Canadian Journal of Administrative Sciences
Revue canadienne des sciences de l'administration
36: 163–176 (2019)
Published online 7 May 2018 in Wiley Online Library (wileyonlinelibrary.com) **DOI**: 10.1002/CJAS.1494

Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices

Marshall David Rice*
York University

Ekaterina Bogdanov
York University

Abstract
We investigate Canadians' level of awareness of the ways in which businesses collect and use their data via existing and emerging technologies, including facial and voice recognition, mobile location tracking and the Internet of Things. In a survey of 1,005 Canadians, we found that many respondents are ill informed about how their data are being collected and used. Such low awareness of data practices is partially explained by the shortcomings of the "privacy notice." We suggest 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. Copyright © 2018 ASAC. Published by John Wiley & Sons, Ltd.

Keywords: privacy, Internet of Things, data collection, emerging technologies, privacy notice

Résumé
Dans cet article, nous examinons le niveau de sensibilisation des Canadiens aux façons dont les entreprises recueillent et utilisent leurs données au moyen des technologies existantes et émergentes telles que la reconnaissance faciale et vocale, la localisation mobile et l'Internet des objets. Dans un sondage mené auprès de 1 005 Canadiens, nous constatons que de nombreux répondants sont mal informés sur la façon dont leurs données sont recueillies et utilisées. Cette faible sensibilisation aux pratiques en matière de données s'explique en partie par les manquements inhérents à l' "avis de confidentialité". Nous suggérons de poursuivre la recherche sur d'autres méthodes afin d'informer les Canadiens sur les pratiques en matière de données d'entreprise et pour aider les particuliers à mieux contrôler leurs données privées dans un monde de plus en plus branché et mobile. Copyright © 2018 ASAC. Published by John Wiley & Sons, Ltd.

Mots-clés: vie privée, Internet des objets, collecte de données, technologies émergentes, avis de confidentialité.

Introduction

Companies today are collecting data in ways that would have been unimaginable just a few years ago. In addition to the well-established practice of tracking a person's web browsing behaviours, newer methods, including facial and voice recognition, location tracking via GPS, beacons, or Wi-Fi ping, and emotional recognition, are increasingly being utilized. The number of data collection points has also increased with the proliferation of smartphones, wearable devices, and the emerging Internet of Things.

Despite the changes in the technological landscape, the regulatory landscape has largely remained the same since the 1970s. For almost 50 years, consumer privacy worldwide has been governed by a framework called Fair Information Practice Principles (FIPPs) (Bruening & Culnan, 2016). The underlying goal of FIPPs is to oblige businesses to disclose enough information about their data practices to allow consumers to make informed decisions. This approach precipitated research into consumers' knowledge of how businesses' data practices impact individuals' privacy. Primarily, such research looked at consumer knowledge of legal limits on data collection by businesses (Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009; Park, 2013). Limited research also explored Americans' objective knowledge of some privacy-impacting corporate data practices related

We thank Ann Cavoukian, Distinguished Expert-in-Residence, Privacy by Design Centre of Excellence at Ryerson University for her thoughts and direction. We also acknowledge financial support from the Osgoode@50 Fund at York University.
*Please address correspondence to: Marshall David Rice, Associate Professor, Schulich School of Business, York University, 4700 Keele Street, Toronto, Ontario, Canada, M3J 1P3. Email: mdrice@schulich.yorku.ca

to, primarily, Internet use (Turow, Feldman, & Meltzer, 2005; Park & Jang, 2014). Our research builds on these findings by focusing specifically on Canadian consumers and exploring their awareness of data practices related both to established and emergent technologies. Our findings are based on a survey of a representative sample of 1,005 Canadian Internet users, who were asked true or false questions about corporate data collection practices.

This paper begins by describing the FIPPs framework of privacy regulation that has informed industry approaches to protecting privacy, as well as the role of consumer knowledge and the privacy notice in this framework. Next, the paper reviews existing research into the two areas of consumer knowledge described above. We then present our findings, discuss their implications on Canadians' privacy, and suggest research into several novel approaches to enhance Canadians' knowledge of corporate data practices.

The FIPPs Privacy Governance Framework

Past research on how informed consumers are about businesses' data practices has been largely influenced by the privacy governance framework prevailing worldwide, FIPPs. The goal of FIPPs-based regulation is to give consumers control over their privacy by providing them with the privacy protections and disclosures they need to make informed decisions.

FIPPs were initially proposed in 1973 by the United States Secretary's Advisory Committee on Automated Personal Data Systems in response to the growing use of automated data systems containing information about individuals (US Department of Health, Education, and Welfare, 1973). The FIPPs model of privacy regulation rests on a theory of informational self-determination, which is the idea that an individual ought to have control over his or her information (Mulligan & King, 2012). This broad mandate of providing individuals with control includes five areas of data privacy. First, companies must disclose their data practices to individuals. Second, consumers must provide their consent to data use and collection. Third, individuals should be able to view their data and correct it if needed. Fourth, organizations should protect the integrity and security of private data. Fifth, 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 10 principles that underpin the Canadian national privacy law known as PIPEDA (the Personal Information Protection and Electronic Documents Act), enacted in 2000. The 10 principles on which PIPEDA is based are:

1. Accountability: an organization is accountable for personal information.
2. Identifying Purposes: the purpose of data collection is to be disclosed before collection occurs.
3. Consent: knowledge and consent of the individual are required.
4. Limiting Collection: information is to be collected by fair and lawful means and to be limited to what is required for the identified purpose.
5. Limiting Use, Disclosure, and Retention: no purpose other than the one identified can be pursued, except with the individual's consent.
6. Accuracy: information is to be accurate, complete and up to date for its purpose.
7. Safeguards: information is to be protected by security safeguards.
8. Openness: information about organizational policies and practices with respect to data is to be made readily available.
9. Individual Access: upon request, an individual is to be informed of the existence, use, and disclosure of his or her information and to be given access to it.
10. Challenging Compliance: an individual is to be able to challenge a practice with a designated person at an organization (Office of the Privacy Commissioner of Canada, 2011).

Consumers' knowledge of when their data are being collected and how it is being used is central to the effective administration of the above principles. An individual who is unaware that his or her data are being collected is unable to consent to the collection, approve the purpose of collection, access data to verify its integrity, or challenge corporate compliance with PIPEDA. In addition, a company that engages in undisclosed practices has less incentive to comply with PIPEDA principles because undisclosed practices cannot be challenged. As a result, the above principles require fairly comprehensive disclosure of data collection and use practices by businesses.

