, refers to the state of being free from the jurisdiction of local law. As a result of the GDPR's above mention clauses their reach is international reaching in comparison to Canada's PIPEDA. Any organization collecting the data and/or information of a EU subject, whether they reside in the EU or not, fall under the eyes of the GDPR and must adhere to there statutes (Coos, 2019).

Finally, in regards to the topics of consent and the right to be forgotten the GDPR are far more explicit. The GDPR requires the providers of data and information to be cognisant of the reasons for data collection and consent explicitly to allowing their data and information the be collected (Coos, 2019). Also, in regards to the right to be forgotten PIPEDA's rules can be seen to be more implied while under the GDPR this right is explicit.

3 Methodology

The purpose of this study is to identify the knowledge or lack thereof of Canadian residents have regarding their online privacy and security, and to identify major challenges/issues with current

policies in place. As the reviewed literature reveals, the Canadian government has implemented a series of preventative and protection acts and policies to aid in protecting Canadian residents' privacy online. However, more demanding protocols are needed to fully assess all areas of the online sphere. While according to The Government of Canada "CASL is designed to help protect Canadians from spam and other electronic threats received from either legitimate businesses or illegitimate actors", "legitimate enterprises can also knowingly and unknowingly cause harm to consumers and the electronic marketplace" (Branch, 2021).

Although most companies and organizations follow protocols outlined, and there are repercussions for those that do not comply, it is evident that by coercion, Canadian residents are releasing and exposing personal information without full comprehension of these actions. More importantly, Canadian residents are participating in the online sphere without clear knowledge of their information's infinite lifecycles and long-term impacts. The Internet of Things: another highly underestimated technological tool with vast capabilities beyond measure. The presupposition of this thesis is the major lack of knowledge of Canadian residence regarding the topic of online data policy.

Canadian residents' unawareness of the full extent of data collection practices presents unethicality to those collecting. Furthermore, an unethical position for those currently operating in the business online marketplace: a structure aimed to increased profit margin for companies. Collection practices from these organizations need to be reevaluated, thus, further government intervention is needed.

The research question is:

1. Are Canadians residents aware of how much digital data is being collected about them while participating in online spheres?

3.1 Research Approach

This thesis uses mixed methods of both quantitative and qualitative research methods. Quantitative research is a strategy that focuses on quantifying the collection and analysis of data through definitive answers. Thus, the research strategy selected was a multi-questioned

comprehensive survey designed to answer the main research question and additional secondary objectives.

The multi-million-dollar online survey platform company, Survey Monkey, highlights the importance of survey research. Moreover, that surveys can help measure the representative value of individual opinions, experiences, and views and when performed well, survey research can provide concrete data on those attitudes and behaviours surveyed, thereby providing key findings utilized in making important decisions ("Why Survey Research and Survey Methodology Matter", 2021).

It is perceived that for this study, a multi-question survey will serve as the most optimal approach, while providing additional critical thinking as ironically the medium used, is the medium in question—The internet of Things. To gauge the research from both a quantitative and qualitative approach, 33 qualitative multiple-choice questions are featured on the survey with 2 qualitative questions. Though proportionately smaller in the sense of overall research methods, the qualitative questions aided in adding a holistic understanding of the study from different viewpoints. This mix of research methods will be used to address the main research question and secondary objectives.

Julia Brannen author *of Mixing Methods*: Qualitative and Quantitative Research, suggests that "researchers ought to be flexible and therefore ought to select a range of methods that are appropriate to the research problem under question" (Brannen, 1995). This older and more widely used terminology for this strategy is called triangulation. Further, Brannen, highlights that "triangulation does not merely involve methods and data but investigators and theories as well" (Brannen, 1995). Moreover, that "large researchers have taken the term to mean more than one method of investigation and more than one type of data" (Brannen, 1995). The benefits of multiple methods of data was the reason for using both qualitative and quantitative research methods.

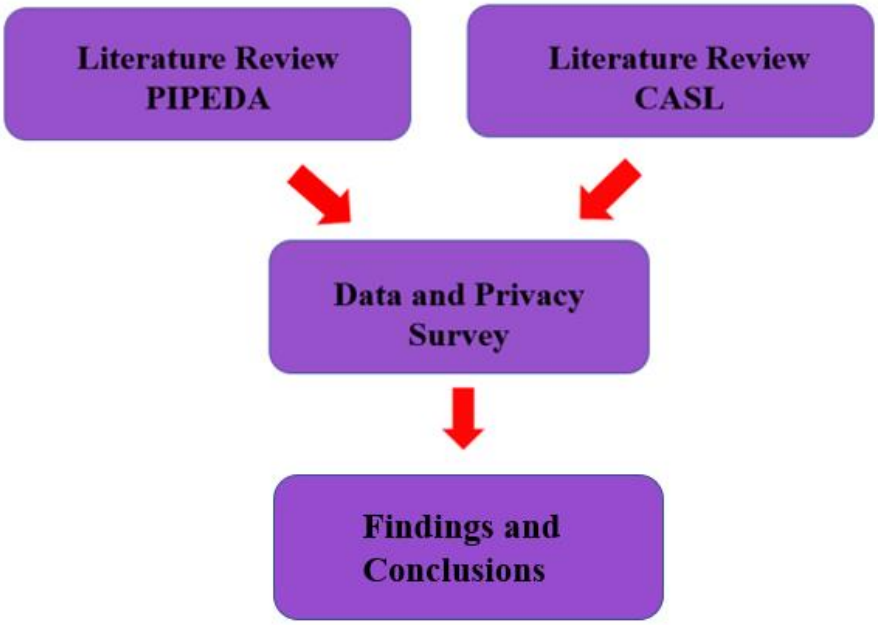
Qualitative research provides critical insights that are difficult to produce or replicate with quantitative research. (Denzin & Lincoln, 2013). Thus, the implementation of qualitative research was essential in researching the opinions and attitudes of Canadian residents verbatim. More

importantly, Ritchie et al (2014), highlight that qualitative research can, and should be conducted in a manner that stands up to external scrutiny, and outlines our views that qualitative studies can be used to draw wider interfaces about the nature of the social world. Providing the opportunity for qualitative research in an online survey format, proved benefitial by providing a medium in which respondents could answer questions honestly, intently, anonymously, and from the protection of their own homes.

Sarah T. Roberts author of *Behind the Screen* (2019), provides an eye-opening look at the many indivisible works that "protect us from seeing humanity's worst on today's commercial internet" (Roberts, 2019). Furthermore, that the internet affords one the opportunity to textually partake in identities separately made from real world embodiments, and that these alternate identities make it much easier to interact with others...behind the screen (Roberts., 2019). Thus, users are more likely to participate honestly in their interactions while their identities are protected in the sense of being "hidden behind a screen". This crutial element of honesty, validitiy and reliability, was taken into consideration with the addition of qualitative answers given the form and distribution of this survey.

Figure 3 — Structure Of Research

Lastly, Figure 3 demonstrates a visual representation of the structure of this research, as well as the plan to answer the research questions presented.



3.2 Data Collection

Data were collected from Canadian residents of 18+ years only to ensure the validity of this study. This survey was distributed online using GoogleForms; therefore, it was not limited to location—all Canadian residents regardless of location could access the survey. Rather, all Canadian residents with access to an internet connected device had access to this survey; a rate of 96% of the population as outlined previously by Statista, 2021. A more than reasonable and viable population accessibility source. Therefore, no additional measures were taken for those who could not access the internet, as most residents of Canada have access. Furthermore, no respondents or requests were sent to the researcher's attention, and no further questions or comments were sent to the inquiry email stated.

As mentioned, this survey consisted of 33 multiple choice questions and featured 2 qualitative open-ended questions (see ***Appendix 2*** *Survey Questions* for complete survey and questions). Secondary data was used to create survey questions and present key findings. This secondary data was used to add an informative aspect to this survey. While respondents answered questions, they were also educated on the digital realm of data collection concomitantly. Finally, the results from the survey itself, presents primary data for future study.

The research conducted and results obtained followed all recommended and legal policy according to JAMK University procedures for research involving human subjects. Respondents were clearly asked to provide informed explicit content, prior to entry into the survey. Any respondents that did not provide consent, results were not collected or used. All respondents provided consent participate in this study, while 0 respondents opted out/did not provide informed consent. Please see **Appendix 5.** Explicit Consent for consent of individuals.

Additionally, all results were safely and privately collected, and will be used for the purpose of this thesis. This study and its results are permitted for use by other academic or researching bodies to further research and literature in this field. Disclaimers of participants rights and reason for conducting this study was listed prior to entry of the survey. See **Appendix 4.** Survey Policy and Disclaimer for full survey policy and disclaimer. The survey was available online for 30 days and distributed through email, social platforms, and word of mouth. A total of 124 responses were submitted and analyzed.

The survey format was open and not in quiz form. This meaning, respondents could scroll through all questions at one time, and could go back and change previous answers. The survey was presented on one page. The reason for this being is, respondents that were provided more knowledge and information on a particular subject later, could cause a reaction in remembering and provoking further thought resulting in changing their knowledge on a previous question answered.

Qualitative answers were collected and analyzed individually. Respondents were given the option to type and leave comments (with no space limit), on their thoughts and opinions about this study. The first free thought question asked respondents to provide any further comments, thoughts, feelings, or concerns regarding the privacy and security of Canadians and their online data. The second free though question then asked respondents to provide any further comments and thoughts regarding this survey. This allowed respondents to share any additional information they thought significant to add to this study of research and to provide a voice for respondents outside of their digital answers. Please see ***Appendix 2.*** *Survey Questions* for complete survey and questions.

3.3 Data Analysis

Univariate analysis was used to identify key metrics such as age, gender, and occupation/industry field. Additionally, univariate analysis was used to provide definitive yes or no results for specific questions. Other variables were measured through various types of survey scales. Statistic solutions, an editing service for dissertations with expertise from both a quantitative and qualitative approach, highlights that survey scales are “the indexes that measure those types of variables that are not directly observed but are instead inferred from the other variables that are directly measured” (Statistic Solutions, 2021). Thus, this survey featured a series of 8 Likert scales that were used to identify survey responders’ agreements to statements.

The Likert scale answer ranges were presented as: 1) Definitely would, Probably would, Probably would not, Definitely would not 2) Extremely aware, Very Aware, Somewhat aware, Not so aware, Not at all aware 3) Very likely, Likely, Neither likely nor unlikely, Unlikely, Very unlikely and 4) A great deal, A lot, A moderate amount, A little, Not at all. In addition, ranking scales were used to

also measure respondents' knowledge to statements. Ranking scales of 1-10, 1 being not familiar and 10 being familiar with were utilized.

SPSS statistics software and Microsoft Excel were used to analyze statistical data. Measures of central tendency were then used to determine the consistency of results for ranking scales of familiarity. With the addition of ranges, quartiles, interquartile range (IQR), and outliers determined. Quartile were utilized to determine the additional values above and below the mean. A quartile can be calculated by dividing the distribution into four groups (Quartile Definition, 2021). To be more specific, "a quartile divides data into three points—a lower quartile, median, and upper quartile—to form four groups of the dataset" (Statistics: Power from Data! Range and quartiles, 2021). Lastly, crosstabulation was used to find correlations and patterns in the collected data.

Triangulation of data was utilized by using multiple methods of research: qualitative and quantitative. Further analysis on participants occupation and industry field in correlation to their knowledge and understanding of the subject was further explored. Additionally, in supplementary to the basic structured questions, respondents were also presented with information regarding the scope of a questions prior to the formal asking of the question. This was to ensure respondents had a clear unwavering understanding of what was being asked. Open ended qualitative questions were utilized to allow respondents to add any relevant information and their overall thoughts, comments, opinions, and attitudes on the matter.

3.4 Verification of findings

To affirm internal validity, the quality of the research presented is evaluated by its reliability and validity. According to Saunders et al. (2009), "reliability refers to the extent to which your data collection techniques or analysis procedures will yield consistent findings". Therefore, there are issues that must be acknowledged that provide limitations of research. It is imperative to investigate the reliability and validity of the research findings and whether reliability and validity were accomplished. Furthermore, to identify if these possible issues positively or negatively affected the internal validity of this study.

Research questions were crafted specifically to incorporate the original framework of the research questions. This provided the means to understand the research question in full detail, and to provide additional insight for critical thinking. As a result, the study provides a consistent link between research questions, theoretical framework, methodology and results. It is hoped that respondents and reviewers of this thesis, will gain more knowledge of the current issues faced with data collection practices in Canada, the policies that are in place, and provide further thought regarding the privacy and security in other nations as well.

The findings of this research will be limited in regard to their generalizability in other contexts as research questions were very specific to the area of study. Questions stated the issue in the proposed question for respondents to answer. For example, Question #7: “Are you familiar with the Personal Information Protection and Electronic Documents Act (PIPEDA)?” Answer: “Yes or No?”. Other questions were also specific and stated which web browsers do you use and which social media platforms do you use.

Researchers investigating social media, search engine optimization, and browser applications may find results useful, as respondents answer what mediums and applications they use and their attitudes and opinions about those mediums. Therefore, the research presented proves reliable for other research pertaining to data collection and The Internet of Things for Canadian residents.

It is also relevant to evaluate GoogleForms as the medium and as the data collection and distribution method. More importantly, to analyze this platforms effect on the reliability and validity of the findings obtained. GoogleForms is a locked platform for applicants possessing a Gmail address email account. However, taken this into consideration, the survey settings were changed to provide anyone with a link access to the survey, regardless of their email provider.

Additionally, with the method of distribution, there is a risk that the data collected may present bias. To negate this issue, distribution was expanded from one central point to various touch point areas of various bodies. With the aid of University faculty and small businesses, this survey was able to be diversified in its applicants’ geographic regions and professions. Data triangulation was used to a gain proper understanding from different perspectives of the investigated phenomenon.

Moreover, secondary research through various reliable and academic sources was conducted to construct the informative survey questions.