The Role of the Privacy Notice in FIPPs-based Privacy Governance Frameworks

FIPPs do not significantly restrict the means of corporate collection and the use of consumer data. In a FIPPs-based privacy governance framework, corporations can collect and use most consumer data in almost any way, as long as the consumer provides informed consent to such collection and use. In order to obtain what corporations present as informed consumer consent to data practices and comply with FIPPs, corporations developed the 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. Since the advent of FIPPs, the privacy notice has served as the key mechanism by which companies provide consumers with information and obtain their consent (Bruening & Culnan, 2016). Corporations generally propose, and regulators generally agree, that if information about corporate data practices is contained in a privacy notice with which the consumer agrees, then the

Can J Adm Sci
36(2), 163–176 (2019)

consumer has provided informed consent to data practices and the corporation is in compliance with FIPPs.

Consumer Knowledge of Legal Limits on Business Data Practices

The emphasis FIPPs places on ensuring that consumers' privacy decisions are informed and the centrality of consumer knowledge of data practices to the effective administration of FIPPs has stimulated academic research into consumers' awareness and understanding of how their data are collected, used and protected.

Broadly, research suggests that consumers believe that the law protects their privacy more than it actually does. Turow has conducted significant research on the topic of consumer knowledge of legal privacy protections. In 2005, Turow Feldman, and Meltzer surveyed 1,500 Americans and asked them true or false questions about the legal rules surrounding companies that collect, share, and sell private consumer data. He found that, for example, 71% of respondents incorrectly believed that a video store is not allowed to sell information about the titles an individual rents. Similarly, 73% of respondents in the same study incorrectly believed that when they give personal information to a bank, privacy laws stipulate that the bank has no right to share this information, even with companies the bank owns (in a 2016 survey by Kezer, Sevi, Cemalcilar, and Baruh, which asked the same question, 40% responded incorrectly). In 2007, Turow, Hoofnagle, Mulligan, Good, and Grossklags reported that The Golden Bear telephone survey conducted in the same year found that 77% did not know the right answer (false) when asked, "if a Website has a privacy policy, it means that you have the right to require the company to delete your personal information upon your request." Another study by Turow, King, Hoofnagle, Bleakley, and Hennessy (2009), conducted in a similar true or false format, found that respondents correctly answered only 1.5 of five questions about online privacy laws, and 1.7 of four questions about offline privacy laws, "because they falsely assume government regulations prohibit the sale of data." A 2010 study by Hoofnagle, King, Li, and Turow highlighted that lack of knowledge of legal limits is especially pronounced among persons aged between 18 and 24. When asked true or false questions about whether certain privacy-impacting data practices are limited by law, 88% of young adults answered two or fewer correctly, while 42% answered no questions correctly.

More recently, additional research was conducted by Park (2013), where he asked 419 adult Internet users in the United States true or false questions about their understanding of the legal limits on data collection and the sharing practices of businesses and government. On six of seven questions presented, fewer than half of respondents gave the correct answer. For example, only 14% knew that it was not the case that e-commerce sites, such as Amazon, are required to give individuals the opportunity to see the information the website has gathered about them. In addition, 40% of respondents thought that it was illegal for a website to share information with its affiliates without telling the consumer the name of the affiliate. In a recent study of African-American young adults, Park and Jang (2014) found that 42.4% of study participants "mistakenly believed that it is illegal for smartphone providers to collect locational data based on their mobile use."

Objective Consumer Knowledge of Privacy-Impacting Corporate Data Practices

While research about how well informed consumers are about the laws and regulations that govern their privacy has been helpful in understanding the extent to which consumer decision-making is informed, one area remains understudied: how much do people actually know about the ways in which companies collect their data? If consumers do not know that data collection is happening, then they can neither make informed decisions, nor engage in privacy-protecting actions, nor ask to access their data, nor file a complaint about the collection with the regulator, as envisioned by FIPPs.

In Canada, research about how much consumers know about privacy-impacting business practices has been limited to three studies, in 2009 (Ekos), 2015 (Phoenix Strategic Perspectives Inc.), and 2016 (Phoenix Strategic Perspectives Inc.) for the Office of the Privacy Commissioner of Canada (OPC), which tested how knowledgeable Canadian consumers feel. 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. In the United States, research similar to that of the OPC was conducted by the Pew Research Center (Rainie, 2016), which reported that 50% feel confident that they understand how their data are being used by companies. No studies have tested Canadians' objective knowledge of privacy-impacting business practices, rather than how knowledgeable individuals perceive themselves to be.

In the United States, knowledge of data practices related to online activities has been tested by Turow et al. (2005) and Turow, Hennessey, and Bleakley (2008), Park (2013), Kezer et al. (2016), as well as Acquisti and Gross (2006). In two national studies of Americans, Turow et al. (2005, 2008) examined whether consumers know that companies have the ability to track their activities across many sites on the web. In both studies, he found that approximately 20% of the American population did not know that their website browsing behaviour could be tracked. In another study, Park (2013) examined 419 American Internet users and asked them questions to determine their level of knowledge of marketing data collection practices on the Internet, finding that "more than 40% of the respondents misunderstood the most basic aspects of institutional data practices. (page 223)" For example, 43% of respondents did not know

that a company can tell that a person has opened an email, even if he or she does not respond. Another recent study by Kezer et al. (2016) indicates similarly low levels of awareness of companies' data abilities related to online browsing among US adults. For example, only 15.1% of respondents to Kezer's survey correctly stated that "when you go to a website, it can collect information about you even if you do not register," and only 5.8% knew that "popular search engine sites, such as Google, track the sites you come from and go to."

Park and Jang's more recent (2014) study found similarly low awareness of companies' data practices on mobile phones. For example, a third of respondents in the study did not know that "companies today have the ability to place an ad that targets you based on information collected on your mobile phone." In 2016, the Pew Research Center found that more than half of consumers cannot identify the cookie as the primary website browsing tracking tool. Qualitative research by Park and Jang (2014) reports that while interviewees 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.

Method and Sample

To investigate the level of Canadians' knowledge about businesses' data practices, a national survey was administered to 1,005 Canadian respondents. Respondents were obtained through a household panel maintained by research company comScore. Respondents were obtained from all 10 provinces and territories and matched provincial population percentages. The participants' ages ranged from 18 to 89 years old with the average being 47.3 years (SD = 13.7).

In the survey, respondents were presented with 16 statements about how corporations can collect, store, and use consumers' private data. Following the methodology used by Turow, some statements presented to respondents were true and some were false (Hoofnagle, King, Li, Turow, 2010; Turow et al., 2005; Turow et al., 2007; Turow et al., 2008). For each statement, respondents were asked to indicate whether they believed the statement was true, false or they did not know. For example, one statement read, "Email services such as Gmail automatically scan emails that people send and receive and show them online advertisements based on their email" (this is a true statement). An example of a false statement is, "Retail stores use cameras to record the way people walk and use that information to identify a particular person when he or she enters the store next." Some statements were related to established technologies, while others concerned technologies that have only recently been introduced.

Analysis

The objective of the survey was to examine the extent to which the Canadian population is aware of how corporations collect and use consumers' personal information. To investigate this, respondents were presented with 16 statements and asked to indicate if each statement was true, false or they "don't know" (DK). If the respondent gave an incorrect answer or indicated that they didn't know, then the response was recorded in Table 1 as "Did not know correct answer." The correct answer to each data collection/usage scenario is indicated in bold, italicized text in Table 1.

As evidenced by the results in Table 1, many Canadians lack a basic awareness and understanding of how companies collect and use their personal data. Specifically, on 10 of the 16 statements, more than 60% of the respondents could not correctly identify how their data were being collected and used.

As seen in Table 1, the highest level of misunderstanding was for the statement, "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" (question adapted from Turow et al., 2005). For this statement, 75% of the respondents did not know the correct answer (false). Our findings precisely match the result found in a study of Americans, 75% of whom also did not know the correct answer to this question (Turow, Hennessy, & Bleakley, 2008).

A total of 73.8% of respondents did not know that companies insert inaudible, high frequency sounds into online advertisements that can then be picked up by all devices to allow advertisers to track users' activities on all their devices (technique described in Center for Democracy & Technology Workshop, 2015). Similarly, 73.8% of respondents did not know the correct answer (true) to the statement, "Some companies put cameras into billboards and smartphone/tablet apps that can recognize people's emotions and use that information to show people advertisements that match their mood."

The highest level of awareness was for the statement, "Social media companies like Facebook record which pages people 'Like' and then use this information to show online advertisements that match the person's interests" (83.3% correctly identified this is a true statement). A total of 75.3% of respondents correctly identified that "Companies track and record people's activities across many sites on the Internet." This is similar to the findings of two US-based studies (Turow et al., 2005; Turow et al., 2008). In the 2008 study, Turow found that 83% of the US sample knew that companies track people's activities around the Web, up from 80% in the 2005 study.

A high percentage of respondents indicated that they don't know how companies collect and use their data. As seen in Table 1, more than 40% of respondents indicated that they don't know how companies collect and use their data on five of the 16 scenarios. Viewed another

Table 1
Awareness of how Canadian companies collect and use personal data

	True (%)	False (%)	DK (%)
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. **(75% did not know correct answer)**	57.4	***25.0***	17.6
Companies insert inaudible, high frequency sounds into online advertisements and TV commercials which can then be picked by all devices (computers, smartphones, tablets, TVs). This allows advertisers to track users' activities on all their devices. **(73.8% did not know correct answer)**	***26.3***	27.6	46.2
Some companies put cameras into billboards and smartphone/tablet apps that can recognize people's emotions and use that information to show people advertisements that match their mood. **(73.8% did not know correct answer)**	***26.3***	26.7	47.1
Companies monitor fitness-tracking devices (such as Fitbit or Apple Watch) and share the health information they collect with insurance companies. **(70.0% did not know correct answer)**	28.3	***30.0***	41.7
Retail stores use cameras to record the way people walk and use that information to identify a particular person when he or she enters the store next. **(69.4% did not know correct answer)**	33.7	***30.5***	35.7
Shopping malls and retail stores use smartphones' Wi-Fi to track people's location even if they don't connect to any Wi-Fi network. **(69.1% did not know correct answer)**	***30.9***	29.0	40.1
Some retailers take pictures of their customers and use facial recognition technology to identify a particular person the next time he or she enters the store. **(67.7% did not know correct answer)**	***32.3***	26.7	41.0
Retailers analyze women's purchase history to determine if they are pregnant in order to send them coupons and ads relevant to pregnancy**.** **(64.3% did not know correct answer)**	***35.7***	25.5	38.8
If a company promises that the data they collect about a person is stripped of their name and contact information, then this information can never be linked back to the individual. **(64.1% did not know correct answer)**	30.0	***35.9***	34.1
Smart voice-activated devices, such as Apple Siri, Microsoft Cortana or SmartTVs, record and store everything people say to them. **(62.1% did not know correct answer)**	***37.9***	22.9	39.2
Email services such as Gmail automatically scan emails that people send and receive and show them online advertisements based on the content of the email. **(58.6% did not know correct answer)**	***41.4***	19.5	39.1
Some smartphone/tablet apps collect information such as the device's phone log, contact list, calendar, location and unique numbers that identify the device and share this data with companies. **(48.9% did not know correct answer)**	***51.0***	17.1	31.8
Specialized companies exist that match information such as people's location, purchasing habits, online and offline activities and interests/hobbies to their names and contact information and share this information with other businesses. **(37.3% did not know correct answer)**	***62.7***	10.5	26.8
Some smartphone/tablet apps track people's location even when they are not using the app and share this location information with other companies. **(30.2% did not know correct answer)**	***69.9***	9.4	20.8
Companies track and record people's activity across many sites on the Internet. **(24.7% did not know correct answer)**	***75.3***	6.6	18.1
Social media companies like Facebook record which pages people "Like" and then use this information to show online advertisements that match the person's interests. **(18.7% did not know correct answer)**	***81.3***	3.1	15.6

way, at least one-third of respondents stated that they don't know how their data are being used in 11 of the 16 scenarios.

Differences in awareness and understanding of corporate data practices were examined among four demographic subgroups: gender, age, income, and education. With respect

to gender, the data show that men had generally higher levels of awareness and understanding of data collection usage and practices than women. Specifically, men had significantly higher awareness or understanding levels on 10 of 16 scenarios. The largest difference was with the statement "Some companies put cameras into billboards and smartphone/tablet apps that can recognize people's emotions and use that information to show people advertisements that match their mood." Thirty-five percent of men correctly identified this statement as true, while only 20% of women did so (chi-square 30.1, $p < .01$).

These findings with respect to gender disparity in objective privacy knowledge are consistent with past studies in the US context (for instance, Turow, Feldman, & Meltzer, 2005; Park, 2015b). Park (2015b) found that privacy-related knowledge was especially low among older and married women as compared to men. A possible explanation for the disparity is that men may tend to be more skilled at various technology-related tasks (Schumacher & Morahan-Martin, 2000). An alternative explanation is women's tendency to perceive themselves as less competent than they actually are (Correll, 2001) and to exhibit lower self-confidence in their abilities and technology-related activities as compared to men (Torkzadeh & Van Dyke, 2002; Schumacher & Morahan-Martin, 2000). This explanation is supported by a 2017 study of Canadians' subjective and objective knowledge of the content of PIPEDA, which found that men were more subjectively confident that they had knowledge of PIPEDA than women, even though there was no difference in objective knowledge between genders (Morrison, 2012). In the context of our study, this tendency may have led women to indicate that they don't know the answer more frequently than men, which led to a lower percentage of correct answers.