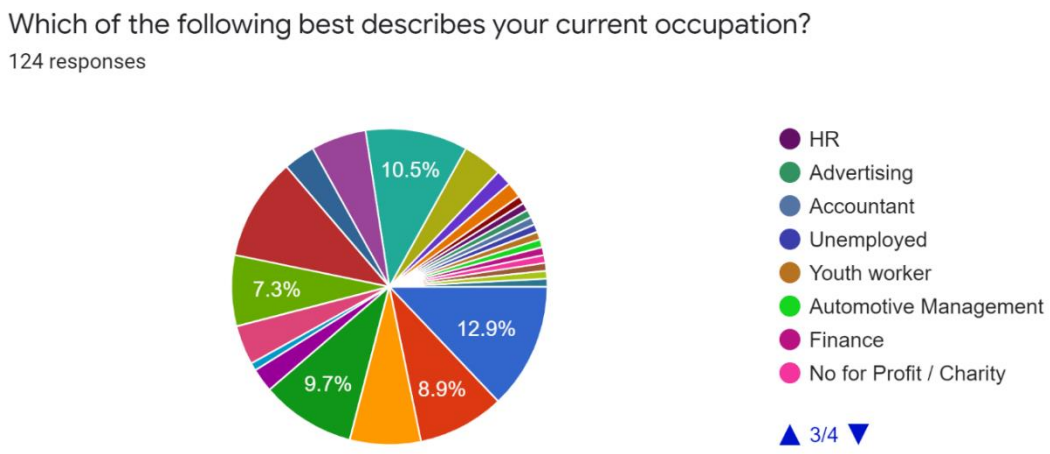
The results presented in this study can change if presented to a different population segment. As individuals are separate entities and behavioural attitudes and opinions cannot be perfectly replicated. Therefore, this data was interpretated subjectively, as the results of this thesis pertains directly to the data samples and key research findings collected. The results/opinions within the current population may also change as they learn more about the topic as well.

4 Results

To gain a full understanding of the demographics of respondents, age, sex and occupation/industry field was surveyed. 42.7% of respondents were aged 25-34, 24.2% aged 55-64, 10.5% aged 35-44, 9.7% aged 45-54, 7.3% aged 18-24 and 5.6% aged 65-74. 61.3% of respondents were female, while 37.9% male and 0.8% chose not to specify.

Occupation/Industry

Figure 4 — Occupation/Industry



The following occupations and industry fields were recorded: Administration: 12.9% | Sales: 10.4% | Self Employed/Entrepreneurs: 10.4% | Health Care: 9.6% | Education: 8.8% | Government: 7.2% | Retired: 7.2% | Student: 7.2% | Marketing: 4% | Trades: 4% | Science/Research: 3.2% |

Hospitality: 2.4% | Technology Consultant: 1.6% | Billing Analyst: 1.6% | Legal: 0.8% | Not For Profit: 0.8% | Homemaker: 0.8% | IT/Software: 0.8% | Advertising: 0.8% | Finance: 1.6% | Accountant: 0.8% | Human Resources: 0.8% | Automotive Management: 0.8% | Unemployed: 0.8 | Youth Worker: 0.8%

Ranking Scales

Figure 5 — CASL Familiarity Scale

1 being familiar, 10 being familiar.

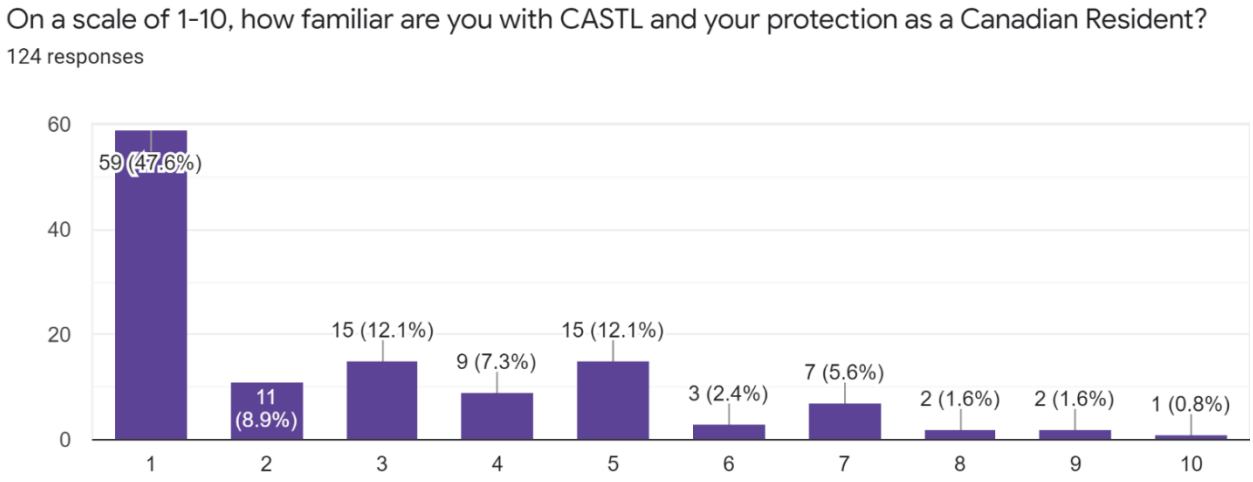
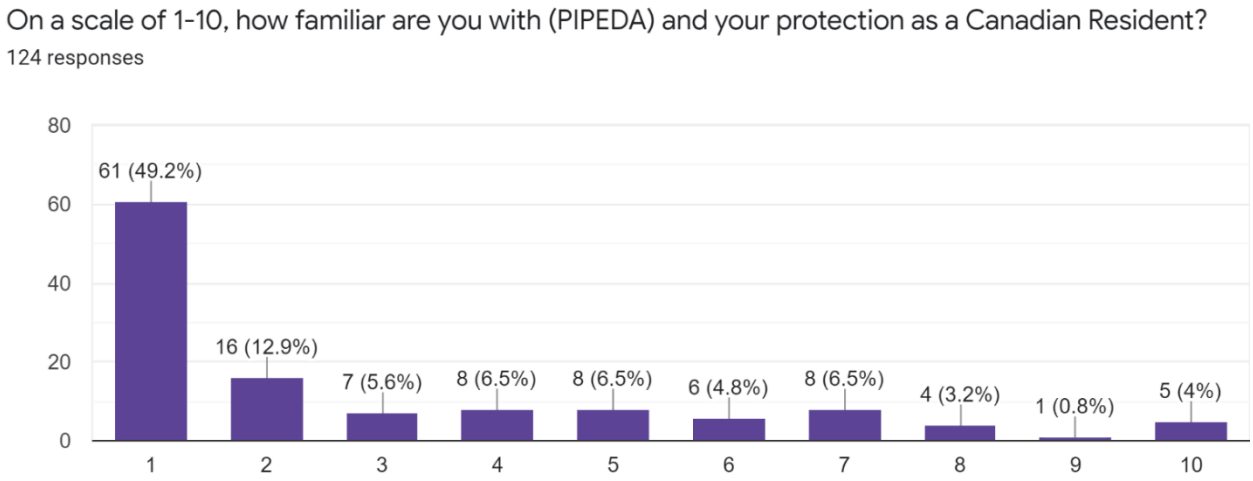


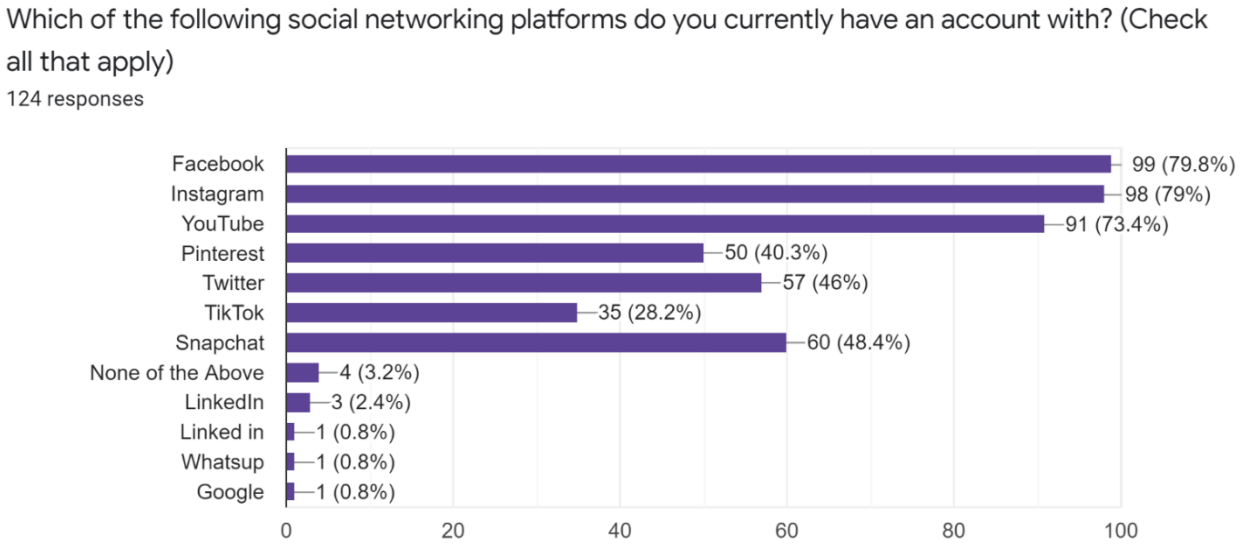
Figure 6 — PIPEDA Familiarity Scale

1 being familiar, 10 being familiar.



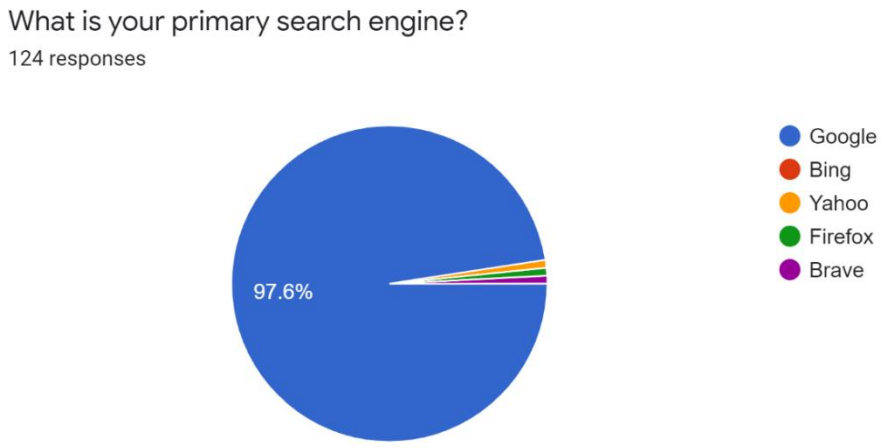
Social Media Platforms

Figure 7 — Social Media Usage



Search Engines

Figure 8 — Search Engine Usage



Likert Scales:

*Do you wish to know more about what is being tracked and what this means for your privacy and security?

- Definitely would: 58.9%
- Probably would: 33.9%
- Probably would not: 7.3%
- Definitely would not: 0%

*Facebook in particular, utilizes various types of tracking software's to follow consumers' activities. This also includes millions of non-Facebook websites all over the web. These tracking tools collect data such as: age, gender, interests, addresses, biometric facial data etc. without users' explicit "opt-in" consent. **Are you aware social media platforms along with many other website, track and collect your data?**

- Extremely aware: 23.4%
- Very Aware: 38.7%
- Somewhat aware: 35.5%
- Not so aware: 1.6%
- Not at all aware: 0.8%

*After answering the previous questions, how likely are you to continue using Facebook and other social media platforms?

- Very likely: 24.2%
- Likely: 38.7%

- Neither likely nor unlikely: 21%
- Unlikely: 8.9%
- Very unlikely: 7.3%

*Are you aware that your data is being tracked and stored by these platforms (Search Engines)?

- Extremely aware: 31.5%
- Very Aware: 35.5%
- Somewhat aware: 29%
- Not so aware: 3.2%
- Not at all aware: 0.8%

*Are you aware that Search Engines and other websites collect information about site users to monitor their online behaviour?

- Extremely aware:16.9%
- Very Aware: 33.9%
- Somewhat aware: 33.9%
- Not so aware: 8.9%
- Not at all aware: 6.5%

*After reading the above, how likely are you to continue using Search Engines?

- Very likely: 38.7%
- Likely: 36.3%
- Neither likely nor unlikely: 21%
- Unlikely: 4%
- Very unlikely: 0%

*After reading the above, are you more likely to clear your search history and internet “cookies”?

- Very likely: 47.6%
- Likely: 32.3%
- Neither likely nor unlikely: 14.5%
- Unlikely: 4%
- Very unlikely: 1.6%

*After completing this survey, how concerned are you about your privacy and security online?