For the purpose of analysis, age was broken down into five groups (18–34, 35–44, 45–54, 55–64 and 65+). These groups follow the age categorization conventions used by Turow in previous studies (Turow, Feldman, & Meltzer, 2005; Turow, 2008). Statistically significant differences were found between age groups in 10 of the 16 questions. On questions where a difference exists, the data shows that the two younger age groups (18–34, 35–44) have better knowledge of corporate data practices than older groups (55–64, 65+). The largest difference between groups was seen in the following statement: "Some smartphone/tablet apps collect information such as the device's phone log, contact list, calendar, location and unique numbers that identify the device and share this data with companies." For this statement, 57% of the youngest age group (18–34) knew that this was true, as compared with only 31% of those 65+ (chi-square 29.2, $p < .01$). These findings may be explained by the fact that younger individuals typically lead the adoption and use of new technologies (Park 2015b), becoming more familiar with new privacy and technology developments than older people.

Income was broken down into three groups (< $40,000, $40,000–$99,999, and $100,000+). The data show that income had a moderate effect on respondents' awareness of how their personal data were being used. Specifically, in eight of the 16 scenarios, there were significant differences in knowledge based on respondent income. In all cases where differences occurred, the data reveal that as income goes up, so does the percentage of correct answers. For example, 23% of respondents who earn less than $40,000 correctly identified that the following statement is false: "Companies monitor fitness-tracking devices (such as Fitbit or Apple Watch) and share the health information they collect with insurance companies." This percentage is significantly lower among individuals who earned $40,000 to $99,999 (31% correct) than the $100,000+ group (39% correct) (chi-square 13.0, $p < .01$). Another example shows that while 84% of the highest income group correctly identified that "Companies track and record people's activities across many sites on the Internet," this percentage falls to 76% for the mid-range income group, and 71% for the low income group (chi-square 10.2, $p < .01$). These findings are consistent with those of Turow et al. (2005) and Park and Chung (2017) in the US context, and may be explained by higher income individuals having more time to consume news, having higher rates of technology use, and a greater concern for their digital footprints (Pew Research Center, 2014).

Respondents' level of formal education had a significant impact on their level of understanding of how their data are being collected and used. Respondents with a university degree gave a higher percentage of correct answers in 11 of the 16 scenarios. The largest difference was seen in the statement, "Retailers analyze women's purchase history to determine if they are pregnant in order to send them coupons and ads relevant to pregnancy." For this scenario, 51% of those with a university degree correctly identified this as a true statement, compared with only 29% of those who did not have a degree (chi-square 45.4, $p < .01$). Education-related differences in knowledge are also similar to those found in the US (for instance, Park and Chung, 2017). Since higher levels of education correlate with higher income in Canada (Finnie, Afshar, Bozkurt, Miyairi, & Pavlic, 2016), the factors that may contribute to higher levels of privacy knowledge among higher income individuals may be implicated here, as well.

Limitations of the Privacy Notice

Our findings are not surprising in light of past research, which has identified the many limitations of the privacy notice. Research shows, for example, that privacy notices are simply too long, complex, and vague for the average person, or even one with legal training, to understand, and are, accordingly, not read (for instance, Milne & Culnan, 2004). Marotta-Wurgler (2015) reports that the average privacy notice is 2,227 words long, while

McDonald and Cranor (2008) calculate that reading all privacy policies a person encounters in a year would take an average of 244 hours.

Moreover, notices are often silent on major issues; they use vague, ambiguous, and mitigating language and undefined terms, contain contradictory statements, and the vast majority of notices is subject to change at any moment without informing the consumer (Cranor, Hoke, Leon, & Au, 2014; Marotta-Wurgler, 2016; McDonald, Reeder, Kelley, & Cranor, 2009). In 2013, research for the OPC found that 62% of Canadians consider privacy notices "somewhat" or "very vague" in terms of giving them information about what a company will do with their data, up from 53% just a year earlier (Phoenix Strategic Perspectives Inc.). Only 47% of Canadians feel confident that they understand how their information will be used when it is shared with an organization (Phoenix Strategic Perspectives Inc., 2015).

It is perhaps not surprising, therefore, that in a 2014 study, only two out of 1,000 consumers reported accessing privacy policies, and those who did spent very little time on them (Bakos, Marotta-Wurgler, & Trossen, 2014). According to research for the OPC, 50% of Canadians rarely or never read privacy policies (Phoenix Strategic Perspectives Inc., 2013). Privacy notices confuse consumers (Protecting Consumer Privacy in an Era of Rapid Change, 2010) and many actually view them as barriers to the services and goods they are attempting to access online (Luo, 2002).

The above-described research into the limitations of the privacy notice presents an initial challenge to the premise that as long as corporate data practices are disclosed in a privacy notice, the consumer is aware of such data practices and consents to them in an informed manner.

Discussion

Summary

Our findings further undermine the belief that the disclosure of corporate data practices in a privacy notice ensures that consumers are informed about such practices. On the contrary, our research indicates Canadians are ill informed about how companies are collecting and using their personal data, despite the existence of, and consent to, privacy notices. The immediate implications of our findings are 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 that the consumer is informed about data practices, as required by FIPPs. New methods of informing Canadians about how their data are being collected and used by businesses must be devised. These new methods must respond to the challenges presented by emerging technologies.

Contributions to Scholarship

Our research builds on earlier studies of consumers' objective knowledge of corporate data practices in several ways. Firstly, it is the first large-scale survey that studies Canadian consumers' actual, rather than perceived, knowledge of how businesses collect and use their private data. Secondly, we extend earlier findings by exploring consumers' objective knowledge of established business data practices, such as capturing Internet browsing history, as well as emergent data collection practices using inaudible beacons, emotional recognition, and others. Thirdly, while previous research has identified a number of problems with the privacy notice as a tool for informing consumers about how their data are being collected and used, our research quantifies the gravity and extent of this inadequacy. A further contribution of this study is to highlight the need to enhance Canadians' digital privacy literacy, and to develop and test novel approaches to disclosure of corporate data practices.

Applied Implications

Our research indicates that Canadians are ill informed about corporate data practices, partially as a result of the inadequacies of the privacy notice as a mechanism for disclosing such practices. The immediate implication of this research is that new methods of informing consumers of how their data are being collected and used are needed in order to comply with the FIPPs requirement that consumers provide informed consent to corporate data practices.

Past research into enhancing corporate data practice disclosure has largely focused on improving the traditional privacy notice. First, shorter, clearer, and more standardized notices have been recommended by the Federal Trade Commission (FTC) in the United States (2012), as well as academics (Martin, 2015). Some scholars have argued for the standardization of particular disclosures, "very much like a menu" (Marotta-Wurgler, 2015, p. 30). There were several government efforts in the US to create simplified model privacy forms (Bruening & Culnan, 2016), and some efforts by private citizens to simplify existing policies, such as a privacy lawyer rewriting Instagram's privacy policy in simple terms for the benefit of adolescent users (Wang, 2017). However, these efforts have met with challenges: businesses indicate that it is difficult to reconcile the desire for simplicity and concision with the requirements of completeness (Bruening & Culnan, 2016). Moreover, consumer testing of a simplified, standardized model privacy notice for mobile applications, developed by the National Telecommunications and Information Administration (NTIA), revealed that many users still did not understand the terms of the simplified notice (Balebako, Shay, & Cranor, 2014).

Another method of notice simplification is the "layered notice," which is a privacy notice that begins with a short summary of the most important terms of the notice, followed by its full text. Layered notices have been recommended by the FTC in the United States (2012) and the OPC in Canada

(Office of the Privacy Commissioner of Canada, 2014). However, research indicates that those who read layered notices were actually less clear on a firm's privacy practices than those who read long notices, and did not choose to read the long notice even if they found that the layered notice did not include the information they sought (McDonald, Reeder, Gage Kelley, & Cranor, 2009).

Privacy seals were another suggested option. Privacy seals are self-regulatory privacy efforts by businesses, whereby companies adhere to a particular set of privacy standards or frameworks, such as TRUSTe, and then display a certification seal to consumers to indicate their compliance. This is intended to allow consumers, presumably familiar with the framework, to quickly appreciate the quality of a particular privacy contract. However, research by Marotta-Wurgler (2015) indicates the low adoption of privacy seals. She notes that, "if seals such as TRUSTe were supposed to reduce search and reading costs and standardize privacy practices by having firms embrace them widely, this presents further evidence that doesn't appear to be working well. (page 18)"

Martin (2015) identifies machine-readable notices as one solution to the issue of consumers believing that they are more protected by privacy policies than they actually are. Such notices rely on programs such as P3P (Platform for Privacy Preferences, developed by the World Wide Web Consortium), which offers businesses the ability to communicate their privacy policies in a manner that can be decoded by a user's browser or device (Bruening & Culnan, 2016; Cranor, 2012). Then the browser would compare the firm's policy with the user's privacy preferences, and take action or issue a notification where there is a discrepancy, in an easily comprehensible and detailed format (Cranor, 2012). Many believed that P3P is too complex to use, so it has not been widely adopted (Lee & Speyer, 1998).

Privacy icons, such as those used in the Mozilla Privacy Icons Project, are designed and displayed to visually identify key information, such as whether a website shares personal information with third parties (Office of the Privacy Commissioner of Canada, 2014). Additional efforts to improve privacy notices include research initiatives by CUPS Lab (The CyLab Usable Privacy and Security Lab at Carnegie Mellon University) to identify the notice formats that best facilitate accurate consumer understanding of privacy policies (Kelley, Bresee, Cranor, & Reeder, 2009). This research found that consumer understanding was best when the notice was presented in table format, similar to a nutritional label (Kelley et al., 2009). However, critics suggest that this could lead to misleading perceptions and limited comparability between businesses, because, unlike nutritional information, information about privacy practices is neither quantifiable, nor constant, nor comparable to a standard (Bruening & Culnan, 2016).

Given the limited effectiveness of the improvements described above, we anticipate that merely improving on the traditional privacy notice will not be enough to effectively inform consumers of data practices in today's mobile, connected environment. The privacy notice is unable to respond to the four key challenges presented by new technologies, such as Wi-Fi pinging, inaudible beacons, and the Internet of Things, which have revolutionized the nature, source, and location of data collection.

The first challenge of emerging technologies is that it is not practicable for mobile consumers to process and consent to written privacy notices. Wi-Fi pings, beacons, or facial recognition-enabled billboards are not preceded by a notification of data collection, let alone a privacy notice. Informing consumers about the data practices related to these technologies is difficult to implement in practice, and at this time, there are no identifiable Canadian industry standards for doing so. Consider, for example, a situation where retailers in a mall rely on location tracking using Wi-Fi pings or audio beacons to gather consumer visit data and movement patterns. How would notice be provided in a meaningful way? On the web or in an app store, people can be asked to read a statement and agree to it before they use the website or app. However, how does a company get a person's advance consent to data collection when it is happening in real time, as he or she is walking? It would be unlikely that people would be able or willing to read privacy statements as they are walking through a mall. At the same time, sufficiently short, real-time notifications, such as pop-ups on the smartphone or a sign at the entrance are not able to provide enough information to inform consumer decision-making about privacy. Such notifications would not identify who is collecting the data and why, how it will be used, where it will be stored, and so on. Moreover, even if sufficient information were provided, the consumer would then have to act on it by providing (or withholding) their consent to collection. This is an impracticably onerous burden to put on individuals on the go. The cognitive overload associated with large quantities of disclosure (Ben-Shahar & Schneider, 2011) and a distracted state of mind are already an issue for consumers processing traditional privacy notices (Stone, 2007; Small & Vorgan, 2008). The problem of distraction will be significantly worse with the growth in data points, sources, and connections associated with the Internet of Things (Brill, 2014), or when the consumer is expected to focus on the notice in an environment where they are in motion and are not actively engaging with their device.

Second, in addition to practical difficulties of written notice-giving, it is often not clear who would be responsible for providing notice. For example, if in-store movement data are collected in a shopping mall by using a Wi-Fi ping or beacon, then who is responsible for notifying the individual that he or she is being tracked? Is it the mall, the particular retailer who uses the data, the business that set up the necessary hardware, the Wi-Fi connectivity provider, the application that detects the beacon signals, or some other party?

Third, approaches taken by some marketers, whether intentionally or not, make consumer notification even more difficult and less intuitive and reduce the options people have to protect themselves from data collection. For example, in this paper we discuss one of the newest data collection technologies, inaudible beacons. Whereas an individual could previously avoid data collection by turning off Bluetooth and Wi-Fi connectivity on his or her mobile device, in the case of inaudible codes, this option is no longer available. Indeed, this is the very benefit that these data collection companies advertise: inaudible codes can reach the 35% of devices whose Bluetooth functionality is turned off (Signal360). What is more, businesses are inserting beacon recognition capabilities into apps that are not related to potential beacon locations (Turow, 2017). For example, rather than requiring that a consumer have a department store application on their smartphone in order to interact with the store's beacons, beacon recognition capabilities might be inserted into an unrelated application, such as a flashlight. This puts the onus on the consumer to, counterintuitively, search for disclosure about data collection pertaining to store visits in the terms and conditions for a flashlight.