- A great deal: 33.1%
- A lot: 27.4%
- A moderate amount: 31.5%
- A little: 7.3%
- Not at all: 0.8%

Other

Figure 9 — Data Usage Practices

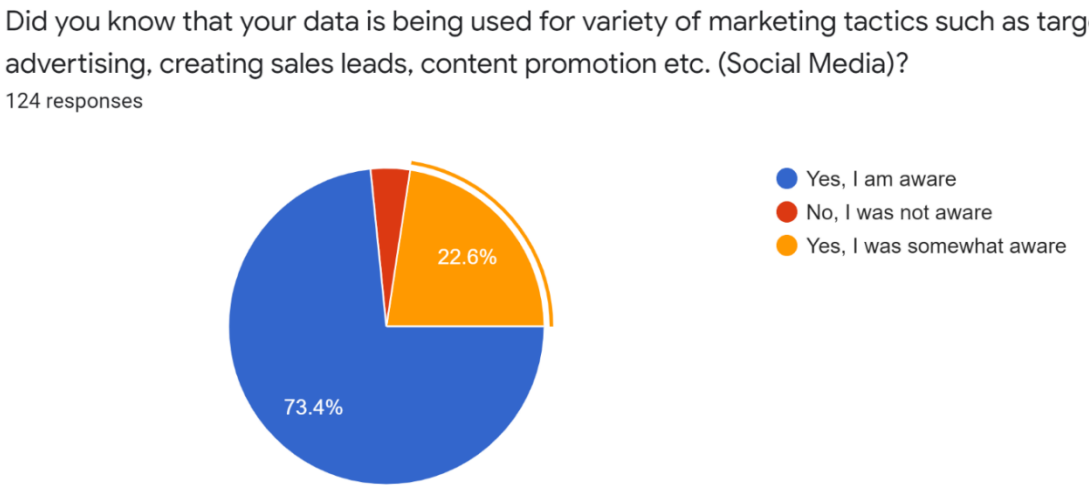


Figure 10 — Marketing Usage Practices

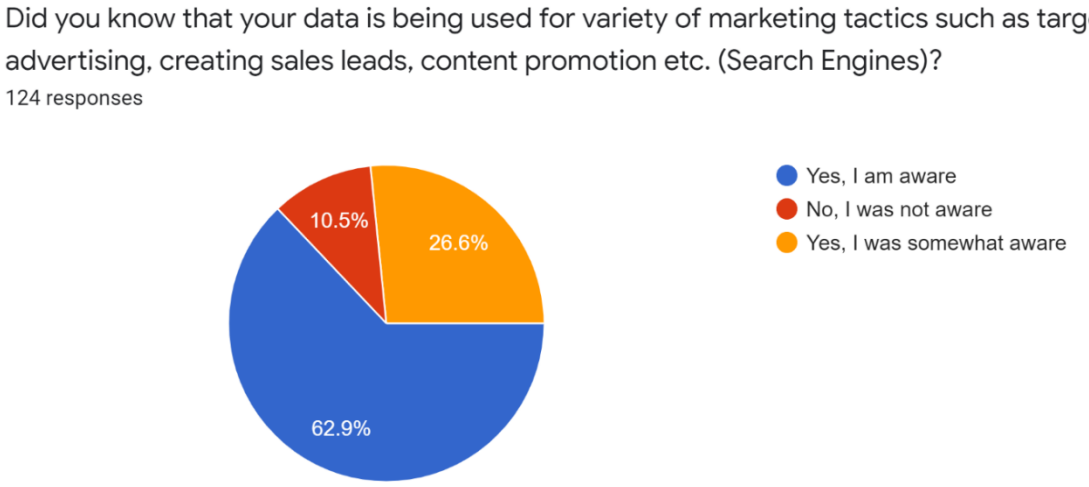


Figure 11 — Protocols & Regulations

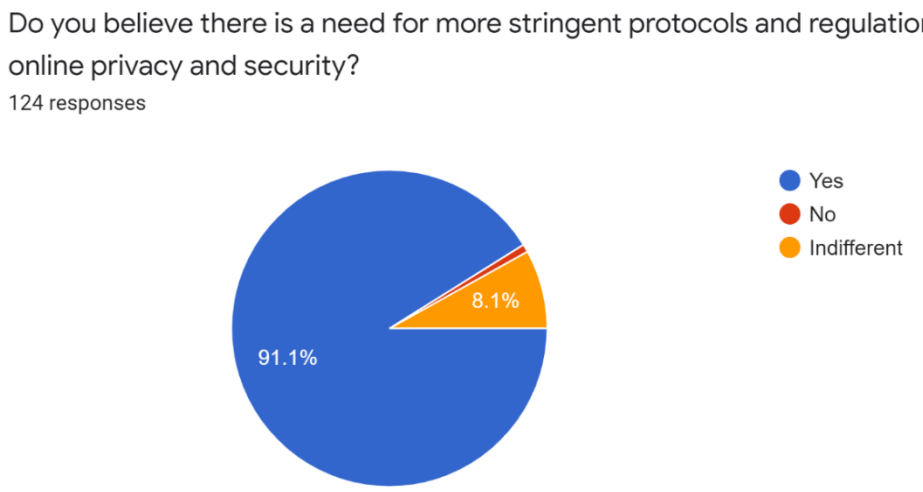
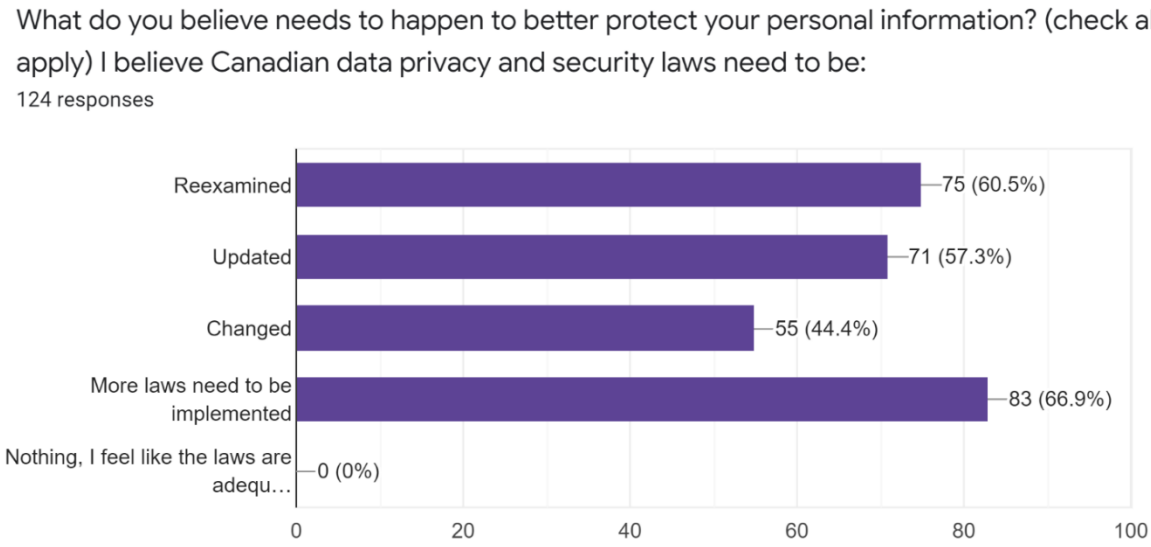


Figure 12 — Protocols & Regulations Recommendations



*How often do you clear your computer search history and “cookies”

- After each browsing session: 2.4%
- Once a day: 7.3%
- Once a week: 11.3%
- Every 2 weeks: 10.5%
- Every 3+ Weeks: 1.6%
- Never: 66.9%

Table 1 — Yes vs. No Questions

	Yes	No
Are you familiar with **Canadian Anti-Spam Legislation** (CASL)?	31.5%	68.5%
Are you familiar with the **Personal Information Protection and Electronic Documents Act** (PIPEDA)?	27.4%	72.6%
Do you use Facebook?	78.2%	21.8%
Are you aware that your data is being tracked and stored by these platforms (Social Media)?	90.3%	9.7%
Did you know that many social media sites/applications not only track their platform, but also track you to other sites, other applications on your phone, and other physical locations you have visited in real life?	75%	25%
Did you know that the Facebook Pixel enables websites and online retailers to gain information about their visitors as the social network analyzes aggregated user behaviour?	57.3%	42.7%
Did you know that social media sites collect, store, mine, and trade your data including trading with overseas and third-party companies?	58.9%	41.1%
You are most tracked online by your IP address and email. Every site you visit, tracks your time spent, and leaves "cookies." Did you know that these "cookies" remain on your computer and assist companies and organizations in determining how to engage with you, which products will attract your attention, and which will most likely convert to a sale?	74.2%	25.8%
Do you clear your search history or computer "cookies"?	56.6%	43.5%
Are you aware that Google is currently in a proposed class action lawsuit in the Supreme Court of British Columbia for allegedly collecting and profiting from Canadians personal information collected without explicit consent?	89.5%	10.5%
Are you aware that website can collect the following data? ~**IP addresses to determine a user's location**. ~ **Information about how the user interacts with websites**. (For example, what they click on and how long they spend on a page) ~**Information about browsers and the device the user accesses the site with** ~**Browsing activity across different sites**. (For example: information insight about the individual user's interests, shopping habits, problems they are facing, etc.)	73.4%	26.6%
Did you know that Search Engines collect, store, mine, and trade your data with third-party companies?	66.9%	33.1%

Qualitative Open-Ended Responses:

Question 1:

*Any further comments, thoughts, feelings, or concerns regarding the privacy and security of Canadians and their online data, please share below:

Respondent unknown: "Interesting stuff. This is intrusive on a other level"

Respondent unknown: "More information be given to the public more regularly about how to combat these privacy moves on a daily usage basis. Governments also need to be more proactive and monitor and oversee the big tech companies with more legislation to protect consumers."

Respondent unknown: "There should be clearer education and communication from our government on what is being collected and how we can opt out or avoid it."

Respondent unknown: "Regarding search engines, I do not think that we have any other option than to accept the consequences that result from using these above-mentioned search engines. But I do think that we need stronger/better aligned laws to protect Canadians."

Respondent unknown: "Govt needs to do more to make companies accountable and protect Canadian citizens."

Respondent unknown: "I do believe google and social media platforms should be more transparent of how much they are collecting to the user. I believe everyone should know that they can literally log on google and navigate to a certain page where it says everything about you (marriage status, interest, income level, etc.) "

Respondent unknown: "This is something that definitely needs to be addressed. All Canadians should have the right to know about that their info is being used and sold."

Respondent unknown: “There are privacy laws concerning many professions, why don’t online privacy protocols fall under the same legislation?”

Respondent unknown: “These people that own these social media platforms have been making BILLIONS on US, the consumer, why wasn't this issue looked into before launching these media platforms? Who dropped the ball? Or ignored the ball?”

Respondent unknown: “It will be very difficult to restrict companies from not using your electronic privacy.”

Respondent unknown: “We need to find a way to make the privacy profitable.”

Respondent unknown: “The privacy/security of Cdns and their online date should be more closely guarded and ought not to be allowed without consent.”

Respondent unknown: “Don't used social media”

Respondent unknown: “Not only should privacy and security laws be reevaluated/changed but this type of information should be made mandatory in our education system as well as tactics to protect ourselves from corporations stealing our personal information without direct and transparent consent”

Respondent unknown: “Indifference to the matter . We live in a digital age . Privacy is our right online but ultimately need to use these platforms /have nothing to hide”

Respondent unknown: “I am acutely aware of the many infringements on my privacy online, but I also selected that I would continue using these platforms. I can only speak anecdotally, but my mindset around these concerns is quite pessimistic in a "they've already spied on all my data, it's too late to bother leaving these platforms now." Personally, I like the idea of GDPR in the EU and it's "right to be forgotten" clause, the problem is I don't see how it could be properly enforced. Following the American hearings against Facebook and other platforms it seemed quite clear that global legislators (Canada included) have a tremendously poor literacy rate when it comes to how

these platforms even work. How do you legislate an entire pillar of modern life when you don't even understand how it works? Do I think more needs to be done? Absolutely. Do I know how to do that? Not in the slightest. Do I think Canadian citizens or government understand the degree to which their privacy is being infringed? No. Glad you're doing research on this!"

Respondent unknown: "People should be able to find simplified, informative summaries of T&C rights and obligations along with the legal summaries when they engage with internet services. Authoritative resources should be easily available to consult by users. We're all warned, but obviously not enough"

Respondent unknown: "Will be difficult to put the genie back in the bottle"

Respondent unknown: "Important information to always be updated/reviewed as technology evolves"

Respondent unknown: "I believe that consumers need to have full transparency and agency regarding how their information is being used in order to make an informed decision on their personal interactions with these platforms."

Respondent unknown: "I use brave browser for privacy n their vpn. Duck duck go as search engine but brave is coming out with their own search engine

Question 2:

*Any further comments and thoughts regarding this survey, please share below:

Respondent unknown: "Informative. Thought provoking."

Respondent unknown: "The survey showed me how casually I have accepted the invasion of privacy by the big tech companies in exchange for access to their social media platforms. It has made me want to be more informed and vigilant. And Yo take more actions to protect my cyber privacy."

Respondent unknown: Important reminder how privacy is being manipulated”

Respondent unknown: “Great informative survey!”

Respondent unknown: “Unsure how much information is shared especially financial etc”

Respondent unknown: “This survey is a wake up call to pay more attention to the websites/search engines that I visit. It 's a reminder how little I know about online collection of data and personal information.

Respondent unknown: “The world is known as a spy 🕵”

Respondent unknown: “I was happy to participate in this survey as it highlights/informs on an important issue that is purposely being with withheld to the public by the corporations abusing their power”

Respondent unknown: “Thanks for sharing this. Very informative.”

Respondent unknown: “good questions. I hope the government will do something about and stope continually collude with BIG TECH.”

Respondent unknown: “Brave browser gives free BaT if u consent to watch adds”

5 Discussion

5.1 Research Questions Analyzed

Based on the results, it appears that majority (over 50%) are unaware or have limited knowledge on data collection. When asked about PIPEDA and CASL, 72.6% of respondents were not familiar with PIPEDA, and 68.5% of respondents were not familiar with CASL. When asked to rank their knowledge on both legislations, for PIPEDA, 49.2% of respondents ranked number 1 in “not familiar” with 80% of total respondents answering under 5. Additionally, CASL, 47.6% ranked

number 1 in “not familiar” with 88% of total respondents answering under 5. It can also be concluded that Canadian residents are not necessarily unaware that data is being collect in general, however, they are unaware of the extent to what is being collected, its overall intended use, and the protections that have been set in place for them.

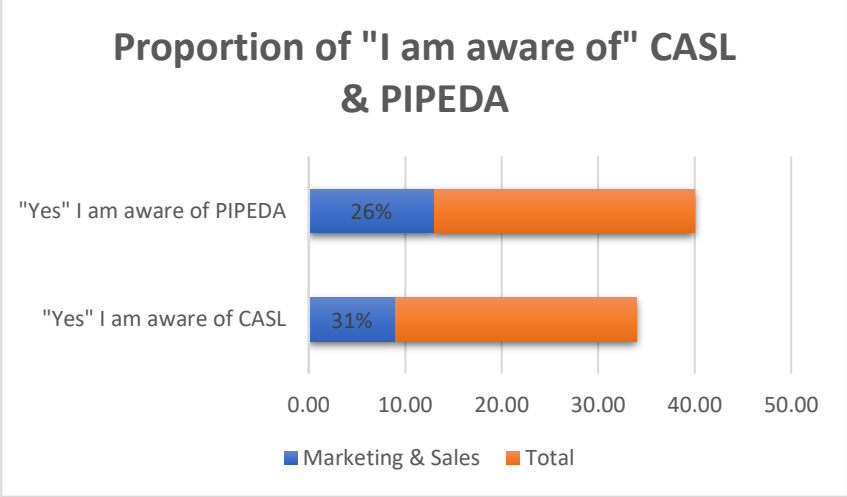
As highlighted in previously and in previous studies, if consumers are not knowledgeable on the intended use and the extent of information gathered, then they can neither engage in privacy-protecting actions, make informed decisions, request their data, or file any complaints regarding the collection with the regulator. More importantly, if Canadian residents are not aware of the laws and policies instated to protect them, how are they able to engage in privacy protecting actions. In support, a respondent stated, “People should be able to find simplified, informative summaries of T&C rights and obligations along with the legal summaries when they engage with internet services. Authoritative resources should be easily available to consult by users. We're all warned, but obviously not enough”, privacy policies or not.