Finally, another development that will make administering the privacy notice more difficult is the explosion in the number of devices that are capable of data collection, fuelled by the Internet of Things (IoT). IoT dramatically increases the number of privacy consents a consumer may have to give, which contributes to the problem of information overload discussed above. Previously, privacy concerns existed only in discrete, easily identifiable online activities that explicitly involved exchanges of information, such as Internet browsing. The proliferation of IoT means that everyday objects, such as refrigerators, light bulbs, cars, and thermostats now also have privacy implications. Given this scenario, the consumer must, again counterintuitively, review privacy information in user manuals or set-up instructions, many of which would previously have been simply discarded. Where privacy-related information is vague, ambiguous, and complicated, the onus is on the consumer to imagine what information can be gathered by, say, a light switch, and how it can be used. IoT devices collect information that could previously only be obtained via survey methods, such as what time people usually wake up, when they come home, or what they eat. IoT-enabled wearable technologies can continuously collect information such as heart rate, glucose level, or calorie use, which could never be done before. Wearable devices' attachment to human bodies and the associated "massive instantaneous data feeding" may make it even more difficult for people to understand privacy issues associated with the data flows (Park & Skoric, 2017, page 77). In addition, with advancements in data analytics technology, innocuous information collected through IoT-enabled devices can be combined to draw inferences about sensitive data (Federal Trade Commission, 2015). As such, IoT and wearable devices have the potential to provide marketers with increasingly more detailed, accurate, and personal consumer profiles, while further obscuring consumer understanding of privacy implications.

In sum, informing consumers about data collection in the modern age is made more difficult by the sheer volume of data collection and consent points, the mobility of consumers, and the unexpected contexts in which data collection takes place. The privacy notice was invented in a time of static data collection moments. Its usefulness has not kept up with technological change. If Canadian society is concerned about addressing the issues uncovered by our research and ensuring that consumers are able to make meaningful decisions about how their data are treated, the current privacy governance framework will require significant changes.

One way to improve consumer awareness of corporate data practices is to enhance the general digital privacy literacy of Canadians. The current interpretation of FIPPs focuses on informing consumers of each discrete instance of data collection and use, and obtaining their consent to each such instance. However, the privacy notice experience has shown that relying on individual companies to provide information about specific data collection instances has not resulted in consumer understanding of the data collection landscape. Canadians' low awareness of companies' data collection capabilities may be more effectively addressed by broader societal education initiatives.

One option for education delivery is introducing a digital privacy unit to Canadian school curricula. In Ontario, the elementary school curriculum already includes information about protecting online privacy in the context of sexting (Ontario Ministry of Education, 2015). The curriculum also includes media literacy, which teaches students to recognize various advertising tactics and implied advertising messages as early as grade two (Ontario Ministry of Education, 2006). Thus, educators have already recognized the value of teaching children about the ways in which new data-sharing technologies can present new risks and challenges, and how companies can exert influence on consumers at an early age. However, new technologies, some of which are discussed in this paper, create many more privacy challenges, and allow for the use of much more refined influence tactics by businesses. Curricula should be updated to reflect this wider range of new issues.

Government-sponsored advertising could also be used to educate the general public on specific data collection and privacy issues. The OPC and its provincial counterparts have gathered extensive resources on a number of privacy topics, although most are currently presented in largely academic format on their websites. Currently, the OPC does not feature any consumer-oriented information about the technologies mentioned in this paper, and presents information for individuals in a somewhat disparate manner, rather than as a single, comprehensive informational guide. These

offices could use their expertise to publish easily accessible and easy-to-read resources describing business data practices related to both established and emerging technologies, as well as the steps individuals could take to protect their information. Then, government-sponsored television advertising could be aired to direct Canadians to these resources. This method of public education has, in fact, been previously used. For example, the Government of Ontario has recently funded similar advertising campaigns to explain the dangers of distracted driving.

On the whole, care should be taken to develop educational initiatives that are accessible and tailored to any unique needs of women, older individuals, and those with less income and formal education. As indicated by our findings, such individuals have particularly low knowledge of corporate data practices, which leaves their data especially vulnerable to corporate exploitation.

Limitations and Future Research Directions

In the past, the privacy notice purported to offer individuals information and privacy control over each discrete instance of data collection. However, as discussed, given the challenges presented by emerging technologies, informing consumers about each instance when their data are being collected and used is no longer practicable. Below we offer several ideas for novel privacy controls, which ought to be subject to further research and experimentation.

One option is a Do Not Track List. For many years, online browsers and other tools have offered users do-not-track capabilities that prevent the collection of their browsing histories. Similar solutions can potentially be implemented in response to the previously discussed issues concerning the capture of information while an individual is moving through a public space. It may be possible to allow individuals to pre-emptively opt out of collection of all mobile, facial, location, and other data. The Future of Privacy Forum (FPF), a non-profit organization that brings together thought leaders to address the privacy challenges of new technologies, offers one means by which this approach could be operationalized. The FPF has created a website called www.smart-places.org, which allows individuals to enter their mobile devices' Wi-Fi and Bluetooth MAC addresses to opt out of data collection by organizations that voluntarily participate in the FPF program. While the premise of the FPF opt-out solution addresses some of the privacy challenges of new technologies we have identified, the program has some practical shortcomings. First, it is a self-regulatory and unenforceable initiative, which has only interested 11 corporations to date. Second, the program is underpublicized, perhaps due to limited funding.

To address these limitations, we suggest a possible solution based on the same premise, but with two key differences: government oversight and involvement, and, ideally, the reliance on technology to simplify the users' task.

A program analogous to www.smart-places.org could be administered by a governmental agency, such as the Canadian Radio-television and Telecommunications Commission. First, governmental oversight and involvement would mean the availability of robust advertising and enforcement capabilities and budgets to allow the program to reach critical mass. Second, the government could require corporations to join the program, which FPF cannot do. Companies could be legally required to purge any data they capture from the listed MAC addresses. As an alternative to data purging, devices could be built to have the capability of emitting certain signals that would alert data collection points such as routers or beacons not to engage with a device on the Do Not Track List. Corporate compliance could be enforced by randomly reviewing the mechanisms that corporations have put in place to avoid the collection of data related to the MAC addresses on the Do Not Track List, and financial penalties could be imposed.

Ideally, a government-mandated program could also rely on technologies to make the task of adding one's information to a Do Not Track List easier. For example, a mobile registration application could detect MAC addresses automatically. Additionally, the Do Not Track List could be expanded to preclude corporate tracking using facial recognition technology. During the registration process, the user could add his or her photograph to the list and companies would have to automatically purge any facial recognition data collected about the photographed individual.

Alternatively, some believe that limiting data collection is impracticable because data collection is now so widespread as to be virtually uncontrollable by the individual. They also note that, currently, the only reliable way to preclude data collection—foregoing the use of a product or service—is untenable. In today's world, it is almost impossible for an average person to not have their data collected in some form. In order to avoid leaving a digital footprint, one would have to never use a credit card or a smartphone, browse the Internet and, as IoT becomes increasingly widespread, perhaps even turn on a light. This inability to avoid generating data is especially significant with respect to novel medical devices, such as contact-lens glucose monitors, since opting out of their use can have significant health-related repercussions (Park & Skoric, 2017).

In addition, scholars and commentators have noted that a focus on preventing data collection undercuts one of the key benefits of modern technologies: the possibility of using Big Data analytics to analyze disparate data sets for beneficial purposes. An example of such use was a study by researchers at Kaiser Permanente who studied medical records of 3.2 million individuals, which had been previously collected for another purpose and retained, and found a link between autism spectrum disorders in children and

their mothers' use of anti-depressants (Croen, Grether, Yoshida, Odouli, & Hendrick, 2011).

Given the difficulty of limiting data collection, and the value of access to large data sets, which can yield unpredictable benefits, some have suggested regulating data use, rather than collection. For example, Craig Mundie (2014), former Chief Research and Strategy Officer at Microsoft, offers a technological alternative to ensuring that an individual's data are used appropriately once they are inevitably captured. He envisions implementing data wrappers similar to those currently in use by Digital Rights Management systems, or the meta-data permissions used by Microsoft Word to govern who can view, edit, or print a document (Mundie, 2014). In such a framework, each piece of data would be wrapped in instructions describing how that data can be used. Any application seeking to use the data would have to have the required approvals to unwrap and access the data. Mundie suggests that consumers should have the opportunity to select trusted third-party organizations to give consent to various data uses on their behalf, in order to limit the burden of keeping up with who should be able to access their data and when. Under this system, technologies and very strict enforcement regimes would have to be created in order to ensure businesses' compliance with the trusted organizations' data use instructions. A similar approach, involving tagging all collected data with metadata that includes the individual's use preferences and then relying on software to verify whether actual usage is consistent with these preferences, was proposed by the World Economic Forum (2013).

Other stakeholders have also proposed the de-prioritization of the consent requirement and relying on other means of ensuring consumer privacy. Such means include requiring complete de-identification of all data collected and directly regulating corporate data uses by establishing no-go zones that would prohibit some uses of certain types of data regardless of consent (Office of the Privacy Commissioner of Canada, 2016).

Still others seek to preserve the consent framework, with some updates to respond to IoT and wearable technologies. The Article 29 Working Party (WP29) in Europe proposes to require companies to allow users to withdraw data collection consent at any time without financial penalty or restriction on device capability (2014). Park and Skoric (2017) describe such a solution as "imperative" with respect to wearable devices like Google Glass, with have especially far-reaching data collection capabilities (page 76). The FTC suggests the inclusion of QR codes on IoT devices to lead consumers to more in-depth information, set-up wizards that explain and select privacy settings, and dashboards that allow consumers to set up and revisit privacy preferences (Federal Trade Commission, 2015). Others recommend establishing enforceable codes of conduct to standardize privacy practices within business sectors (Office of the Privacy Commissioner of Canada, 2016).

Ultimately, the privacy challenges posed by the complexity of today's technological landscape will require a multi-faceted response. First, governments have a significant role to play in developing privacy standards and enforcement mechanisms, as well as providing general education and centralized means of protecting privacy. The adequate protection of individuals' privacy in today's increasingly data-rich world will almost certainly require subjecting the technology industry to greater governmental oversight instead of relying on the effectively self-regulated privacy notice model. Several studies have suggested that self-regulation has been ineffective in the online sector (for instance, Park, 2011, 2015; Campbell, 1998; Kang, 1998; Lessig, 1999) and there is no evidence to suggest that this would change in today's technological landscape. On the contrary, in today's environment, "industry will need a clearer regulatory scope regarding data-mining practices" (Park & Skoric, 2017). (page 76)

Second, the implementation of robust privacy protection measures will require the co-operation of businesses. Businesses are better placed to be proactive in protecting consumers' private data. In particular, businesses can implement "Privacy by Design" principles developed by Ann Cavoukian (2011), the former Privacy Commissioner of Ontario and a renowned privacy advocate. The "Privacy by Design" principles stipulate that privacy must become central to the design of devices, as well as business and data practices, instead of being treated as an afterthought. Under this approach, all businesses involved in data collection and use, including device manufacturers, data processers, and data users, would need to proactively identify the privacy risks that arise from their activities. Then, these companies would need to design devices and practices in a way that mitigates privacy risks by embedding privacy as the default, ensuring data security and maintaining transparency, among other measures.

Finally, the wide variety of existing practices and technologies means that there is no single method of ensuring consumer awareness of, and informed consent to, data collection in all contexts. Some manner of privacy notice may remain an appropriate solution in situations where data collection occurs in a discrete moment, in a static environment (such as Internet browsing on a computer). When the consumer is in motion, a different approach is required. For example, a centralized means to opt out of collection, such as a Do Not Track List, can address the privacy of location, facial recognition, and similar data collected in real time. A version of IoT-specific safeguards developed by WP29 in Europe and the FTC may be used to address the privacy challenges of IoT-enabled devices, including wearables. A Do Not Use or similar solution can be used to address the privacy challenges of other technologies, such as inaudible beacons.

While this study advances our knowledge of Canadians' understanding of data collection practices, it is limited by the

fact that an online panel was used for data collection. While online panels have, in recent years, become more representative of the Canadian population as a whole, it is reasonable to assume that only certain types of individuals join an opt-in consumer panel.

In conclusion, future research is needed to arrive at the most appropriate combination of solutions to respond to technological changes. However, regardless of what the optimal mix of means of promoting consumer literacy and privacy protections will be, one thing is clear: changing the status quo will require considerable political will and public support.

JEL Classification: M38

References

Acquisti A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Lecture notes in computer science, Vol. 4258: Privacy enhancing technologies* (pp. 36–58). Berlin, Germany: Springer.

Article 29 Data Protection Working Party. (2014, September 16). Opinion 8/2014 on the recent developments on the Internet of Things. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Bakos, Y., Marotta-Wurgler, F., & Trossen D. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. *Journal of Legal Studies, 43*(1), 1–35.

Belabako, R., Shay, R., & Cranor, L. F. (2014). Is your inseam a biometric? A case study on the role of usability studies in developing public policy. Retrieved from https://doi.org/10.14722/usec.2014.23039

Ben-Shahar, O., & Schneider, C.E. (2011). The failure of mandated disclosure. *University of Pennsylvania Law Review, 159*, 647–749.

Brill, J. (2014). The Internet of Things: Building trust and maximizing benefits through consumer control. *Fordham Law Review, 83*(1), 205–217.

Bruening, P., & Culnan, M. J. (2016). Through a glass darkly: From privacy notices to effective transparency. *North Carolina Journal of Law & Technology, 17*(4), 515–580.

Campbell, A. J. (1998). Self-regulation and the media. *Federal Communications Law Journal, 51*, 711.

Cavoukian, A. (2011, January). Privacy by design: The 7 foundational principles. Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

CBC News. (2016, October 4). 6 Telemarketers fined for violating Do Not Call List. Retrieved from http://www.cbc.ca/news/business/do-not-call-list-crtc-1.3790871

Center for Democracy & Technology. (2015, October 16). Comments for November 2015 workshop on cross-device tracking. Retrieved from https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking

Correll, S. (2001) Gender and the career choice process: The role of biased self-assessments. *American Journal of Sociology, 27*, 307–336.