Furthermore, another respondent’s feedback was that the privacy and security of Canadians’ and their online data “should be more closely guarded and ought not to be allowed without consent”. Another respondent stated, “Not only should privacy and security laws be reevaluated/changed but this type of information should be made mandatory in our education system as well as tactics to protect ourselves from corporations stealing our personal information without direct and transparent consent”.

More importantly, a respondent stated, “I believe that consumers need to have full transparency and agency regarding how their information is being used in order to make an informed decision on their personal interactions with these platforms.” Respondents’ general overall comments related to not feeling that adequate consent is obtained by these organizations for the use and storage of their personal data and information. Not only does this present an infringement of their rights to privacy and security, this also offers an element where they no longer own the data that is collected against them. Consequently, through policy and terms disclaimers, organizations are legally able to collect and own all the data collected for infinite measures of time.

It was speculated that respondents whose professions fell in the fields of business: marketing, advertising, or sales would generally have more knowledge regarding CASL, PIPEDA and data collection and privacy. This was speculated given, data collection and business to consumer (B2C) strategy often falls under this realm of information. As speculated, those in the advertising field ranked high in the familiarity with CASL and PIPEDA. On the contrary, respondents whose occupation or industry field was marketing or sales, did not account for the majority of respondents that were aware of CASL and PIPEDA. In fact, these industry fields only accounted for 31% of the total yes responses in being aware of the CASL legislation and 26% of the total yes responses for PIPEDA.

Figure 13 — CASL & PIPEDA Survey Proportion



Similar to this, it was speculated that the higher numbers on the ranking scale of familiarity of CASL and PIPEDA would also be heavily proportioned to those operating in the marketing, advertising, and sales industry. However, the results present a very different scenario as the proportion of marketing and sales respondents did not account for higher rankings of knowledge for both CASL and PIPEDA, while only advertising remained in the higher portion of the scale. The following chart illustrates the proportion of marketing and sales respondents compared to the total number of respondents for each level of familiarity.

Figure 14 — CASL Survery Proportion Familiarity

1 being familiar, 10 being not familiar

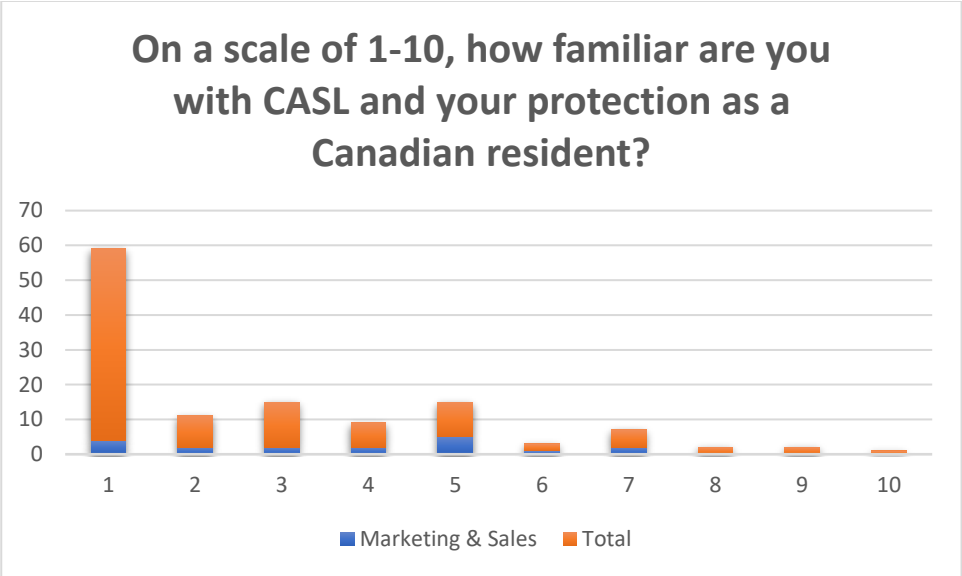
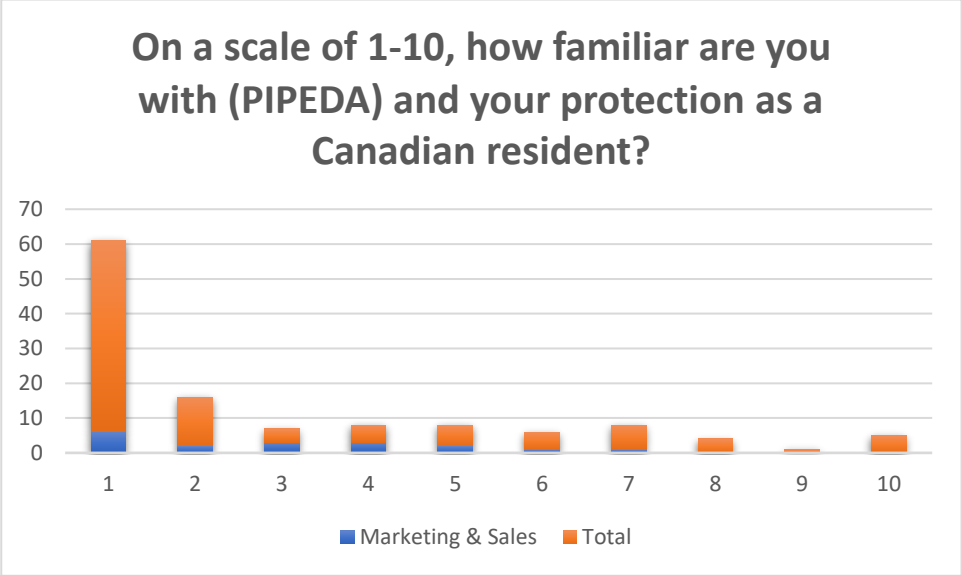


Figure 15 — PIPEDA Survery Proportion Familiarity

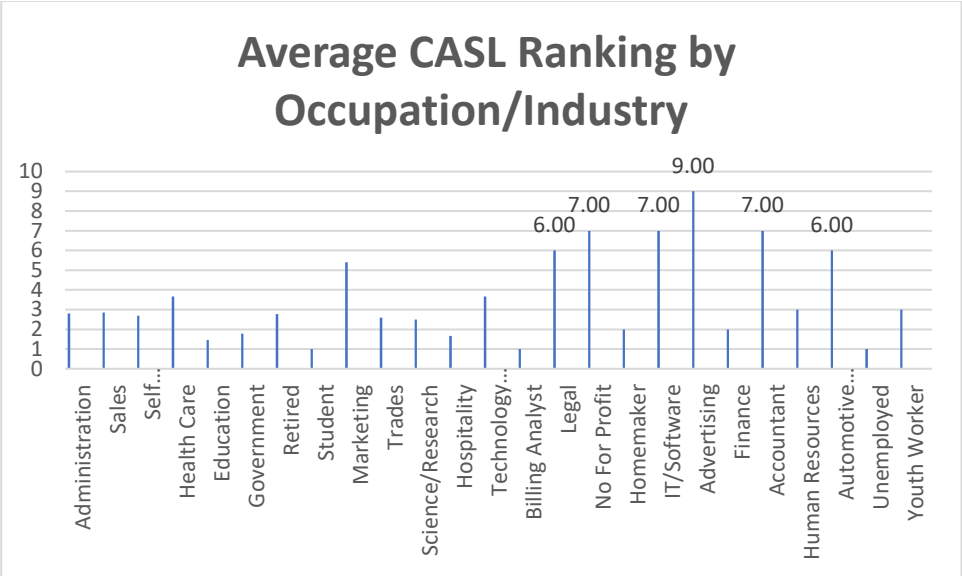
1 being familiar, 10 being not familiar



Further, the top 6 occupations/industry fields that were most familiar with CASL were: Advertising, Not For Profit, IT/Software, Accountant, Legal, and Automotive Management. Although IT/Software and Legal seem relevant regarding the topic of study and legislations knowledge, the other 4 occupations/industry fields were not anticipated.

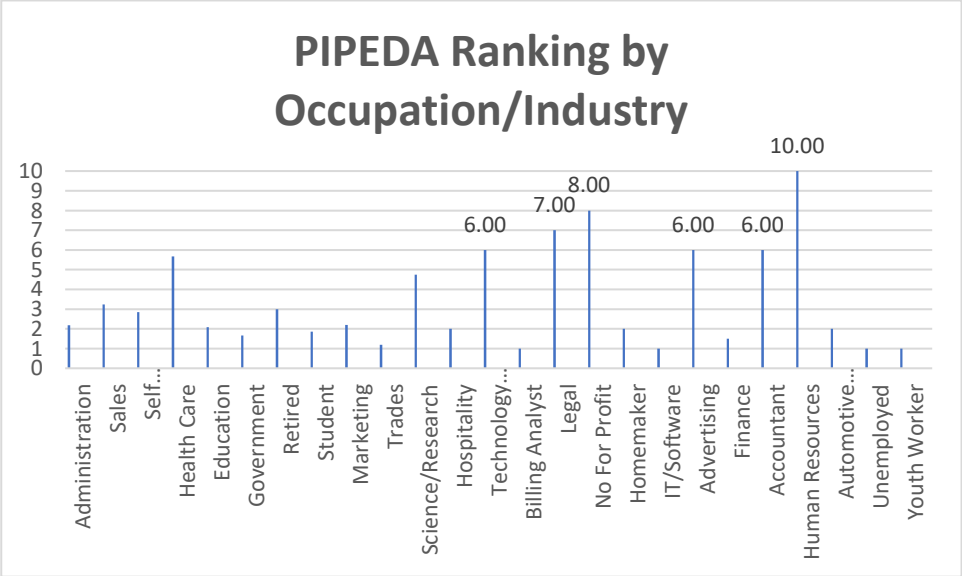
Figure 16 – Average CASL Ranking by Occupation/Industry

1 being familiar, 10 being no familiar



For PIPEDA, the top 6 occupations/inudustry fields that were the most familiar with the legislations were: Human Resources, Not For Profit, Legal, Technology Consultant, Advertising and Accountant. Again, legal, technology consultant and advertising, were all relevant feilds to this study. However, the remaining three were additional occupations/fields whose knowledge on this subject was not anticipated.

Figure 17 — Average PIPEDA Ranking by Occupation/Industry



The data recorded regarding the familiarity scales was indicative to respondent's overall knowledge of current legislation and regulations. Additionally, since all samples are drawn from the same population, the samples are said to be independent and identically distributed (Deep, 2006). The avaerage respondents age was 39.9 and fell within the range of 35 to 44 years of age with a majority of respondents female.

For both familiarity scales results present right skewed distribution (See Figures 18 & 19). Therefore, the medium was used to determine the average. For CASL the average was 2 suggesting a very low overall average. The range, which is the distance between the largest and smallest number was 9.

The Quartiles for CASL were Q1: 2, Q2: 2 and Q3: 4. These measures were used to measure the lack of consistency or fixed pattern; liability to vary or change. Given the results, the data of the CASL ranking scale remained consistently low on the lower end of the scale.

The IQR, a measure of statistical dispersion, is equal to the difference between 3rd and 1st quartiles. Since IQR is a measure of spread which is used for data sets that are skewed, this was utilized for both CASL and PIPEDA familiarity ranking scales. The IQR for the CASL familiarity scale is 3. This was then used to identify outliers which is an extremely high or low value compared to the other values in the data set. Though an outlier of 9 was identified, this is not data that should be considered abnormal.

For PIPEDA, the average was also low, 2. The range presented 9 and the quartiles were: Q1: 1, Q2: 2, and Q3: 5. Again, this data set also remained consistently low on the lower end of the ranking scale of knowledge. IQR was determined as 4 with no outliers identified in the data set. See below for a full break down of measures of central tendecies.

Table 2 – Statistics – CASL, PIPEDA & Age

Statistics

		CASL	PIPDA	Age
N	Valid	124	124	124
	Missing	0	0	0
Mean		2,8065	2,9758	39,9919
Median		2,0000	2,0000	33,0000
Mode		1,00	1,00	28,00
Std. Deviation		2,24759	2,64871	14,79095
Range		9,00	9,00	47,00
Minimum		1,00	1,00	21,00
Maximum		10,00	10,00	68,00

Table 3 — Additional Measures Of Central Tendency (CASL)

CASL ADDITIONAL MEASURES OF CENTRAL TENDENCIES	
MEAN	2.81
MEDIAN	2
MODE	1
RANGE	9
QUARTILES	Q_1 -→ 1 Q_2 -→ 2 Q_3 -→ 4
INTERQUARTILE RANGE	3
Outliers	9, 10

Table 4 — Additional Measures Of Central Tendency (PIPEDA)

PIPEDA ADDITIONAL MEASURES OF CENTRAL TENDENCIES	
QUARTILES	Q_1 -→ 1 Q_2 -→ 2 Q_3 -→ 5
INTERQUARTILE RANGE	4
Outliers	None

Figure 18 — Distribution Of CASL Familiarity Scale

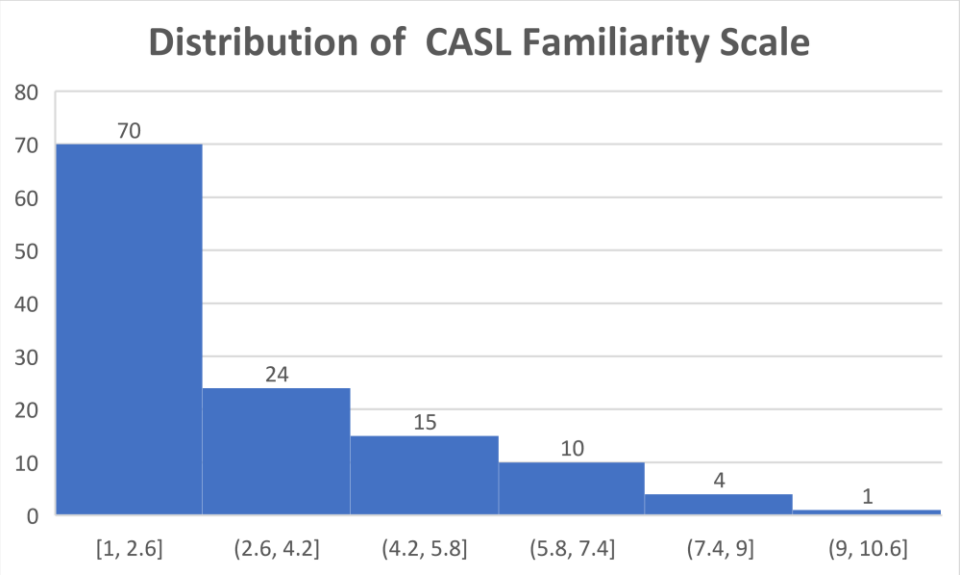
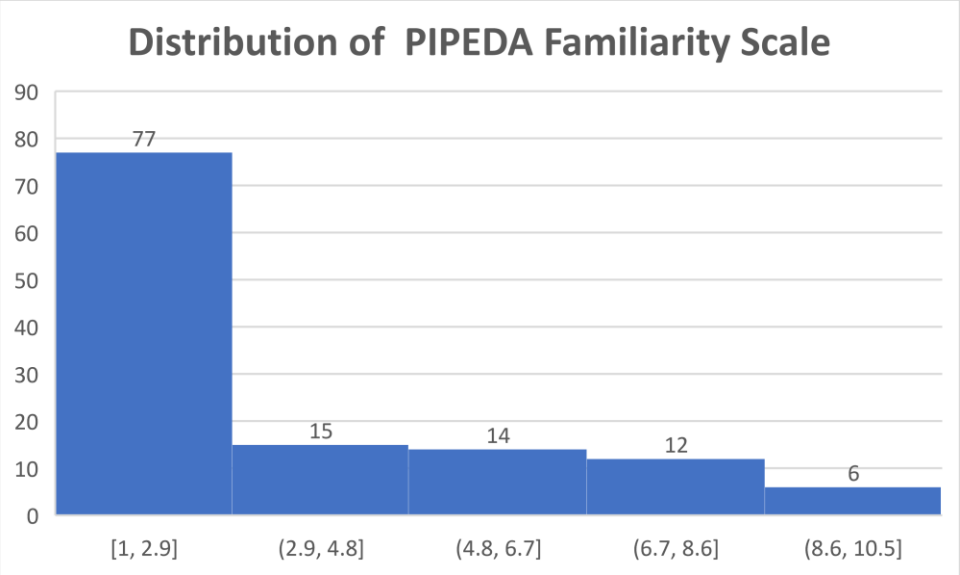


Figure 19 — Distribution Of PIPEDA Familiarity Scale



The correlation between CASL and PIPEDA is high and presents a 48.7% variable degree. Further, with this positive correlation, the data sets rise and fall together. The level of significance is zero, therefore, the findings can be accepted as 100% positive. The correlation between CASL and age is low at 4.4%, and the correlations of PIPEDA and age is also low at 5.6%. The level of significance for both CASL and age and PIPEDA and age are both very high. However, correlations are not only low but are insignificant. Thus, the only significant thing is the relationship between CASL and PIPEDA.

Table 5 — Correlations – CASL, PIEPDA & Age

Correlations

		CASL	PIPDA	Age
CASL	Pearson Correlation	1	,487**	,044
	Sig. (2-tailed)		,000	,628
	N	124	124	124
PIPDA	Pearson Correlation	,487**	1	,056
	Sig. (2-tailed)	,000		,534
	N	124	124	124
Age	Pearson Correlation	,044	,056	1
	Sig. (2-tailed)	,628	,534	
	N	124	124	124

Are Canadians residents aware of how much digital data is being collected about them while participating in online spheres? When asked questions pertaining to the knowledge of being

tracked, information being stored, and the practices of online organizations, respondents were aware. Regarding social media, a wholesome 90.3% of respondents are aware that their data is being tracked and stored by social media platforms, 75% of respondents knew that social media sites and applications not only tracked their platforms but also track them to other sites, other applications and other physical locations in real life, 73.4% of respondents were aware that their data is being used for a variety of different marketing tactics such as targeted advertising, creating sales leads and content promotions, and 57.3% of respondents knew that Facebook analyzes aggregated behaviours and enables websites and online retainers to gain information about their visitors.

Though, it seems users are quite aware of the general principles of being tracked online, 92.8% of respondents wished to know more in some capacity about what is being tracked and what this meant for their privacy and security. Similarly, with search engines, respondents also seemed very aware of being tracked and understood the use of “cookies”. 74.2% of respondents were aware that “cookies” remain on your computer and assist companies and organizations in determining how to engage with you, which products will attract your attention, and which will most likely convert to a sale. While most respondents (56.5%), clear their search engine “cookies” 66.9% of total respondents never cleared their internet browsing history.

Similar to social platforms, 33.9% of respondents were very aware of the fact that search engines and other websites collect data and information about site users to monitor their online activity, and 62.9% of respondents know that that data collected is being used for variety of marketing tactics such as targeted advertising, creating sales leads, content promotion, etc. 73.4% of respondents answered yes to being aware that websites collect informational insight about user’s interests, problems they are facing, shopping habits, , etc., and 66.9% of respondents were privy to the fact that these websites and search engines collect, store, mine, and trade your data with third-party companies. However, after presenting respondents secondary information regarding these data collection practices, 79.9% of respondents answered in some capacity of likeliness, that after reading the above, they are more inclined to clear their search histories and internet cookies to negate being tracked.

What does this plethora of digital data mean for Canadian's privacy and security online? To answer to secondary objective, this plethora of data means there are current risks to the information

being collected. These risks include data being traded, being stolen or getting into the wrong hands, used for marketing and advertising tactics, increase annoyance in daily lives, and may lead to unnecessary shopping (when used for repeated advertising). An issue CASL aimed to protect with its anti-spam principle. Additionally, through investigating the privacy notice, it can be understood that the companies collecting the data, possess legal ownership of all data.

When respondents were asked how concerned they were about their privacy and security online, particularly after completing the survey, 60.5% of respondents answered within “a lot” and “a great deal”. Further to this point, qualitative responses favoured that Canadian residents should know more and be more active in what is being collected about them online. One respondent highlighted “There should be clearer education and communication from our government on what is being collected and how we can opt out or avoid it”. In addition, regardless of privacy policies and disclaimers, one respondent said “I do believe google and social media platforms should be more transparent of how much they are collecting to the user. I believe everyone should know that they can literally log on google and navigate to a certain page where it says everything about you (marriage status, interest, income level, etc.).”, and another respondent said the “[government] needs to do more to make companies accountable and protect Canadian citizens.”

Overall, respondents wanted more information and knowledge about privacy and security while operating in online spheres. One respondent exclaimed “this survey is a wake up call to pay more attention to the websites/search engines that I visit. It's a reminder how little I know about online collection of data and personal information”, while another respondent said “the survey showed me how casually I have accepted the invasion of privacy by the big tech companies in exchange for access to their social media platforms. It has made me want to be more informed and vigilant. And [to] take more actions to protect my cyber privacy.”

Qualitative open-ended answers provided evidence for the third and final objective. Most respondents’ comments supported the fact that people need to be more aware of what is being collected about them, showed concerned for their privacy and security, and suggested that laws and regulations regarding online data privacy and security need to be further implemented. Private browsers were offered as recommendations by some respondents, while others, urged the government to make this information more available for those in the dark. A respondent stated:

“This is something that definitely needs to be addressed. All Canadians should have the right to know about that their info is being used and sold.”

As for future implications, 0% of respondents thought nothing should be done and felt like laws regarding privacy and security are currently adequate. In fact, nearly all respondents selected the options for laws to be reexamined, updated, changed and more laws need to implement (see Figure 12). This was also a high touch point in qualitative feedback from respondents. Society and technology are ever evolving, and it is important that they both evolve synonymously. A respond highlighted that it is “important [that] information [is] always updated/reviewed as technology evolves”, another stated that “more information [needs to] be given to the public more regularly about how to combat these privacy moves on a daily usage basis. Governments also need to be more proactive and monitor and oversee the big tech companies with more legislation to protect consumers.”

Some respondents did not think there was a choice in the matter. One respondent explained, “Regarding search engines, I do not think that we have any other option than to accept the consequences that result from using these above-mentioned search engines. But I do think that we need stronger/better aligned laws to protect Canadians.” Thus, Canadian residents feel the need for more stringent protocols regarding their online privacy and security. However, what will this mean for the marketing and business sphere.

As mentioned previously, updating, and changing laws for the benefit of consumers will fundamentally change the way organizations react and engage with their consumers. Some respondents suggested making privacy more profitable, while others want organizations to be held accountable for this invasion. While a majority of respondence share the stance of Canadians needing more protection while operation in online sphere, 52.9% of respondents answered in some way likely, that they would continue using social media platforms after this survey while a higher 75% said they would likely in some form, use search engines and websites after completion of this survey. To speak to this irony, a responded stated, “I am acutely aware of the many infringements on my privacy online, but I also selected that I would continue using these platforms. I can only speak anecdotally, but my mindset around these concerns is quite pessimistic in a "they've already spied on all my data, it's too late to bother leaving these platforms now." Therefore, perhaps Canadians have accepted this way of life as they feel they have no alternative.

Canadians should be allowed to their data and should be allowed to request their data to be eased. Which brings the idea of “right to be forgotten” and the leaning on other countries for successful direction regarding online privacy and security. Respondents also shared their liking of the privacy policies of other nations. One respondent stated, “[personally], I like the idea of GDPR in the EU and it's "right to be forgotten" clause, the problem is I don't see how it could be properly enforced. Following the American hearings against Facebook and other platforms it seemed quite clear that global legislators (Canada included) have a tremendously poor literacy rate when it comes to how these platforms even work. How do you legislate an entire pillar of modern life when you do not even understand how it works? Do I think more needs to be done? Absolutely. Do I know how to do that? Not in the slightest. Do I think Canadian citizens or government understand the degree to which their privacy is being infringed? No...” Therefore, it can be concluded that there is not entirely enough action nor research available to support this sector. Furthermore, that the principles of online data privacy and security should further be studied by individuals, academia, and research, as well as governing bodies.

5.2 Comparing The Results Of A Quantitative Study To A Literature Review

A major overarching hinderance was explored regarding the effectiveness of PIPEDA, CASL, and the digital world: Valid informed consent. With the support of academic literature and the research conducted for this study, it can be concluded that Canadian residents are not aware of how much data is being collected about them. What does this mean? If consumers are ignorant to the methods being used to collect their data and information, how is it possible for them to provide informed consent? Furthermore, in instances of coercion of consent under circumstances of digital undue influence, consent can thus be deemed voidable.

Consequently, if Canadian residents’ data and information is being collected by methods unaware to them, how are they expected to be able to put in place privacy protecting actions, ask to access their collected data, or file a complaint if their collected data and information is used in a way they would not approve of? If consumers are unaware of the methods organizations use to capture their data, then the vary laws put in place to protect them, PIPEDA and CASL, have been circumvented and rendered utterly useless.

The need for fully aggregated compressive protocols regarding cyber security and privacy are imperative. Sandy Parakilas, Former Facebook Operations Manager and Former Uber Product Manager, stresses in an interview on data privacy that he "[thinks] we need to accept that it's okay for companies to be focused on making money. What is not okay is when there is no regulation, no rules, and no competition, and [these] companies are acting as sort of de facto governments..." (Orlowski, 2020). More importantly, highlighting that "we have almost no laws around digital privacy..." (Orlowski, 2020). The main implications for organizations and stakeholders regarding these changes, would mean changing the business and marketing world as we know it, a change for the better of citizens.

5.3 Assessment Of The Results In Light Of literature

Rice and Bogdanov research from their Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices, indicates that "Canadians are ill informed about how companies are collecting and using their personal data, despite the existence of legislation, and despite the existence of, and consent to privacy notices" (Rice & Bogdanov, 2018). Further, Rice and Bogdanov, apotheosize that "the privacy notice is a historical relic that is ill-suited to many of today's data collection realities, and the mere provision of, and consent to a privacy notice does not ensure consumers are informed about data practices" which are requirements of FIPP, PIPEDA and CASL (Rice & Bogdanov, 2018).

As mentioned, research in Canada regarding consumers knowledge on privacy-impacting business practices is limited to four studies:

1. Canadians and Privacy: conducted by Ekos Research Associated Inc. (2009)
2. Canadians on Privacy: conducted by Phoenix Strategic Perspectives Inc. (2018)
3. Canadians on Privacy: conducted by Phoenix Strategic Perspectives Inc. (2016)
4. Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices: conducted by Canadian Journal of Administrative Science (2018)

Similarly, to the existing above literature, the research results of this thesis are indicative to the notion of the ill-informed. Furthermore, summit a call to action for Canadian residents and the

Canadian government. Rice & Bogdanov emphasize that “the call for new methods informing Canadians about how their data are being collected and used by businesses must be devised [and] these new methods must respond to the challenges presented by emerging Technologies” (Rice & Bogdanov, 2018).

5.4 Limitations Of The Research

While this study aims to understand Canadians residents’ knowledge and understanding of data collection practices, it is limited to the fact that the population sample size was too small for statistical validity. For “true” sample size, 10% of the population must be sampled, with a maximum sample size of 1000. With a population of 37.59 million in Canada, it would have been recommended that 1,000 surveys were completed as opposed to 124 completed in this sample. In addition, the proportion and correlation of occupations/industry fields to results could present disproportionate, as there were not even comparative samples sizes for each occupation/industry fields recorded. For example, only one respondent’s industry field was advertising, and this one respondent’s answers may not be an accurate representation of the average opinions of advertising personnel collectively.

Other areas of limitation were sample distribution. Although everyone with a link could complete the survey, tracking entries required a valid Gmail email address, which not everyone has. Therefore, it presented the possibility of completing the survey multiple times. Other limitation of this study includes questions omitted from the survey. Respondents were not asked if they read the privacy policy, and this information could have presented beneficial to results section. However, it can be confidently stated that the other research questions carefully considered and answered the questions of this thesis. The results and findings of this study are reliable but subjective and are limited to the application of this thesis.

Other major limitations were the lack of available academic literature on the subject in Canada. Therefore, data for rigorous research was unavailable. It was extremely benefitable that previously mentioned 3 of 4 works on data privacy in Canada we available through the Government of Canada website services. There was limitation however, in access the empirical study framework and a fee had to be paid to gain access. Nonetheless, the topic of thesis is extremely relevant and has added a new body of work in the available literature of data collection and privacy in Canada.

Additionally, new methods can now be investigated as this thesis provided a literature review on Canadian legislation. With the lack of accessible information on this topic, it was imperative to instead review the current legislations in place that are protecting Canadian residents to offer commentary, critical thinking, and analysis. Although, the structure differed from traditional literature reviews, the information reviewed and analyzed was imperative to this study and to the Canadian landscape of data collection, privacy, and security.

Lastly, as mentioned briefly, this study experienced limitations regarding geographic distribution. Given, the research was conducted in Toronto Ontario, geographic bias may be presented as it can be assumed that a majority of survey respondents live and operate in the Toronto or Greater Toronto Area (GTA). Thus, by having a majority of Toronto GTA respondents, attitudes and opinions of other Canadian residents in other provinces were not recorded proportionately. Perhaps provincial governments have different campaigns in place to educate citizens in other regions. However, these are limitations we bring to light ethnically and voluntarily as there were not questions on the survey requiring respondents to enter their location.

5.5 Recommendations For Future Research

It is simple to conclude Canada is either far behind in adapting to the new data collection era, or perhaps has very different views from the masses regarding the need to protect their citizens. The latter, however, would pose the question: Are they in support of data collection for aiding in making their consumer journeys more customized and simplistic, or against? Future recommendations for research of this topic are worth studying because of the implications it can bring regarding the marketing and business world in Canada. Therefore, this topic is worth studying from all viewpoints: society, industry, and businesses. By providing insight on the current protection or lack thereof of Canadian residents, individuals can learn their liberties—more importantly perhaps investigate ideas they are not currently informed or aware of.

The crucial changes, updates, reexamination, and additional policies needed regarding privacy law in Canada will change the business sphere are we know it. It will shift the economic market and change the way organizations interact and access their consumers. Furthermore, these changes will heavily benefit consumers while seriously weakening incremental dollars for businesses for a

multi-billion-dollar marketplace industry. Despite its harm to organizations, this is a necessary change.

It is important to recognize that this is not to question the importance of technology and technological advancements, but rather to question the business model of organizations that are so financially driven that which is not in the best interest of humans, the psychology of beings, or privacy and security. Harris for example explains how he has been called the closest thing Silicon Valley has to a “conscience”; but “What of the industry now?... [I am simply] asking tech to bring “ethical design” to its products” (Orlowski, 2020).

There are two alternative solutions to the crisis of privacy and security that this thesis recommends and will explore.

1. The Private Technology Industry
2. Technological empowerment applications for users

Other suggestions for solutions to current issues are private browsers. Qwant Brower’s is known as the browser engine that respects your privacy. Another option for internet users is NordVPN, which is a virtual private network service provider. If policy and law are not changed to reflect the current issues faced, will private browsing become more prominent in society? Additionally, will networks begin to offer privacy options within these platforms themselves for an additional fee? This thesis began with the idea that privacy is the most sought out commodity in a modern age where it seems your privacy is for sale. Perhaps there is a need for further research and resources for the development of a new sector of more private Technologies and The Internet of Things. Perhaps as mentioned, making privacy more profitable.

Other option are Internet program extensions or applications offered by companies like the UK’s Gener8 Inc., Job Search Television Network, Inc. (Digi.me application), and the American company, Brave. These organizations offer browser extensions and applications that allow users to earn money for the data that is being collected. This provides an alternative to users strictly selling their data solely to gain access to a website or information. Moreover, it provides potential for users to gain value in the data collected about them by placing a portion of that value back into the user’s hands. If companies and organizations are making millions off the data they collect on you, instead

of safeguarding your privacy, you can “sell it” but for a returned value. “Control and be rewarded from your own data” (Gener8, 2021).

These extensions offer various points systems that can be changed into products, dollars, or crypto currencies. Ultimately, it provides an empowerment friendly option that allows consumer to get more out of the data collection process and what is being traded for a share of some of the profits that exist because of them. These platforms offer options for a different narrative and presents a story for additional user empowerment and value.

Although increasing private technologies offered in the industry and the use and emergence of technological empowerment models and applications are a great solution to tackle the privacy and security crisis at hand, many other issues emerge with these alternative methods. The main one being ethicality. Private technologies or privacy options offered on current technologies for example presents privacy as a commodity. Moreover, by creating technologies that offer means to protect your data through additional fees, creates the unethical principle of why people should have to pay to protect their own information. Additionally, paying for private browsing may be an option many can use right now to safeguard some people’s lives and privacy, but what can be said about the wealth gap it will create: if those who seek privacy cannot afford privacy options.

Although none of these above-mentioned alternatives are complete or permanent solutions to the issues faced, they are potential solutions based on the current knowledge we have regarding the crisis of privacy until we can find more sustainable and ethical solutions. Thus, it brings us back to government action and intervention as the best long-term course of action.

In 1995, the EU implemented its EU Data Protection Directive which served as the data protection standard among the various EU Member States. However, its implementation was not deemed satisfactory, and to improve the situation, the General Data Protection Regulation was adopted (Voigt & Von dem Bussche, 2017). These regulations have a transcontinental application and provide various new or reinforced data protection obligations that require all data controllers and processors of information to “implement technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services” (EU General Data Protection Regulation (GDPR), third edition, 2019).

The EU's take on data privacy and security serves as importance as there is no need completely reinvent the wheel, but rather adopt to current already active and successful frameworks in other global industries. It is recommended for the Canadian government to further research data privacy laws in national whose citizens feel protected, the EU in particular.

Lastly, it would be beneficial to conduct further qualitative research regarding Canadians and their knowledge of privacy. Qualitative research provides a new perspective and a more conscious and reflective choice regarding results. It had been noted earlier that a high percentage of people do not read privacy notices or policies when given. Perhaps this presents a digital gaze in which people do not fully read and comprehend vast amounts of information given in digital forms. Thus, perhaps respondents presented that same occurrence when presented survey questions in an online format. Therefore, it is suggested that a focus group would be recommended further test these findings and to gain more understanding of where Canadian residents thoughts, opinions and attitudes stand regarding this topic.

Nevertheless, Canadian residents and the respondents of this study want 3 things:

- More clear information on what data collection is being conducted – more resources.
- For companies to have more liability and regard concerning their data collection practices.
- More stringent protocol and current protocols to be updated and reexamined.

Further, that with the combination of all three, Canadian residents will not only be more informed of the implications of operating in the online sphere, but it will also serve as an aid in in the protection of those who are in fact ill-informed. Personal data and information can and should only be used for the purposes that which it was collected. If organizations are using the data collect for other intended purpose, they must obtain consent again and further, state this in a method that is clear and not easily dismissed. Personal data must be protected by enforcing appropriate safeguards. Although knowledge is power, a lack thereof should not equate to complete and utter personal invasion through societies technological tools.

References

Affairs, O. (2021). Canada's Anti-Spam Legislation.
https://fightspam.gc.ca/eic/site/030.nsf/eng/home

Branch, A. (2021). Horizontal Evaluation of Canada's Anti-Spam Legislation (CASL) - Audits and evaluations.
https://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/h_03875.html

Brannen, J. (1992). *Mixing Methods: Qualitative and Quantitative Research* (*1st ed.).* London: Routledge.
https://doi.org/10.4324/9781315248813

Business Insider. (2021). You're not alone, no one reads terms of service agreements.
https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11

Canada House of Commons. (2017). Canada's Anti-Spam Legislation. Ottawa.
https://www.ourcommons.ca/Content/Committee/421/INDU/Reports/RP9330839/inDurp10/indurp10-e.pdf

Canada's National Observer. (2021). Class-action lawsuit alleges Google has turned Canadians' electronics into tracking devices.
https://www.nationalobserver.com/2020/09/08/news/class-action-lawsuit-alleges-google-has-turned-canadians-electronics-tracking

Castells, M. (1997). *An introduction to the information age*. City, *2*(7), 6-16.
https://doi.org/10.1080/13604819708900050

Castells, M. (2012). *The rise of the network society*. Malden, Mass.: Wiley-Blackwell.

Coos, A. (2019, September 6). PIPEDA vs. GDPR: The Key Differences *EndPoint Protector*.
https://www.endpointprotector.com/blog/pipeda-vs-gdpr-the-key-differences/

Deep, R. (2006). *Probability and statistics.* Burlington (Mass.): Academic Press.

Denzin, N., & Lincoln, Y. (2013*). Strategies of qualitative inquiry (3rd ed*.). Thousand Oaks, CA: SAGE.

Ekos Research Associates Inc. (2009). Public opinion survey. Ottawa: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2009/ekos_2009_01/

Eysenbach, G. (2011). Infodemiology and Infoveillance. *American Journal Of Preventive Medicine*, 40(5), S154-S158. doi: 10.1016/j.amepre.2011.02.006

Facebook. (2021). Data Policy. https://en-gb.facebook.com/policy.php

Gener8. (2021) https://gener8ads.com/

Global News. (2021). Failure to report Canadian privacy breaches could mean big fines after Nov. 1. https://globalnews.ca/news/4619728/failure-to-report-canadian-privacy-breaches-could-mean-big-fines-after-nov-1/

Government of Canada. (2021). Enforcing Canada's Anti-Spam Legislation (CASL). https://crtc.gc.ca/eng/internet/pub/20200930.htm

IT Governance Ltd. (2019). *EU General Data Protection Regulation (GDPR)*, (*3rd ed*.). United Kingdom.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, *10*(1). https://doi.org/10.5817/CP2016-1-2

Kissell, J. (2021) Joe On Tech. http://joeontech.net/what-is-technology-anyway.html

Morgan, J. (2021). A Simple Explanation Of 'The Internet Of Things'. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=4a3e77791d09

Mulligan, D. K., & King, J. (2012). Bridging the gap between privacy and design. *Journal of Constitutional Law*, *14*(4), 989–1034.

Office of the Privacy Commissioner of Canada. (2000). *Personal Information Protection and Electronic Documents Act*. Ottawa.

Office of the Privacy Commissioner of Canada. (2010). *Canadian Anti-Spam Legislation*. Ottawa.

Office of the Privacy Commissioner of Canada. (2011). Cookies. Ottawa: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/cookies/02_05_d_49/

Office of the Privacy Commissioner of Canada. (2021). The Personal Information Protection and Electronic Documents Act (PIPEDA). Ottawa. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Orlowski, J. (2020). *The Social Dilemma* [DVD]. United States: Netflix.

Park, Y., & Mo Jang, S. (2014). *Understanding privacy knowledge and skill in mobile communication. Computers In Human Behavior*, *38*, 296-303. https://doi.org/10.1016/j.chb.2014.05.041

Pew Research Center. (2014). Public perceptions of privacy and security in the post-Snowden era. https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Phoenix Strategic Perspectives Inc. (2016). Public opinion survey. Ottawa: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

Privacy and Anti-Spam Laws. (2021). https://www.fasken.com/en/knowledge/doing-business-canada/2019/06/privacy-anti-spam-laws/

Quartile Definition. (2021). https://www.investopedia.com/terms/q/quartile.asp#:~:text=Key%20Takeaways-,The%20quartile%20measures%20the%20spread%20of%20values%20above%20and%20below,four%20groups%20of%20the%20dataset.

Rice, M., & Bogdanov, E. (2018). Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices. *Canadian Journal Of Administrative Sciences / Revue Canadienne Des Sciences De L'administration, 36*(2), 163-176. https://doi.org/10.1002/cjas.1494

Ritchie, J., Lewis, J., McNaughton Nicholls, C., & Ormston, R. (2014). *Qualitative Research Practice* (*2nd ed*.). London: SAGE Publications Ltd.

Roberts., S. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. United States of America: Yale University Press.

Saunders, M., Lewis, P. and Thornhill, A. 2009. *Research Methods for Business Students. 5th edition*. Harlow: Prentice Hall.

Sophocles. (1000). *Antigone*. Play, Athens.

Statista. (2021). Number of internet users in Canada 2019. https://www.statista.com/statistics/243808/number-of-internet-users-in-canada/#:~:text=Canada%3A%20number%20of%20internet%20users%202000%2D2019&text=In%202019%2C%20Canada%20had%20an,96%20percent%20of%20the%20population

Statistic Solutions. (2021). https://www.statisticssolutions.com/survey-scales/

Statistics: Power from Data! Range and quartiles. (2021). https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch12/5214890-eng.htm

The Ins and Outs of Wearable Technology. (2021). https://www.investopedia.com/terms/w/wearable-technology.asp

Unilever. (2021). Privacy Notice [Image]. https://www.unilever.ca/

Vaynerchuk, G. (2011). The Thank You Economy. [Maumee, Ohio]: Dreamscape Media, LLC.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). AG: Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7_1

What are Cookies?. (2021). https://www.kaspersky.com/resource-center/definitions/cookies

Why Survey Research and Survey Methodology Matter. (2021). https://www.surveymonkey.com/mp/why-survey-understanding-survey-methodology/#:~:text=Surveys%20can%20help%20gauge%20the,used%20to%20make%20important%20decisions.

Zwilling J.A. Henckels Ltd. (2021). This website uses cookies [Image]. Retrieved from https://www.zwilling.com/ca/

Appendices

Appendix 1. Key Terms

Infodemiology and infoveillance: “framework for an emerging set of public health informatics methods to analyze search, communication and publication behaviour on the Internet”.

“Infodemiology data (derived from unstructured, textual, openly accessible information produced and consumed by the public on the Internet, such as blogs, websites, and query and navigation data) can be collected and analyzed in near real-time. We developed a proof-of-concept infoveillance system called Infovigil, which can identify, archive, and analyze health-related information from Twitter and other information streams from Internet and social media sources. The system was developed to demonstrate and explore the potential of infoveillance for measuring public attention, attitudes, behavior, knowledge, and information consumption, as well as for syndromic surveillance, health communication, and knowledge translation research”.

Source: Eysenbach, G. (2011).

Cookies: “Cookies are text files with small pieces of data that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience. Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you”.

Source: What are Cookies?. (2021).

Magic cookies: “Magic cookies are an old computing term that refers to packets of information that are sent and received without changes. Commonly, this would be used for a login to computer database systems, such as a business internal network. This concept predates the modern “cookie” we use today”.

HTTP cookies: "HTTP cookies are a repurposed version of the “magic cookie” built for internet browsing. Web browser programmer Lou Montulli used the “magic cookie” as inspiration in 1994. He recreated this concept for browsers when he helped an online shopping store fix their overloaded servers. The HTTP cookie is what we currently use to manage our online experiences. It is also what some malicious people can use to spy on your online activity and steal your personal info”.

Source: What are Cookies?. (2021).

Third Party Cookies: “Third-party cookies are created by domains that are not the website (or domain) that you are visiting. These cookies are usually used for online-advertising purposes and placed on a website through adding scripts or tags”.

Source: What are Cookies?. (2021).

Privacy Notice: “The privacy notice is a statement or document disclosing a company’s data-related practices. Consumers are invited to read the privacy notice and must usually consent to the terms of data collection and use it contains before using the company’ s service”.

Source: Government of Canada. (2021).

Internet of Things: “Related to any device with an on and off switch to the Internet and/or to each other. This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and other digital technologies”.

Source: Morgan, J. (2021).

Office of the Privacy Commissioner of Canada: “Office of the Privacy Commissioner of Canada provides support and information in regard to the protecting of personal information. They are responsible for enforcing the Federal privacy laws in Canada”.

Source: Office of the Privacy Commissioner of Canada. (2021).

Canadian Radio-television and Telecommunications Commission (CRTC): “The CRTC is the Administrative Tribunal that governs broadcasting and telecommunication in Canada for public interest.

Source: Source: ("Privacy and Anti-Spam Laws", 2021)

Federal Competition Bureau: “The Competition Bureau is the independent agency that is responsible for ensuring that markets operate in the correct manner. The Bureau is responsible for enforcing the Competition Act, The Consumer Packing and Labelling Act and the Precious Metals Marking Act”.

Source: ("Privacy and Anti-Spam Laws", 2021)

Commercial Electronic Messages: “A CEM is defined broadly in CASL as an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity”.

Source: ("Privacy and Anti-Spam Laws", 2021)

Express consent: “A person who seeks express consent for the doing of an act described in any of sections 6 to 8 must, when requesting consent, set out clearly and simply the following information:

- the purpose or purposes for which the consent is being sought.
- prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies that other person.
- any other prescribed information (Canadian Anti-Spam Legislation, 2010).

Source: Office of the Privacy Commissioner of Canada. Personal Information Protection and Electronic Documents Act (2000)”.

Personal Information Protection and Electronic Documents Act (PIPEDA): “A Canadian law that governs how private sector organizations collect, use a disclose person information and data for the course of commercial business”.

Source: Office of the Privacy Commissioner of Canada. Personal Information Protection and Electronic Documents Act (2000).

Canadian Anti-Spam Legislation (CASL): “CASL is a Canadian federal law that deals with spam and other electronic threats. This legislation was implemented as a means to protect Canadians while ensuring that businesses can continue to compete in the global marketplace”.

Source: Office of the Privacy Commissioner of Canada. Canadian Anti-Spam Legislation (2010). Ottawa.

Technologies: “Machinery and equipment developed from the application of scientific knowledge”

Source: Kissel, J. (2021).

Wearable Technologies: ”Also known as "wearables", is a category of electronic devices that can be worn as accessories, embedded in clothing, implanted in the user's body, or even tattooed on the skin and are usually able to access the Internet in some capacity”.

Source: The Ins and Outs of Wearable Technology. (2021).

Appendix 2. Survey Questions

1. This survey is intended for Canadian Residents only. Please confirm that you are a Resident of Canada.

2. What is your age?

3. What is your gender?

4. Which of the following best describes your current occupation?

5. Are you familiar with **Canadian Anti-Spam Legislation** (CASL)?

6. On a scale of 1-10, how familiar are you with CASL and your protection as a Canadian Resident?

7. Are you familiar with the **Personal Information Protection and Electronic Documents Act** (PIPEDA)?

8. On a scale of 1-10, how familiar are you with (PIPEDA) and your protection as a Canadian Resident?

9. Do you use Facebook?

10. Which of the following social networking platforms do you currently have an account with? (Check all that apply)

11. Are you aware that your data is being tracked and stored by these platforms (Social Media)?

12. Do you wish to know more about what is being tracked and what this means for your privacy and security?

13. Facebook in particular, uses different types of tracking software's to follow consumers' activities. This also includes millions of non-Facebook sites all over the web. These tracking tools collect data such as: age, gender, interests, addresses, biometric facial data etc. without users' explicit "opt-in" consent. **Are you aware social media platforms along wit many other website, track and collect your data?**

14. Did you know that many social media sites/applications not only track their platform, but also track you to other sites, other applications on your phone, and other physical locations you have visited in real life?

15. Did you know that your data is being used for variety of marketing tactics such as targeted advertising, creating sales leads, content promotion etc. (Social Media)?

16. Did you know that the Facebook Pixel enables websites and online retailers to gain information about their visitors as the social network analyzes aggregated user behaviour?

17. Did you know that social media sites collect, store, mine, and trade your data including trading with overseas and third-party companies?

18. After answering the previous questions, how likely are you to continue using Facebook and other social media platforms?

19. What is your primary search engine?

20. Are you aware that your data is being tracked and stored by these platforms (Search Engines)?

21. You are most tracked online by your IP address and email. Every site you visit, tracks your time spent, and leaves "cookies." Did you know that these "cookies" remain on your computer and assist companies and organizations in determining how to engage with you, which products will attract your attention, and which will most likely convert to a sale?

22. Do you clear your search history or computer "cookies"?

23. How often do you clear your computer search history and "cookies"

24. Are you aware that Google is currently in a proposed class action lawsuit in the Supreme Court of British Columbia for allegedly collecting and profiting from Canadians personal information collected without explicit consent?

25. Are you aware that Search Engines and other websites collect information about site users to monitor their online behaviour?

26. Did you know that your data is being used for variety of marketing tactics such as targeted advertising, creating sales leads, content promotion etc. (Search Engines)?

27. Are you aware that website can collect the following data? **~IP address to determine a user's location. ~Information about how the user interacts with websites.** (For example, what they click on and how long they spend on a page) **~Information about browsers and the device the user accesses the site with ~Browsing activity across different sites.** (For example: information insight about the individual user's interests, shopping habits, problems they are facing, etc.)

28. Did you know that Search Engines collect, store, mine, and trade your data with third-party companies?

29. After reading the above, how likely are you to continue using Search Engines?

30. After reading the above, are you more likely to clear your search history and internet "cookies"?

31. After completing this survey, how concerned are you about your privacy and security online?

32. Do you believe there is a need for more stringent protocols and regulations in Canada regarding online privacy and security?

33. What do you believe needs to happen to better protect your personal information? (check all that apply) I believe Canadian data privacy and security laws need to be:

34. Any further comments, thoughts, feelings, or concerns regarding the privacy and security of Canadians and their online data, please share below:

35. Any further comments and thoughts regarding this survey, please share below:

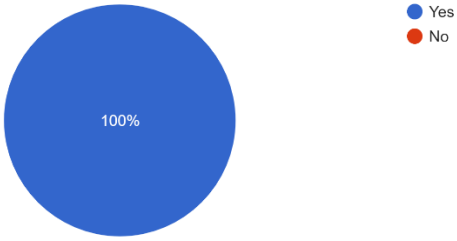
Survey Link:

https://docs.google.com/forms/u/2/d/1DD6ifRRXKH6SJLdZlpslgcBaPjHEpqffE_59cfs4zIw/edit?usp=forms_home&ths=true

Appendix 3. Survey Answers

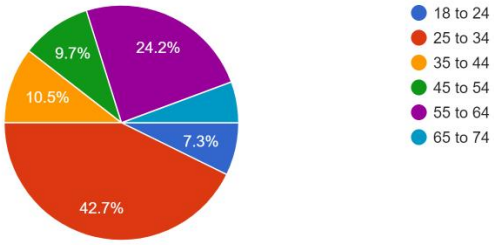
This survey is intended for Canadian Residents only. Please confirm that you are a Resident of Canada.

124 responses



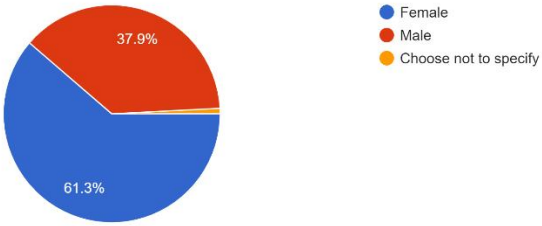
What is your age?

124 responses



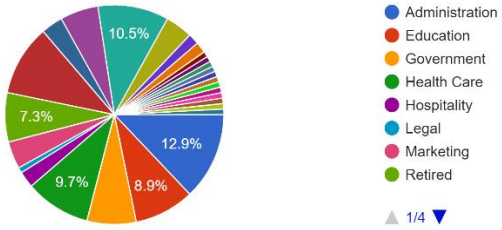
What is your gender?

124 responses



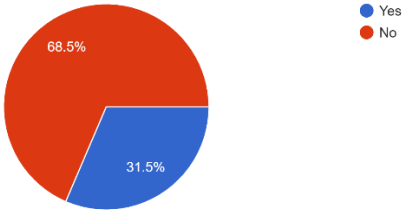
Which of the following best describes your current occupation?

124 responses



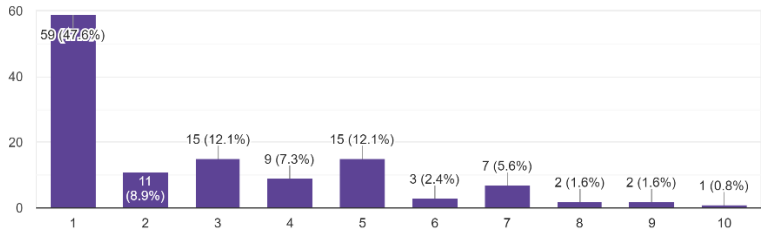
Are you familiar with **Canadian Anti-Spam Legislation** (CASTL)?

124 responses



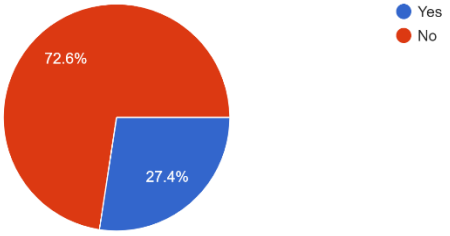
On a scale of 1-10, how familiar are you with CASTL and your protection as a Canadian Resident?

124 responses



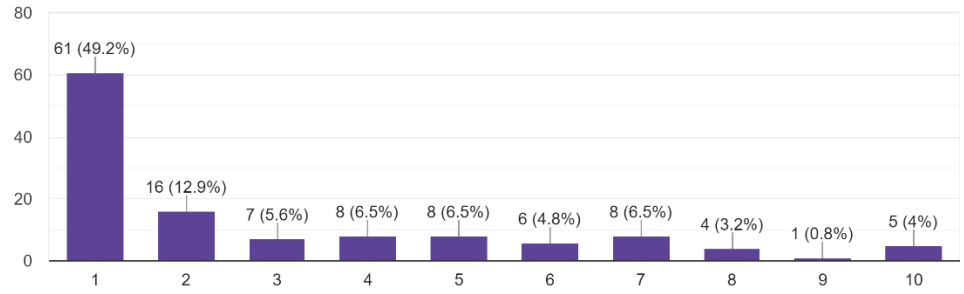
Are you familiar with the **Personal Information Protection and Electronic Documents Act** (PIPEDA)?

124 responses



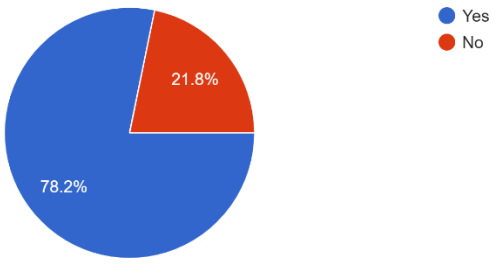
On a scale of 1-10, how familiar are you with (PIPEDA) and your protection as a Canadian Resident?

124 responses



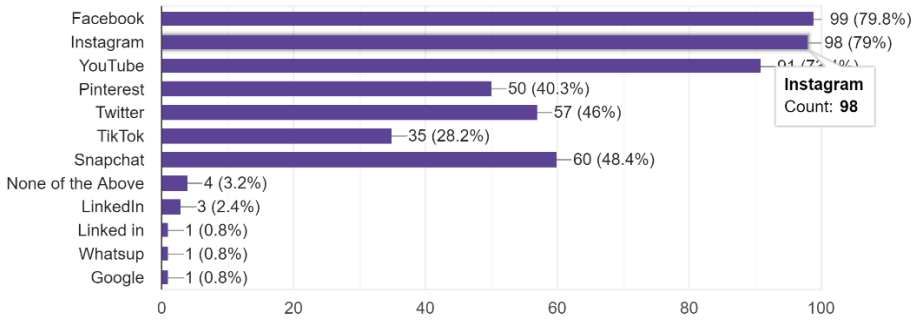
Do you use Facebook?

124 responses

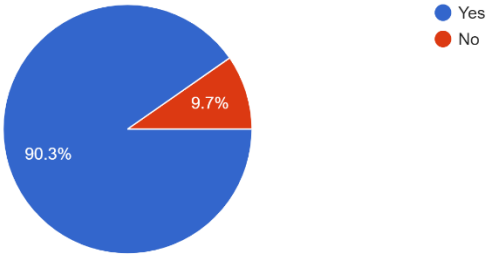


Which of the following social networking platforms do you currently have an account with? (Check all that apply)

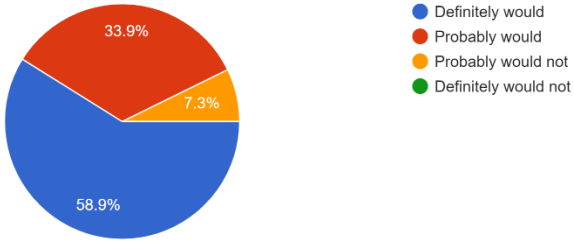
124 responses



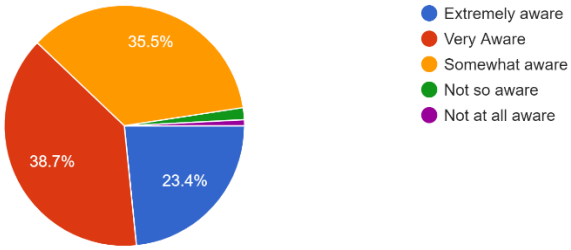
Are you aware that your data is being tracked and stored by these platforms (Social Media)?
124 responses



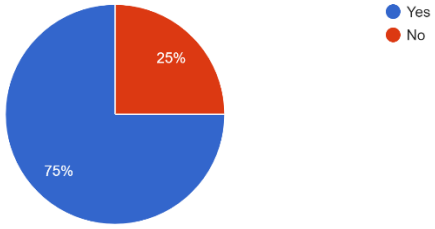
Do you wish to know more about what is being tracked and what this means for your privacy and security?
124 responses



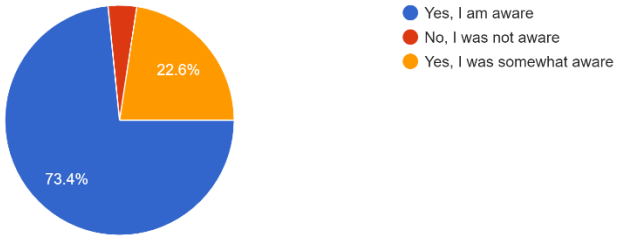
Facebook in particular, uses different types of tracking software's to follow consumers' activities. This also includes millions of non-Facebook sites all over the w...**sites, track and collect your data**?
124 responses



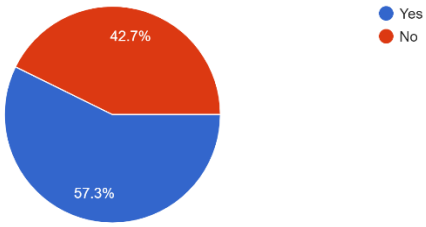
Did you know that many social media sites/applications not only track their platform, but also track you to other sites, other applications on your phone,...er physical locations you have visited in real life?
124 responses



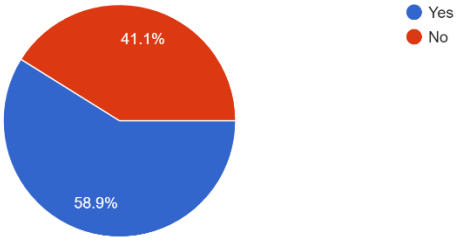
Did you know that your data is being used for variety of marketing tactics such as targeted advertising, creating sales leads, content promotion etc. (Social Media)?
124 responses



Did you know that the Facebook Pixel enables websites and online retailers to gain information about their visitors as the social network analyzes aggregated user behaviour?
124 responses

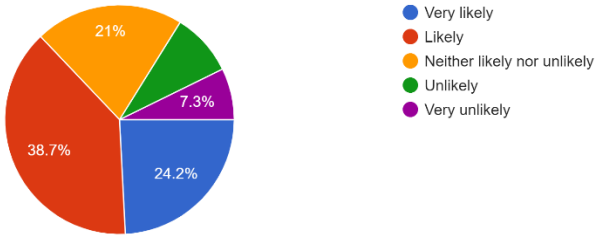


Did you know that social media sites collect, store, mine, and trade your data including trading with overseas and third-party companies?
124 responses



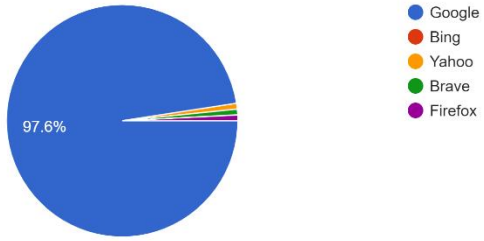
After answering the previous questions, how likely are you to continue using Facebook and other social media platforms?

124 responses



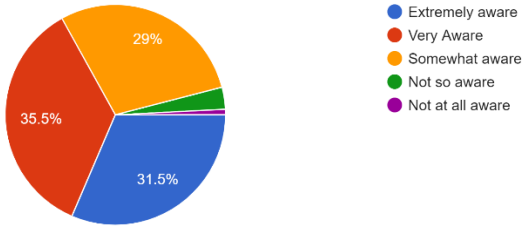
What is your primary search engine?

124 responses



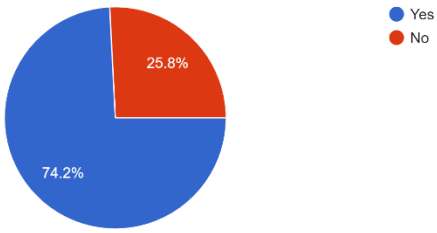
Are you aware that your data is being tracked and stored by these platforms (Search Engines)?

124 responses

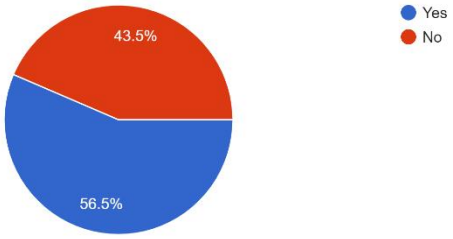


You are most tracked online by your IP address and email. Every site you visit, tracks your time spent, and leaves “cookies.” Did you know that thes...tion, and which will most likely convert to a sale?

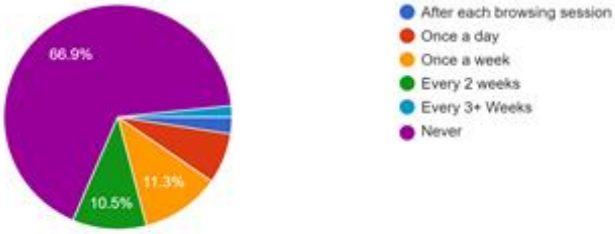
124 responses



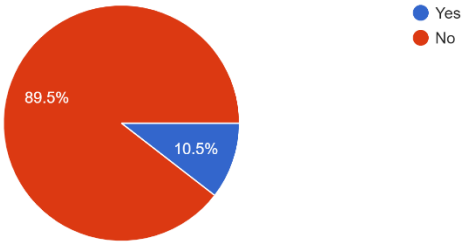
Do you clear your search history or computer “cookies”?
124 responses



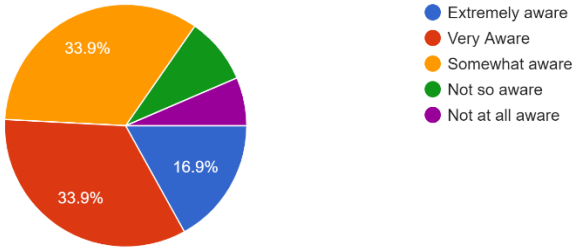
How often do you clear your computer search history and “cookies”
124 responses



Are you aware that Google is currently in a proposed class action lawsuit in the Supreme Court of British Columbia for allegedly collecting and profi...nal information collected without explicit consent?
124 responses

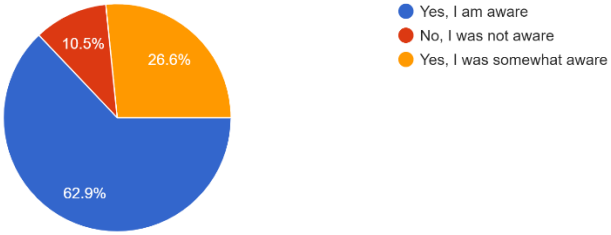


Are you aware that Search Engines and other websites collect information about site users to monitor their online behaviour?
124 responses



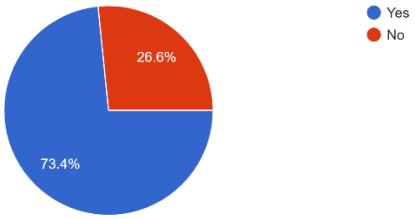
Did you know that your data is being used for variety of marketing tactics such as targeted advertising, creating sales leads, content promotion etc. (Search Engines)?

124 responses



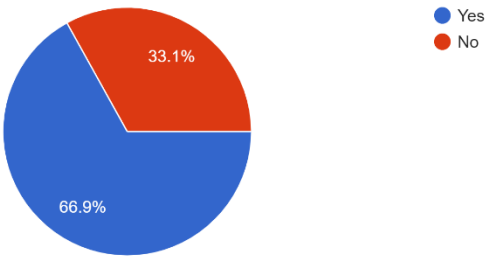
Are you aware that website can collect the following data? ~**IP addresses to determine a user's location**. ~**Information about how th**...er's interests, shopping habits, problems they are facing, etc.)

124 responses



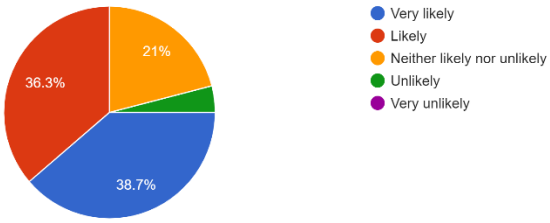
Did you know that Search Engines collect, store, mine, and trade your data with third-party companies?

124 responses



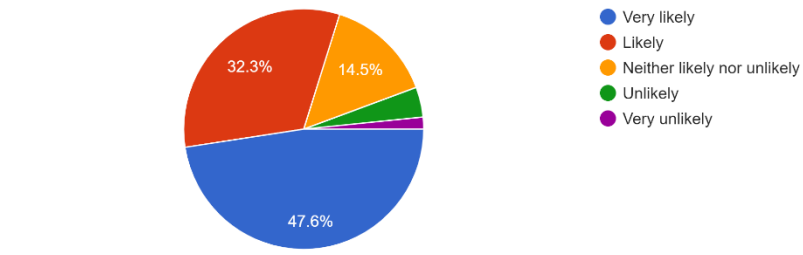
After reading the above, how likely are you to continue using Search Engines?

124 responses



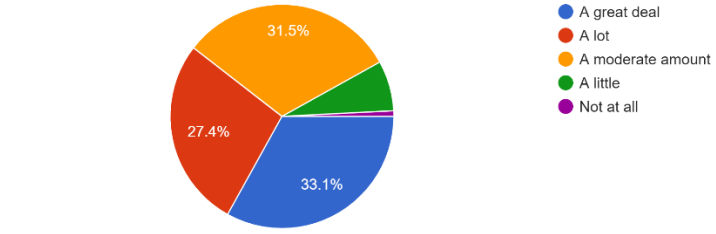
After reading the above, are you more likely to clear your search history and internet “cookies”?

124 responses



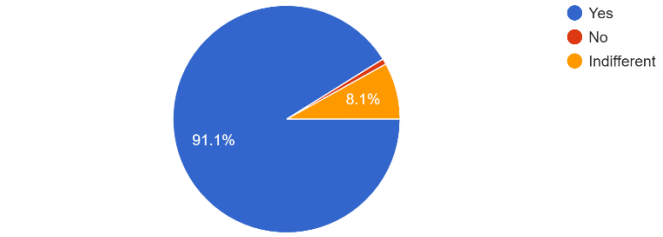
After completing this survey, how concerned are you about your privacy and security online?

124 responses



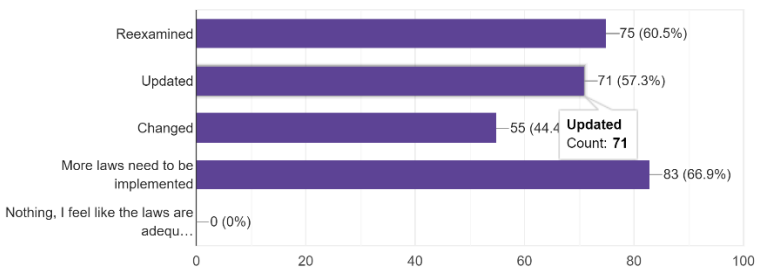
Do you believe there is a need for more stringent protocols and regulations in Canada regarding online privacy and security?

124 responses



What do you believe needs to happen to better protect your personal information? (check all that apply) I believe Canadian data privacy and security laws need to be:

124 responses



Appendix 4. Survey Policy & Disclaimer

The Privacy and Security of Canadian Residents Online Survey Policy and Disclaimer

The purpose of this research project is to investigate Canadian Residents opinions and attitudes on data collection, privacy, and security online. This is a research project being conducted by Evelyn Wiltshire at JAMK University. You are invited to participate in this research project because you are a Canadian Resident. Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. If you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalized.

The procedure involves completing an online survey that will take approximately 10 minutes. Your responses will be confidential, and we do not collect identifying information such as your name, email address or IP address. The survey questions will be about Canadian Resident's knowledge of online data collection.

We will do our best to keep your information confidential. All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you. The results of this study will be used for scholarly purposes only and may be shared with JAMK University representatives.

If you have any questions about this research study, please contact Evelyn Wiltshire at cwiltresearch@gmail.com or JAMK University located at Rajakatu 35, 40200 Jyväskylä, Finland. This research has been reviewed according to JAMK University procedures for research involving human subjects.

ELECTRONIC CONSENT: Please select your choice below.

Clicking on the "consent" option below indicates that:
• you have read the above information
• you voluntarily agree to participate
• you are at least 18 years of age
If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

Appendix 5. Explicit Consent

ELECTRONIC CONSENT: Please select your choice below.

- I consent to this survey
- I do not consent (disagree)

Figure 20 — Explicit Survery Consent