Cranor, L. F., Hoke, C., Leon, P. G., & Au, A. (March 31, 2014). Are they worth reading? An in-depth analysis of online advertising companies' privacy policies. Retrieved from https://ssrn.com/abstract=2418590

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law, 10*, 273–308.

Croen, L., Grether J., Yoshida, C., Odouli, R., & Hendrick, V. (2011). Antidepressant use during pregnancy and childhood autism spectrum disorders. *Archives of General Psychiatry, 68*(11), 1104–1112.

Culnan, M. & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*, 104–115.

Ekos. (2009). Canadians and privacy. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2009/ekos_2009_01/

Federal Trade Commission. (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers*. Washington, DC.

Federal Trade Commission. (2015). *Internet of Things: Privacy and security in a connected world*. Washington, DC.

Finnie, R., Afshar, K., Bozkurt, E., Miyairi, M., & Pavlic, D. (2016) *Barista or better? New evidence of the earnings of post-secondary education graduates: A tax linkage approach [research report]*. Ottawa, ON: University of Ottawa Education Policy Research Initiative.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes & policies? Retrieved from http://repository.upenn.edu/asc_papers/399

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193–1294.

Kelley, P.G., Bresee, J., Cranor, L. F., & Reeder, R.W. (2009). *A "nutritional label" for privacy*. Symposium on Usable Privacy and Security (SOUPS). Retrieved from https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

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

Lee, K., & Speyer, G. (1998, October 22). *Platform for Privacy Preferences Project (P3P) & Citibank* [white paper]. Retrieved from https://www.w3.org/P3P/Lee_Speyer.html

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic books.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*(2), 111–118.

Marotta-Wurgler, F. (2015). Does "notice and choice" disclosure regulation work? An empirical study of privacy policies. *Michigan Law: Law and Economics Workshop*.

Marotta-Wurgler, F. (2016). *Understanding privacy policies: Content, self-regulation, and markets* (New York University

Law and Economics Working Papers 435). Retrieved from http://lsr.nellco.org/nyu_lewp/435

Martin, K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing, 34*(2), 210–227.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 540–565.

McDonald, A. M., Reeder, R. W., Gage Kelley, P., & Cranor, L. F. (2009). A comparative study of online privacy policies and formats. *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*. Berlin, Germany: Springer, 37–55.

Milne, G., & Culnan, M. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.

Morrison, B. (2012). Do we know what we think we know? An exploration of online social network users' privacy literacy. *42nd Atlantic Schools of Business Conference Proceedings, 35*, 419–438. Retrieved from http://www.library2.smu.ca/handle/01/25696#.Wj1V5f-nFOQ

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

Mundie, C. (2014). Privacy pragmatism: Focus on data use, not data collection. *Foreign Affairs, 93*(2), 28–38.

Naryanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. Retrieved from http://ieeexplore.ieee.org/document/4531148/?reload=true

Office of the Privacy Commissioner of Canada. (2011, September 16). PIPEDA fair information principles. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Office of the Privacy Commissioner of Canada. (2014, May 8). Guidelines for online consent. Retrieved from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405/

Office of the Privacy Commissioner of Canada. (2016, May). A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/#fn64

Ontario Ministry of Education. (2006). *The Ontario curriculum grades 1 – 8: Language*. Ottawa, ON: Queen's Printer for Ontario.

Ontario Ministry of Education. (2015). *The Ontario curriculum grades 1 – 8: Health and physical education*. Ottawa, ON: Queen's Printer for Ontario.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40* (2), 215–236.

Park, Y. J, & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296–303.

Park, Y. J. (2015a). My whole world's in my palm! The second-level divide of teenagers' mobile use and skill. *New Media & Society, 17*(6), 977–995.

Park, Y. J. (2015b). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior, 50*, 252–258.

Park, Y. J., & Chung, J. E. (2017). Health privacy as sociotechnical capital. *Computers in Human Behavior, 76*, 227–236.

Park, Y. J., & Skoric, M. (2017). Personalized ad in your Google Glass? Wearable technology, hands-off data collection, and new policy imperative. *Journal of Business Ethics, 142*, 71–82.

Pew Research Center. (2014, November). Public perceptions of privacy and security in the post-Snowden era. Retrieved from http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf

Phoenix Strategic Perspectives Inc. (2013, January). Survey of Canadians on privacy-related issues. Retrieved from https://www.priv.gc.ca/media/3323/por_2013_01_e.pdf

Phoenix Strategic Perspectives Inc. (2015, January 28). 2014 survey of Canadians on privacy. Retrieved from https://www.priv.gc.ca/media/3484/por_2014_12_e.pdf

Phoenix Strategic Perspectives Inc. (2016, December). 2016 survey of Canadians on privacy. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig 1

Rainie, L. (2016, September 21). The state of privacy in post-Snowden America. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Ramirez, E., Brill, J., Ohlhausen, M. K., Wright, J. D., & McSweeny, T. (2014). Data brokers: A Call for transparency and accountability. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Schumacher, P., & Morahan-Martin, J. (2000). Gender, Internet and computer attitudes and experiences. *Computers in Human Behavior, 38*, 296–303.

Signal360. One simple, integrated solution. Retrieved from www.signal360.com/#solution

Small, G., & Vorgan, G. (2008). Meet Your iBrain. *Scientific American Mind, 19*(5), 42–49.

Stone, L. (2007). The Harvard Business Review list of breakthrough ideas for 2007: Living with continuous partial attention. *Harvard Business Review, 85*(2), 28–29.

Torkzadeh, G., & Van Dyke, T. P. (2002). Effects of training on Internet self-efficacy and computer user attitudes. *Computers in Human Behaviour, 18*, 479–494.

Turow, J., Hoofnagle, C. J., Mulligan, D. K., Good, N., & Grossklags, J. (2007). The Federal Trade Commission and consumer privacy in the coming decade. *I/S: A Journal of Law and Policy for the Information Society,* 3(*3*), 723–749.

Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' understanding of privacy in the marketplace. *Journal of Consumer Affairs, 42*(3), 411–424.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. Retrieved from https://doi.org/10.2139/ssrn.1478214.

Turow, J., Feldman, L., & Meltzer, K. (2005). Open to exploitation: America's shoppers online and offline. *A report from the Annenberg Public Policy Center of the University of*

Pennsylvania. Retrieved from http://works.bepress.com/joseph_turow/10/

Turow, J. (2017). *The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power*. New Haven, CT: Yale University Press.

US Department of Health, Education and Welfare. (1973). *Records, computers and the rights of citizens: Report of the secretary's Advisory Committee on Automated Personal Data Systems*. Washington, DC: Author.

Wang, A. B. (2017, January 8). A lawyer rewrote Instagram's terms of use "in plain English" so kids would know their privacy rights. Washington Post. Retrieved from www.washingtonpost.com.

World Economic Forum. (2013, February). Unlocking the Value of Personal Data: from Collection to Usage. *World Economic Forum*. Retrieved from http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf