"Whether it's moral is a whole other story": Consumer perspectives on privacy regulations and corporate data practices

Leah Zhang-Kennedy
University of Waterloo

Sonia Chiasson
Carleton University

Abstract

Privacy laws govern the collection, use, and disclosure of personal information by businesses. Through an online survey with 300 participants and a follow-up interview with 32 participants, we investigate Canadians' awareness of their privacy rights and how businesses manage their personal information. Further, we explore how Canadians respond to hypothetical privacy violations using ten scenarios adapted from real cases. Our participants are generally aware of having privacy rights but have insufficient knowledge and resources to exercise those rights properly. Participants did not necessarily equate compliance with the law as sufficient for ethical conduct. Through our analysis, we identified a "moral code" that consumers rely on to assess privacy violations based on the core moral values of trust, transparency, control, and access.

1 Introduction

Despite rapid technological change, the Canadian regulatory landscape under the Fair Information Practices Principles framework that has governed consumer privacy has remained largely unchanged for the last 50 years [8]. From this framework, Canada has devised ten Fair Information Principles (FIPs) under Canadian privacy law known as the Personal Information Protection and Electronic Documents Act (PIPEDA). The core principles of PIPEDA are: 1) accountability, 2) identifying purposes, 3) consent, 4) Limiting Collection, 5) Limiting Use, Disclosure, and Retention, 6) Accuracy, 7) Safeguards, 8) Openness, 9) Individual Access, and 10) Challenging Compliance (described in Appendix A4.1).

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

We investigated Canadians' perspectives on their privacy rights and corporate data practices relating to their digital data through a survey with 300 Canadian residents and followed-up with 32 interviews. The studies explored general privacy perceptions and self-reported knowledge of businesses' data collection and usage practices towards consumer data. Participants described their understanding of their own privacy rights and their interpretations of ten scenarios describing corporate data privacy practices adapted from real privacy cases published online [24] by the Office of the Privacy Commissioner of Canada (OPC) to guide compliance with PIPEDA.

Our work makes two main contributions. First, we expand the literature on individuals' privacy perspectives and understanding about corporate data practices. Participants perceived significant challenges to consumer privacy protection: a lack of awareness, difficulty enforcing privacy laws, rapid technological change, and safeguarding against hackers. They were largely unaware of the PIPEDA FIPs and unsure how they applied to the provided scenarios. The interviews uncovered that participants relied on an informal "moral code" to judge privacy violations. This code was derived from personal values of trust, transparency, control, and access. Participants wanted businesses to follow this moral code even when it exceeded legal requirements.

Second, our mixed-study methodology enables a better understanding of users' reasoning and interpretation of the situation when faced with privacy violations. Participants identified various barriers that prevented them from raising privacy concerns with businesses or regulatory bodies, even though most feel it was primarily the consumer's responsibility to report such privacy violations. We observed ambivalence from participants, as they felt that individuals were largely powerless when faced with corporate privacy violations, regardless of whether these violated regulations or their own moral code. Our work increases awareness of end-user perspectives among stakeholders and supports calls for change. It can also inform educational efforts and may prompt privacy-supportive systems to help users manage their privacy in this context.

2 Background

Personal information on digital platforms could be exposed to other individuals, but may also be collected, used and shared with institutions [7]. Social privacy involves privacy situations with other individuals, whereas institutional privacy concerns users' relationships with organizations who collect, use, and share their personal data to provide online services [30]. Past research shows that users tend to focus their privacy concerns on the appropriateness of shared information in a social context and neglect institutional privacy risks [30]. A study that focuses on social media users [32] found that privacy is understood universally as a matter of controlling one's own data relating to personal autonomy and that concerns and engagement in protective tactics centres on being personally affected by privacy violations. Many consumers feel ill-informed about how their data is collected and used [27, 28, 31].

Even though users recognize a need to protect their private data, many feel they have little control over their own data [32]. Mayer's Integrative Model of Organizational Trust [22] posits that trust is the perception of an organization's ability, benevolence, and integrity. The perceived effectiveness of privacy legislation and the trust users have towards organizations could affect their perceived effectiveness of privacy policies, perceived benefits of information disclosure, and their assessments of online privacy risks [41].

Privacy has been described in several distinct but related theories. Privacy could be described as the right to be left alone [34]. Yet, this does not capture the relationship between consumers and corporate organizations. When consumer behaviour is observed in context of privacy, a paradox is often observed [14, 19]. Reasons for the privacy paradox commonly describe consumers' lack of awareness [12, 27] and the notion of privacy as a commodity: trading personal information for convenience, goods, and services [3, 5]. Other theories define privacy as a state subjective to individuals' perceptions and beliefs [34]. Altman [6] defines privacy as the "the selective control of access to the self or to one's group." Similarly, Westin [42] described privacy as the perceived control an individual has over the collection and use of personal information. Solove [35] argues that privacy has many different meanings serving various functions in different contexts. The notion of *contextual integrity* considers the flow of information about individuals that are related to the context and could be violated when the informational norms associated with a given situation are breached [23]. Though context-dependent privacy research (e.g., [18, 39]) enables inferences about privacy decisions, further research is needed to identify conditions that lead to disclosure decisions [18].

In a recent position paper, Abdul-Ghani [1] positioned the extent to which consumers are aware of the data collection mechanism used by organizations and the tools available to consumers to protect their personal information as an ethical issue that could impact modern digital marketing practice. For example, institutional privacy assurances such as privacy policies can help to reduce individual privacy concerns [44]. The problem is that users seldom read privacy policies before agreeing to the terms and conditions because policies are long and difficult to understand [4]. Palmatier and Martin [26] recommended several ways for organizations to act ethically regarding the collection, use, storage, and dissemination of consumer data, including minimizing data collection, more transparency and control, and protecting data from data breaches, and regular audits of organizational privacy practices. Of course, other competing priorities for organizations may render these options less desirable from their perspective than their current practices, especially if current practices technically comply with the relevant regulations.

Some researchers [25] have proposed privacy as a dynamic, dialectic process, where privacy regulation is under continuous negotiation and management conditioned by one's own expectations and experiences. However, existing research on users' understanding of privacy rights shows that although many like the concepts of having privacy rights, users generally do not know what their rights are [17]. Furthermore, since users seldom read privacy policies, their expectations regarding corporate data practices are often mismatched against the actual data practices, leading to unintended sharing of personal information online [29].

3 Methodology

Our mixed study methodology was cleared by our university's research ethics board and consisted of a survey and follow-up one-on-one interviews with a subset of participants. We consulted a law and privacy expert during the development of the survey and pilot tested with lab members. We collected 300 survey responses from Canadian residents using Prolific[1] for recruitment. Participants (148 self-identifying as male, 149 as female, and 3 as non-binary) were compensated $3.40 CAD for completing a Qualtrics[2] questionnaire, which took on average 14.2 minutes to complete ($SD = 8$ minutes). Table 1 summarizes our participants' demographics. We had more participants from the province of Ontario and in the 20s to 30s age range with lower levels of education and income compared to the most recent Statistics Canada census data [37]. Note that we did not exclude participants from Quebec (QC), but the province is primarily French-speaking. Thus, we believe that this impacted their interest in our English-language survey on Prolific. Using Westin's privacy clusters, 8% of participants are marginally concerned (i.e., low privacy concern), 75% are pragmatists (i.e., medium privacy concern), and 16% are fundamentalists (i.e., high privacy concern). We found reasonable agreement between our user clusters compared to

[1] https://www.prolific.co
[2] https://www.qualtrics.com

past studies [2, 10, 13, 33].

From the survey sample, we pseudo-randomly invited (i.e., ensuring broad coverage of demographics) 32 interested participants to a virtual follow-up interview that lasted on average 39 minutes ($SD = 11$ minutes). Each interview participant was compensated $20.70 CAD. The participants' identities were anonymized with a code name (e.g., P1, P32)

3.1 Survey

The survey (see Appendix A) contained Likert-scale and multiple-choice questions with a "Prefer not to answer" option for all questions. The survey is divided into four sections, with the first section containing demographic information. The second section included Westin's privacy index questions. The third section focused on self-reported knowledge of Canadian privacy regulations, privacy rights and protection, how businesses collect, use, and share personal information, and perceptions of smart technology's impact on privacy.

In the fourth section, each participant was randomly assigned to five out of ten privacy vignettes created from real privacy complaints against organizations, investigated by the Office of the Privacy Commissioner of Canada (OPC). Randomizing five of ten vignettes enabled us to explore a broader range of data privacy scenarios without overburdening the participants. Each case's conclusions are based on factual analysis through court decisions and OPC findings, which provide reasonable guidelines for whether the organization's actions were in compliance or violation of a provision of PIPEDA. We selected ten cases with clear outcomes, covering a range of FIPs, and that are likely to occur in everyday life from twenty candidate cases. For brevity, we summarized the scenarios in Table 2. More information about the selected cases is available in Appendix A4.2.

Each vignette was displayed one at a time and accompanied by three five-point Likert-scale questions (Strong agree to Strongly disagree); the questions are: 1) I think scenarios like this are likely to happen; 2) I would be concerned about my privacy in this scenario; 3) I think the business acted appropriately in a lawful manner based on the situation described. Lastly, we asked participants to select "Which of the privacy principles do you think apply in this situation" from a checklist. To ensure a baseline understanding of the ten FIPs, we displayed the OPC's official descriptions of the principles for each scenario.

3.2 Interview

Approximately one-third ($n = 111$) of the survey participants volunteered to be contacted via email for a follow-up interview. We sent these participants a screening questionnaire containing the interview consent form; 79 participants responded, and 53 agreed to schedule an interview. In the final stage, 32 participants completed the interview via video conferencing.

The semi-structured interview consisted of two parts (see Appendix A2). In the first part, we asked general questions regarding personal information and how Canadian privacy laws protect consumer privacy. We then asked participants to explain whether they think companies and existing laws provide adequate protection and what other protections should exist. We inquired about whose responsibility it is to report privacy concerns. If the participants had a previous privacy concern or complaint against a business, they recounted the incident. Lastly, participants shared their thoughts about the biggest challenges facing consumer privacy protection.

In the second part, the participants clarified and elaborated on their responses to their previously completed vignette scenarios in the survey. We were particularly interested in their opinions about whether the business had acted appropriately under the law and whether they would be concerned about their privacy if faced with the scenario. If relevant, they were asked to share a similar situation they experienced. We re-read the scenarios from the survey before participants responded and encouraged them to thoughtfully discuss their responses to the scenarios. The interviews were audio-recorded, then transcribed using Trint[3] speech-to-text software and manually checked for accuracy.

3.2.1 Grounded Theory analysis

We chose Grounded Theory methodology [11] to analyze the interview data to form an explanatory theory about how consumers assess privacy violations in the collection, use, and disclosure of their personal information. In the first iteration, the lead researcher read all transcripts to gain an overall understanding, then coded all transcripts point-by-point in Atlas.ti[4] qualitative analysis software and developed 106 descriptive codes. Through Axial coding, we developed a codebook by looking for patterns and connections within the codes, and generated 13 groups. Figure 1 shows a sample of the codes grouped into higher-level concepts.

A research assistant used the developed codebook to conduct a second independent analysis of 10 out of 32 interview transcripts). We used Krippendorff's alpha coefficient [20] to measure the agreement of the two coders because it is sensitive to small samples, whereas Cohen's kappa assumes an infinite sample size [21]. Krippendorff [20] suggests $\alpha \geq 0.667$ as the minimum acceptable value. Our test showed moderate agreement between the two researchers' analyses, $\alpha = 0.741$. The two researchers met and resolved the coding variability by explaining their rationale for the analysis and discussed until they reached a mutual agreement. The lead researcher then re-coded the remaining interview based on the agreed

[3] https://trint.com
[4] https://atlasti.com

Province and Territory				Gender				Age Group				Level of Education				Income			
	Survey	StatCan	Interview		Survey	StatCan	Interview		Survey	StatCan	Interview		Survey	StatCan	Interview		Survey	StatCan	Interview
ON	55%	(38%)	59%	Male	49%	(49%)	50%	18 to 19 years	4%	(N/A)	0%	No high school	1%	(12%)	3%	<$15k	6%	(21%)	0%
BC	16%	(13%)	19%	Female	50%	(51%)	50%	20 to 29 years	42%	(13%)	22%	High school	18%	(24%)	6%	$15k-$34k	16%	(30%)	16%
AB	12%	(12%)	13%	Non-binary	1%	(N/A)	0%	30 to 39 years	36%	(14%)	50%	College	14%	(22%)	19%	$35k-$74k	34%	(33%)	31%
NS	6%	(3%)	6%					40 to 49 years	10%	(13%)	13%	Bachelors or higher	64%	(29%)	66%	$75k-$149k	31%	(14%)	38%
MB	4%	(4%)	3%					50 to 59 years	4%	(15.0%)	9%	Other Professional	2%	(11%)	6%	$150k-$199k	4%	(2%)	6%
SK	3%	(4%)	0%					60+ years	3%	(23%)	6%	No answer	0.3%	(N/A)	0%	>$200k	2%	(2%)	6%
NL	1%	(2%)	0%													No answer	6%	(N/A)	3%
PE	1%	(0.4%)	0%																
NB	0.7%	(2%)	0%																
QC	0%	(23%)	0%																
YT	0.3%	(0.1%)	0%																
NT	0%	(0.1%)	0%																
NU	0%	(0.1%)	0%																

Table 1: Participant demographic information for the survey and interview study. Survey demographics are compared to national averages from Statistics Canada's most recent census data (in brackets).

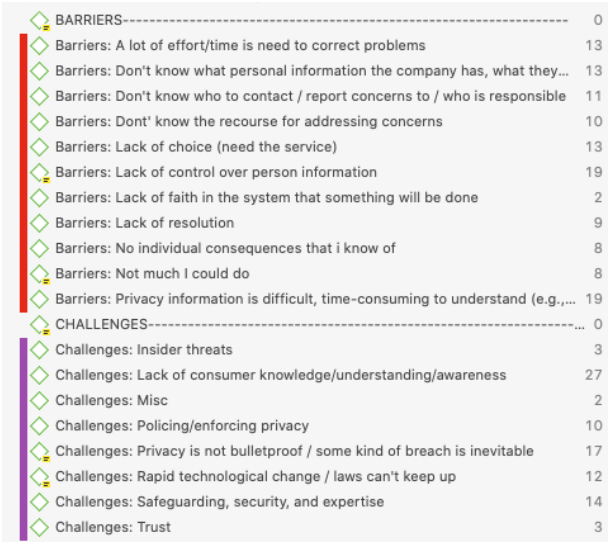

Figure 1: A subset of codes used in the open coding process in Atlas.ti. The codes are grouped into related concepts based on the axial coding process in the format "Concept: Code".

analysis. Lastly, we used Selective Coding to integrate results into a theory unifying core themes and grounded in the data.

4 Survey Results

The majority of participants owned at least two types of internet-connected devices. Desktop, laptops, and mobile phones are the most common (99%), followed by tablets (70%), gaming consoles (68%), and smart media devices (65%). Less than half owned home assistants (42%), wearables (37%), and smart appliances (37%). Some have a car with a smart system (19%) and home security systems (12%); few have internet-connected toys, monitors, and trackers (8%), and medical health monitors (3%).

4.1 Technology's impact on privacy

Only 36% rated their knowledge of how these technologies affected their privacy as good or very good. As summarized in Figure 2, participants felt they had poor knowledge about how new technology like home assistants, smart devices, and smart cars, and other connected devices affect their privacy. Even though they reported having highest knowledge about how desktops and laptops, followed by tablets, home security systems, and mobile phones affect their privacy, participants were not very confident about these either.

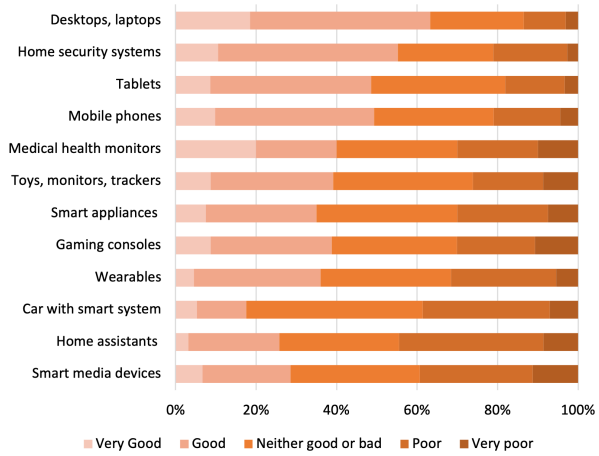

Figure 2: Self-reported knowledge of how to protect personal information across a variety of devices.

4.2 Information management practices

As summarized in Figure 3, participants reported being diligent in applying some information privacy management practices while neglecting others. We note that these are self-reported behaviours. Therefore, they may not fully reflect actual behaviours. Participants believe themselves to be most diligent in avoiding sharing their Social Insurance Number (SIN), exercising safe password practices, downloading files from reputable sources, and installing the latest software updates. They reported being less attentive about using encryption and disabling Wi-Fi and Bluetooth when not in use and when moving through public spaces. More than half would withhold sharing optional information, but less than half think about why their data is needed, who will use it, and how it

Scenario	Description	Compliant	Principles
S1-outsourcing-abroad	Your email provider notifies you that your email subscription will be outsourced to the US. You will be asked to accept or decline the new services upon login to your new account.	Yes	Accountability; Consent
S2-GPS-tracking	Your telecommunications employer notifies you that they will begin tracking your location via Global Positioning System (GPS) on company vehicles to manage workforce productivity, safety, and company assets.	Yes	Identifying Purposes; Consent; Limiting Collection; Limiting Use; Safeguards; Openness
S3-opt-out-consent	Your cellular provider notifies you by mail that the company intends to use customers' personal information for secondary marketing purposes. You could have your name removed from the marketing list by contacting the company; otherwise, it will assume your consent.	Yes	Consent
S4-over-collection	You are asked for your personal identification information (Utility bill and driver's licence) for the purpose of verifying your identify for receiving a free $10 gift card.	No	Accountability; Consent; Limiting Collection; Openness
S5-amending-consent	You receive a notice from your bank that its changing their policy to use your personal information for the secondary purpose of marketing. The notice outlines who would have access to customers' personal information and how to withdraw your consent.	No	Consent
S6-identify-theft	Your personal information was used by a fraudster to open a credit card account using your personal information, and your bank assumed the financial loss for the account balance	No	Accuracy; Safeguards
S7-safeguarding-data	A connected toy manufacturer, of which you are a customer, notifies you that they are improving security after a data breach resulting in the potential compromise of you and your child's personal information.	No	Safeguards
S8-openness-of-collection	You are asked to create a User ID and provide your credit card information to access online services from a well-known technology company to download a free app. Instructions for downloading without providing the information is posted in the website's support section.	No	Identifying Purposes; Limiting Collection; Openness
S9-accessing-password	Your request to directly access your login-related information (date, time, and IP address) from a web-based company after suspicious password reset is denied based on the explanation that only law enforcement can have access, not clients.	No	Accountability; Safeguards; Individual Access; Challenging Compliance
S10-challenging-exceptions	Your physician refuses to provide your insurance company his personal notes after your medical examination because he claims it is not part of your official medical record.	No	Individual Access

Table 2: Scenario descriptions (condensed version) and the relevant privacy principles. The OPC ruled the first three scenarios compliant with PIPEDA and the rest in violation.

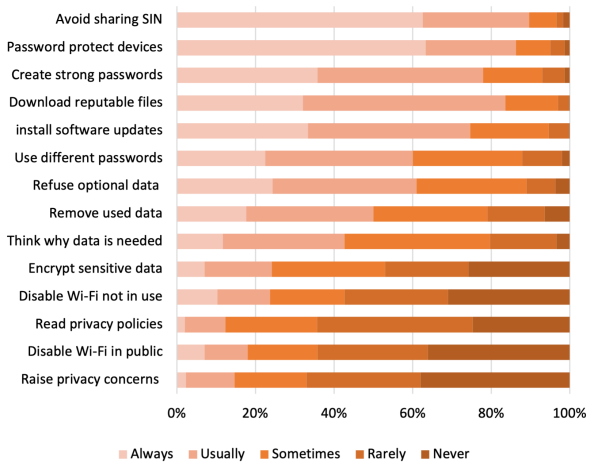

Figure 3: Self-reported information privacy behaviour.

would be used before providing it online. Unsurprisingly, many participants do not read privacy policies. Only half said they would remove their personal information when they no longer need the product or service. Even though 67% of participants indicated that they are concerned about their personal information held by companies, few said they would raise a privacy concern if companies mishandled their personal information.

4.3 Awareness of privacy rights

Only a third of participants indicated that they have good knowledge of their privacy rights (29%) and how to protect those rights (37%). This overall low level of knowledge is reflected in the low awareness of how businesses manage their personal information. Most participants are aware of the information management practices for only some or none of the services and products that they use. We used Friedman's Analysis of Variance to determine how their awareness differed across the eight types of data management practices (Figure 4). We found an overall statistically significant difference between perceived awareness of different practices ($\chi^2(8) = 559.987, p < .0005$). Pairwise comparisons with a Bonferroni correction for multiple comparisons revealed a statistically greater perceived awareness for *what is collected*, *why it is collected*, and *how it is collected* compared to the other practices.

4.4 Applying FIPs

We first asked the participants whether they felt the scenario were likely to happen in real life to ensure that our selection of scenarios was relatable. Over 75% of participants agree that the majority of scenarios (S2-S3, S5-S8) are likely to happen. Over half of participants agreed that the remaining

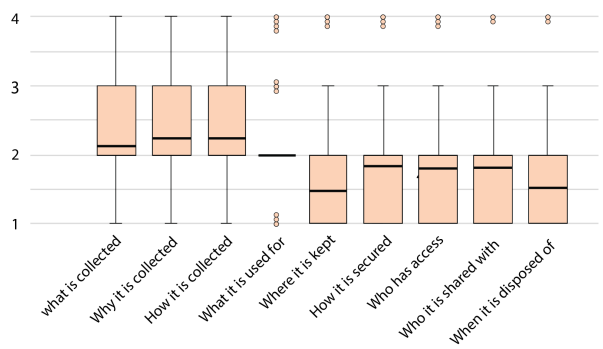

Figure 4: Perceived awareness of ways businesses manage personal information for services and products currently used; Likert scale responses: 1 = none, 2 = some, 3 = most, 4 = all

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
Accountability	58%	54%	48%	51%	47%	82%	81%	51%	60%	44%
Identifying Purposes	35%	65%	58%	81%	65%	44%	32%	55%	33%	40%
Consent	74%	55%	81%	66%	77%	39%	24%	52%	46%	47%
Limiting Collection	34%	49%	42%	64%	42%	23%	41%	54%	32%	41%
Limiting Use	43%	47%	48%	62%	46%	26%	36%	42%	44%	49%
Accuracy	15%	34%	18%	19%	18%	56%	14%	19%	19%	25%
Safeguards	41%	42%	26%	47%	43%	79%	81%	36%	61%	27%
Openness	58%	55%	56%	47%	57%	31%	47%	55%	32%	50%
Individual Access	45%	40%	35%	33%	37%	45%	28%	33%	53%	59%
Challenging Compliance	40%	32%	25%	32%	38%	38%	26%	31%	46%	43%
Don't know	11%	7%	4%	3%	9%	3%	5%	11%	9%	13%

Figure 5: Percentage of participants who applied the FIPs to each scenario (S1-S10). The blue scale represents the principles used by the OPC in its official case interpretations. Darker cells represent a higher percentage.

three scenarios were likely (55% to 68%). After reading each scenario, the participants selected the FIPs they thought would apply to the situation. Figure 5 summarizes the percentage of participants who selected each principle per scenario compared to the OPC interpretations. Our participants generally over-applied the principles to privacy situations. This may be because they have insufficient understanding of the principles, or insufficient detail to appreciate the scenarios' nuances fully. We would not necessarily assume that a layperson would have perfect alignment with the OPC, but these responses give a general sense of their interpretations. Laypersons' misapplication of the FIPs (compared to regulators) suggests that consumers (i) have misconceptions of their privacy rights and (ii) have low efficacy to hold organizations accountable for privacy violations.

5 Interview Results

This section reports our qualitative findings regarding participants' understanding of personal information and how Canadian privacy laws protect consumer privacy. We recorded the frequencies during data analysis to help with identifying trends, but deliberately avoided reporting numbers in the paper, as is recommended for inductive approaches like Grounded Theory [16]. Instead, we use descriptive language (e.g., most, some, few, none) where appropriate. Supplementary interview results that are not central to our research question are included in Appendix C.

5.1 Canadian privacy protection

Most participants admitted to being "unaware of what privacy laws are and what is required of companies" or unclear about the "specifics" of what the law says, but "do know that there are laws in place." P5 explained,

> *I don't know the letter of the law and what the laws specifically are, but my gut feeling is that privacy or personal information probably isn't super well protected... because so much information gets put onto the Internet... I don't doubt that there are laws in place that try to protect that as much as possible. I just see it kind of as an inevitable thing that information will leak out one way or another. (P5)*

5.1.1 Effectiveness of existing privacy laws

Participants' overall consensus is that the law offers "weak", "ineffective", and "unregulated" protection. Some preferred other "hardcore" international regulatory bodies like the European GDPR. P5 explained, *"I think of what I read, the [Canadian] laws... sound really good. I just doubt whether they are put into place in a way that actually protects information."* P7 also believed not enough is being done: *"I don't know if that's from a lack of [laws], you know, how the requirements are written or if it's on the side of them enforcing the rules. It feels like not enough is being done. I don't know exactly why or where that is."*

Some believe businesses do their best to protect consumers' information, but it is not *"bulletproof"* (P2). *"Generally"*, said P20, *"I'm assuming [companies] have security systems in place... because of the idea if something was breached and something leaked out, it would be bad publicity for that company. So I think they're trying to do as best they can."*

Another group believed businesses have no incentives to protect consumer privacy because *"information and data are hugely profitable for companies"* (P1). Because information is valuable, it is *"in their financial best interest to obfuscate what they're collecting"* (P7).

Others simply "don't know" whether companies provide reasonable protection. P4 declared, *"I feel like I don't necessarily have enough understanding of how our information is being used... so I'm not sure I have an opinion on like what... because I don't really know what is a reasonable level of privacy... and what companies are doing right now."*

5.1.2 Responsibility for reporting privacy violations

The majority believed that the affected individuals (e.g., consumers) *"who felt that their privacy was violated"* (P5) are responsible for reporting concerns *"to the proper channels and take care of the problem"* (P2). Unfortunately, none of our participants could clearly identify the "proper channels" or who is accountable for businesses' compliance.

These participants internalized privacy violations as something that happens to them personally, and therefore they should be responsible for reporting. When asked about why consumers should report privacy concerns, P18 thought is it because *"[consumers] are the only ones that are concerned about our privacy... The companies are not going to bring it up... unless it involves a lot of money... and reaches the news."* Another believed the *"onus [is] on people to be to help themselves be informed about things... [otherwise] you're susceptible to being taken advantage of... and people using your information in an unethical way"* (P21).

The most common recourse is to report concerns directly to the business, but some also believed it is their responsibility to report to government agencies because *"the government wouldn't know unless you report them"* (P13). Many participants assumed the existence of a federal authority and government agency like a "privacy commissioner", "better business bureau", or "ombudsman", but none of the participants were aware of the process for reporting. *"I don't even know who to go to,"* said P23, *"I'm sure there's someone in government that's responsible for it... it seems like an owner's task to try to figure that out and lodge a complaint that probably will fall, if I'm being realistic, on deaf ears."*

A small number of participants believed that anyone who is aware of the privacy violation, like *"conscientious employees should whistle blow if they see something going on illegally"* (P7). Few mentioned that companies are responsible for bringing privacy violations forward to the consumer or a government agency because *"they have a legal and ethical responsibility"* (P11). Ultimately, participants thought that the responsibility *"falls on the consumer"* (P21) because *"your rights aren't really protected without you having to go out and do something on your own"* (P13).

5.1.3 Challenges for consumer privacy protection

Our participants identified four main challenges (C1–C4) for consumer privacy protection.

C1. Lack of awareness: Even though most participants believed consumers are responsible for reporting privacy violations, they also did not know how to address privacy concerns. For example, P11 had not raised any privacy concerns with companies because

> *I didn't know who I should raise that concern with. Should I bring it up with the company... send them an email... send it to some sort of privacy watchdog organization in the country? So I didn't raise a concern, but it wasn't because I didn't have a concern, I just didn't know what to do. (P11)*

Many participants felt that they lack awareness of the ramifications of information disclosure. P18 declared, *"the general population are... not aware of what not to provide to the companies,"* P11 elaborated,

> *As a Canadian consumer, there are so many things that, you know, I'm guilty of signing up for. I really have no clue what information [companies] have on me and how they're using it... It's not something that's clear to Canadians where to look, what they should advocate for. What's a reasonable expectation of information to give up? What's unreasonable? (P11)*

On the enforcement side, P31 admitted, *"I don't really know what the government does to ensure that information is being stored correctly and securely, or even collected lawfully. My perception has always been that it's the sort of thing that only gets dealt with when a problem comes up."*

The problem is that *"Canadians are not educated enough on the privacy laws that are available to protect their information,"* said P22. As one possible solution, our participants suggested more public awareness about the resources available. For example, *"finding out about the [privacy] commissioner of Canada that I didn't even know existed before now"* (P9).

C2. Enforcing privacy laws: Policing consumer privacy is a daunting task because of its "breadth" and "scope". *"Consumer privacy can be violated in so many different ways,"* explained P25, *"[it's] impossible to police every single application, every single website out there to see whether or not they're complying with whatever laws have been put in place."* Most participants recognized that many of the products and services they use operate in the United States or other countries: *"So many companies operate internationally that it's easy for some companies to sort of skirt around that... a company bases their servers in Thailand... whether a Canadian can enforce any sort of laws on that company is really questionable"* (P25). Therefore, privacy enforcement is viewed as *"an issue of scale with the incredible amount of data compared to... the limited resources of the government"* (P7). Enforcement is viewed as one of the *"biggest steps aside from the law itself"* (P14).

As a result of poor enforcement, our participants believe firmer laws with harsh penalties for non-compliance should be put in place, and they frequently used GDPR as an example of the type of enforcement they would *"like to see in Canada"* (P4). Highlighted protections included the right to permanently delete information and the right to refuse to provide information. If a company *"break the rules... they can get fined"* (P18). Some viewed these protections as *"what a company should have been doing already"*, but implementing the rules would *"force a lot more companies to adopt better privacy practices"* (P32).

C3. Rapid technological change: Our participants identified the reality that *"technology is evolving, and the law*

doesn't keep up" (P27). The "technology" mentioned include artificial intelligence, personal home assistants, and other "smart" devices. *"we're not even sure how to legislate for [these technologies]"*, said P10, *"because... they're still under development."* P11 elaborated:

> *The limitation to protecting [consumer privacy] is the pace of change. I think it outpaces how quickly governments can respond and implement laws and policies... by the time [laws] roll out and by the time new technologies or new areas that affect privacy take place, there's often a lag period before policies are made. (P11)*

This group recognized that the online space is *"the most difficult place to protect Canadians... "If we were to be a hundred percent protected"*, retorted P31, *"[the government] would have to be passing new laws every day."* Consumers' lack of awareness for protecting their privacy is partially due to *"the combination of this old and new technology and people's [lack of] understanding of how it works and what they need to do"* (P27).

Our participants are unsure of how to "fix" privacy concerns under existing and new technology, but instead recommend improved usability and access to privacy resources, tools, and information to keep consumers better informed about their data. Suggestions included displaying information in "more accessible" and "user-friendly" formats. For example, reducing lengthy privacy policies to succinct summaries or short videos. From a utilitarian perspective, some envisioned more accessible ways to find their personal information held by companies in a centralized database where *"I could access which companies have information on me and how long are they able to hold it for"* (P11).

C4. Hackers: "Hackers" from both outside and inside companies (e.g., malicious employees) were seen as a significant threat and limitation in protecting consumer data. Companies *"try the best they can,"* explained P2, *"they try to encrypt it, they try to protect it, but there's always someone that can get their hands on [the data], [and] you can never find out who this person is."*

In the face of a data breach, some believe it is *"not really the company's fault that the leak even happened"* (P2). Hackers *"who want your data are willing to go to extreme lengths to get it... trying to stay one step ahead is difficult if not impossible task for a lot of companies, especially medium to small companies"* (P23). Staying ahead of the hackers is an arms race: *"[companies] got to stay one step ahead of the hackers... [It] requires them hiring people that would be hackers... It's kind of like hackers against hackers trying to stay one step ahead of people trying to steal the data"* (P13).

Part of the problem is the lack of security expertise to safeguard consumer data. For example, P3 said, *"small business owners, they start up a website and they take credit card payments through it, but they don't make sure that their website is secure."* Some believed a lack of security expertise to protect against data breaches is not unique to small companies. P27, a part-time auditor, declared to *"have both identified and read about audit findings that are simply mind-boggling, not for small organizations, but for Fortune 500 organizations... Organizations believe they are secure, but in reality they have huge cracks in their security walls."*

Since most believe it is impossible to completely safeguard against hackers, companies should simply *"do everything that they can... to ensure that it's harder for people to break into their system"* (P9). These participants believe it is in the companies' best interest to safeguard consumer data against hackers to uphold their reputation and *"continue to have a good name"* (P12).

6 A moral code for data privacy

We found that participants do not rely on legal guidelines to determine whether what companies do with their data is appropriate. Instead, they weigh the severity of the violation against their own 'moral code' centred on what they feel is right and wrong. Legally compliant conduct is not necessarily interpreted as ethical and moral, nor as protective of the autonomy and privacy and consumers. P21 clearly describes the boundary between legal and ethical conduct in response to the scenario *S8-openness-of-collection*:

> *Do I think that they acted appropriately under the law? I'm hard-pressed to say it's illegal. I mean, I could be wrong on that one, but I don't think that they're being particularly ethical. You know, the fact that you have to kind of jump through hoops to be able to not provide your credit card information for something that's free, that's a little concerning to me... I don't like the optics of it, but are they being unlawful by asking for your credit card information, even for free stuff? To my knowledge, I don't think it's unlawful. (P21)*

Our participants repeatedly identify this boundary between legal and ethical as the "grey zone" where the companies' actions could be technically legal but unethical. As P6 explained in response to S1-outsourcing-abroad: *"I think that's a bit of a grey zone... I think what they did is a kind of a grey area where they can't really be prosecuted or have anything really done to them. I think they acted accordingly, I want to say, but I really don't approve of it."* This 'grey zone' our participants described is based on their perceptions that laws, by definition, are vague with many loopholes that businesses could take advantage of:

> *Just because the law can be vague. I think that it's written that things need to be transparent, and technically [what they did] does fall under the definition of being transparent. Now whether it's moral is a whole other story. I think they've found a loophole in the wording of the law that makes it advantageous for them. They'll end up with more people on their marketing list if they do it the way they're doing it... (P3)*

.

Pillars	Moral Code	Sub-Codes
I	Trust	Intuition, Reputation, Size, Security Expertise
II	Transparency	Honesty, Purpose, Best Interest
III	Control	Choice, Consent
IV	Access	Access, Usability, Recourse

Table 3: The components of the moral code

This sets the stage for the last step of our Grounded Theory analysis. We propose that participants' understanding and perspective follows a "moral code" for data privacy. We based our model on the identified codes, patterns, and relationships between concepts identified in the analysis. We refined the results into four core values that consumers use to navigate their information disclosure: trust towards the organizations, transparency of the organization, feelings of control over personal information, and access to privacy information. We summarize the components of the moral code in Table 3. Participants' responses to the ten privacy scenarios from Table 2 offer examples of the moral code in practice.

6.1 Pillar I: Trust

Trust towards companies strongly influenced our participants' perceptions of whether the companies' privacy conduct was appropriate, with some participants weighing privacy decisions entirely based on trust towards the business.

Intuition: In judging privacy violations, participants relied primarily on their gut feelings towards a situation. For instance, P5's response to *S1-outsourcing-abroad*,

> *I feel really uncomfortable about that situation because it feels like they're holding your data hostage and switching you from the country with laws that you initially signed up for... to a whole different system that you might not be familiar with. I would assume that they're following the law because at least they're informing you... (P5)*

Participants used words like "red flag", "creepy", "sketchy", "annoyed", "sneaky", "uncomfortable", and "suspicious" to describe questionable conduct. P6 admitted: *"[the situation] just seems kind of sketchy to me. You know, it's not a very academic term... but it kind of rubs me the wrong way."*

Reputation: We avoided naming specific companies in the scenarios, but some participants indicated that their attitude towards a privacy violation would depend on the business. For example, in response to *S1-outsourcing-abroad*, P2 explained that they wouldn't be concerned if the company was Google because *"They're reputable,"* while others expressed distrust if the business was Facebook under the same scenario. Similarly, in *S3-opt-out-consent*, P3's interpretation of whether the business acted appropriately under the law would *"depend on my company." "If it were a reputable company,"* continued P3, *"I wouldn't be concerned... [If it's] a brand new cell phone company, I would be a little bit concerned because they don't have the reputation... to protect my data."*

Some participants defaulted to trusting reputable companies. P31 explained, *"I deal with companies that I believed to be reputable. So I would assume that they're following the rules and the regulations and doing things properly... I assume they're not breaking the law."*

Size: Our participants perceived larger companies to be more trustworthy. P2 explained: *"Bigger companies just have a standard to live by... "* Others shared similar opinions, such as *"a large company... would know better"* (P8). They believed that larger companies have *"a human resource person or someone who's appointed to deal with privacy and legal issues,"* and are, therefore, *"better informed than a small [company], who may not have the staffing to deal with [privacy and legal issues]"* (P8). Smaller companies may be *"not be as compliant... [because they] just don't have the professional expertise to know what the law is exactly"* (P8).

Security expertise: Some participants also believed that small to medium-sized companies lack security expertise for protecting data against hackers. This is because *"even experts have to continually keep up with hackers who are, you know... have a lot of incentive and they may be very well educated and capable people, more so than the actual people who were dealing with the security for the company... only the largest companies with deep pockets could afford to get an adequate level of security"* (P8). These participants shared the view that even though they may not like the idea of sharing certain information with businesses, they felt more at ease with sharing their data with large companies because they perceived them to be better equipped to protect their data. P21 explained in response to scenario *S8-openness-of-collection*:

> *The fact that you said that it's a fairly well-known company asking for the information, I feel fairly safe that they're going to protect my personal information. I mean, ultimately, any company is going to be at risk of being hacked or having their information taken from them. But I usually feel a lot safer when it's like a big company versus it being, you know, someone smaller like fly-by-night. (P21)*

Participants thus believe that privacy protections and standards vary significantly across different organizations, and they generally placed greater trust in larger companies.

6.2 Pillar II: Transparency

Whether a business is transparent and forthcoming about its conduct influenced our participants' assessment of the severity of privacy violations and their acceptance of an organization's privacy practices.

Honesty: Being honest and forthcoming were identified as essential values. Obfuscating privacy-compromising practices is viewed as dishonest and unethical. In P12's words, *"I feel like it's dishonest. I don't think it's the most ethical thing. I think companies are always out to sort of serve their own*

interests. And if it's not in their interests for you to be aware of all that information, they're not going to make it always easy for you to find." P23 described the concern further in *S8-openness-of-collection*, *"[the company is] hiding important information in spots where, you know, vulnerable, uneducated, unknowing people would never [look], would never see... I think that's sleazy... why hide that information?"*

Many of our participants were willing to forgive certain types of misconduct if the organization is honest about it. For example, in the event of a data breach in *S7-safeguarding-data*, many participants believed that the recovery effort is redeemable because the business did not try to cover up the breach. P4 explained, *"security breaches happen. So I wouldn't fault them for the actual security breach. If afterwards, they do everything to try and deal with the breach appropriately, then that's fine..."*

Purpose: Participants showed greater comfort and acceptance towards data collection if they understood and agreed with its purpose. For example, in *S2-GPS-tracking*, most thought it reasonable to track company vehicles because they are the company's property and not an employee's private space. Hence it was not considered an intrusion of privacy.

From a legal perspective, the business in *S4-over-collection "said what information they needed, explained what they're going to do with it, and [said] they're not going to keep it past that time... which keeps all within the guideline"* (P32), but our participants felt uneasy about *"whether [the company] actually needed that information in the first place"* (P32). *"A grocery store doesn't need my driver's license number or utility bill for... confirming who you say you are"* (P24).

Best interest: If a business has acted with the consumers' best interest in mind, our participants view the actions as ethical. In the case of being denied access to online accounts, P21 said, *"I've had that issue with an e-mail address being hacked previously... and jumped through a whole lot of hoops to get [my] account back... they ask for a lot of information that maybe shouldn't be necessary. But ultimately, I think they're trying to protect the consumer. They're trying to ensure that you are actually you."* In a similar situation in *S9-accessing-password* where the business denied the individual's access, our participants rationalized that the business acted responsibly from an ethical point of view. *"It sucks that I have to jump through all these hoops to get my answer"*, responded P22, *"but it sounds like they're doing a better job of respecting and looking after my data."* P31 agreed, *"seeing that I tried to get information from them and they said 'no'... I'd probably actually feel better about it. So I'd change my password and wouldn't feel concerned."*

6.3 Pillar III: Control

Our participants felt that they lacked control over their personal information once a company collects it. For example, P28 said in response to *S4-over-collection*, *"I just have this feeling that once you send this information, you really have no idea what they're doing with it. Like they're saying they're going to do that. But you have no idea what actually happens to it after."* P22 agrees, saying that *"Once you enter [your information] it goes to this kind of black hole of not knowing... What do they do with it? You're kind of at their leisure, at their discretion."*

Choice: When asked about why they would give their personal information when feeling uneasy doing so, our participants identified a lack choice for the services and products they need as one of the main reasons. P1 explained, *"I don't even know if I'm on any Canadian servers because most of the stuff we use is in the US and beyond... I don't know the alternatives. I mean, if I went looking for Canadian alternatives to the services I use, I suspect I wouldn't find that many [laughs]."* P1 continued, *"you gotta pick the Apple or Microsoft or Google these days because it's pretty much the 3 things that make devices and software to put on them,"* P7 complained, *"You sort of need to sign away your rights to be able to do things."* Our participants felt cornered when organizations try to provide the perception of choice and control over personal information. In *S1-outsourcing-abroad*, P5 felt *"they're holding your data hostage"* if the customer does not agree to the terms. These participants felt uneasy giving away their information but believed they had no other options. In the words of P11, *"I kind of went into a spot where I didn't necessarily have an alternative option, so I complied, but I just kind of didn't like it."*

Consent: All participants agreed that obtaining consumers' consent before data collection is the basis of lawful conduct. Several participants held the view that consent should always be explicit. "Opt-out" consent was viewed as being unethical practice. P23 explained in response to *S3-opt-out-consent*:

> *I don't know if the law is an "opt-out" or an "opt-in" type of law, but... but I don't think they acted ethically... It shouldn't be like, hey, if you don't want this, then you have to do, you know, jump through the hoops in order to make sure that you don't want this. It should be. Hey, if you want to be included, give us a call... and [opt-out] is not the way that consent works, nor should it work that way. (P23)*

Similarly, in *S5-amending-consent*, P19 felt the business should *''get the confirmation from customers that they feel comfortable with [the changes in the terms and conditions] rather than letting them know that, you know, we're [already] doing that."* Consent should, therefore, be *"brought about by the individual, and the individual should be the one to make the decision–full stop"* (P23).

6.4 Pillar IV: Access

Our participants wanted *"a better sense of accessibility of [their] data"* (P5), including access to how companies manage their personal information, more usable privacy informa-

tion, and clear recourse for addressing privacy concerns.

Access: Our participants identified that they lack access to details about how companies handle their personal information, what information companies have about them, where their data is stored, how long the data is kept, and when it gets destroyed. P8 recounted their experience requesting access to personal data:

> *I have in a couple of instances tried to contact companies about what information they have about me, and had some positive replies in terms of they've given me the information, sent me the information, or said that they would delete the information. Although I can't guarantee that it's gone. At least, they said they would. I have also received no response from some places, in which case I assume that they're probably not deleting it. And then also there's the case of companies that go under and you can't... I tried to contact [a company] that I knew had quite a bit of information about me and they're gone, but it doesn't mean their databases are gone. If a company goes bankrupt or something. I think in many times in a lot of those things are just ignored. So where are they kept? Where's the servers, and what happened to them? Did anybody ever delete it properly? Did the hard drive just get thrown into the garbage somewhere? (P8)*

In response to the scenario *S7-safeguarding-data*, P9 raised the concern that *"we have no idea what's happening with our information. The only time that we ever find out... that something is wrong is when there is a big announcement that the information was breached and this many customers were affected... But apart from that... I don't feel like I know anything"* (P9). Denying consumers access to their personal information could erode trust. In *S10-challenging-exception*, P13 believe the doctor *"acted appropriately under the law, but don't think that it's right that there are notes about you that you're not allowed to see."*

Usability: Unsurprising, participants' lack of awareness is partially due to not reading terms and conditions before signing up for a service or product because they are "absurdly long". Even those who are privacy-conscious find it challenging to understand privacy policies. After experiencing a data breach, P23 said, *"I started being more aware of privacy and who I give my information to and even going as far as looking at companies policies as to their storage of user data. And a lot of it's, you know, I would say, verbose. Like it's not really clear on what they're doing with their with your data or information, you're sort of just asked to trust them unilaterally."* When responding to scenarios like *S3-opt-out-consent* and *S8-openness-of-collection*, Our participants are conscious that companies recognize that most people don't read policies and take advantage of the "loopholes" in getting users to agree to their terms and services. *"I feel like it's dishonest,"* said P12.

Recourse: While our participants realize they have legal privacy rights and that businesses are under certain obligations to protect consumer privacy, barriers exist that prevented participants from identifying and challenging a business who infringes on their privacy. For those who had raised a concern, many did not have a satisfying resolution. Several of the companies our participants contacted did not follow up to confirm whether the concern was addressed. P32 said, *"I emailed the company, and they called me, and I actually spoke to... their supervisor... they assured me they would sit down and look at their process and see if there were anything they could do... at least... they said they would (laughs), but I don't know what happened after that."* When a company doesn't follow-up, people tend to give up and *"just let it go"* (P19). Understandably, some of our participants had *"a lack of faith in the system that something is going to be done"* (P23) if they raised a concern, and they *"don't trust companies to be as accountable as they should be."* (P26) Aside from not knowing whom to report concerns to, P1 elaborated, *"as far as if they would actually do anything... like what do you do? Go to the police and tell them Facebook's not doing what you asked them to? ... There's nothing really clear beyond just going to the company and hoping they actually listen to you, which they usually don't."*

7 Discussion and future work

A commonality between many existing privacy theories is that individuals' perceptions of privacy depend on situational circumstances. Privacy regulations like PIPEDA define privacy through regulations for controlling the flow of personal information about individuals. We suggest that there exists a misalignment between privacy regulations based on FIPs and privacy theories like contextual integrity [23], organizational trust [22], Solove's Taxonomy of Privacy [35], and our concepts of Moral Codes. These works show that preserving privacy is not only a matter of controlling the flow of personal information, but also how privacy practices and norms meet individual and societal values. Our work contributes to identifying specific moral values that individuals abide by in making privacy decisions.

The Government of Canada has recently suggested changes to PIPEDA in conjunction with the Digital Charter that specifically mandates "the ethical use of data to create value, promote openness and improve the lives of people—at home and around the world" as one of the guiding principles [15]. As indicated by our results, PIPEDA's FIPs focusing on the basic technical and legal responsibilities of organizations are insufficient to address the ethical and ecological concerns that emerge and ascend to the top of minds during consumers' privacy decision-making. Our participants' Moral Codes suggest new rights and expectations for privacy, including increased access, meaningful choices, clearer information, the ability to move or remove information, and real accountability through stronger enforcement. Based on our study results, we propose the following recommendations.

Consent Model: Most participant concerns center on

PIPEDA's current model of "implied" consent that allows businesses to claim they have an individual's consent to use their information in a certain way without asking for it. For example, the cellular company in the compliant scenario *S3-opt-out-consent* could argue it has "implied" consent because they are using existing customers' information and, by signing up for the service, customers must have implied consent to receive marketing material. Our participants deemed this approach within the boundary of the law but highly unethical. This observation suggests that mismatches between corporate privacy practices and individuals' personal values were likely to be viewed as unethical. Many participants referenced the GDPR as a model they would like to see incorporated into Canadian law. An organization under GDPR must have "legitimate interests" to use personal information, such as fraud prevention. Our results suggest that this model is in closer alignment with the Moral Codes that consumers abide by, such as *Purpose* and *Best interest*. Therefore, we recommend adopting a consent model similar to GDPR's "legitimate interest" model to replace the "implied consent" model in PIPEDA.

Control and Access: Descriptions of the FIPs appeared to satisfy participants' moral expectations superficially, but in practice, they were disappointed with their weak enforcement and vague applicability to real-life privacy situations, leaving individuals powerless to control and access their personal information. For example, many participants felt "trapped" and like they had no choice but to agree to *S1-outsourcing-abroad* for fear of losing their data. PIPEDA provides "right of access" and limited "right to deletion" of inaccurate or outdated personal information. Our participants also desired stronger rights to deletion and the "right to data transfer", where they could request their personal information in an accessible and portable format to transmit it to a different organization. However, usability testing needs to be conducted on which data formats (e.g., CSV, JSON, XML) are more usable and accessible to end-users, possibly developing new human-readable formats. Other usability issues that create barriers for control and access identified by our participants, such as the presentation of privacy policies and privacy settings, could be addressed by standardizing certain key interface elements. For example, the State of California Department of Justice has released a standard "Privacy Options Opt-Out Icon" to direct users to opt-out [36].

Assessment Tools: Our results suggest participants were ill-equipped to identify privacy violations and hold businesses accountable using legal frameworks like the PIPEDA. Instead, they relied on their own moral assessment of businesses' privacy conduct based on trust, transparency, control, and access. Therefore, we suggest using the Moral Codes as a framework to develop tools that help organizations align their practices and policies with consumer expectations. For example, the Information Commissioner's Office (ICO) in the UK has developed a three-part test [40] with an ethics component to help businesses determine whether they have a legitimate interest in processing consumers' personal data.

We further propose that an independent entity such as the Better Business Bureau [9] could conduct an assessment and provide ratings for organizations on the basis of their privacy practices. Our Moral Codes could be used as one of the criteria guiding this type of assessment. This would enable customers to seek out organizations that meet their privacy expectations and may serve as incentives for organizations to improve their practices.

Despite this potential incentive, a key problem lies with how to convince corporate organizations to take these steps. Competing corporate priorities mean that there is little incentive for them to prioritize "moral" or privacy-preserving designs, and in many cases, there are significant economic and competitive disincentives. Our view is that this issue requires increased governmental regulation and oversight, and only once this is in place will there be sufficient interest in making practical changes. However, studies such as this one help increase awareness among stakeholders, and provide supporting evidence to those in positions to push for change.

Limitations: We chose to present participants with scenarios and information about the privacy principles, which may have primed them and increased their privacy concern. This was a considered methodological choice because we wanted participants to engage with the principles and provide their perspectives, but we also knew from background research that people were likely unfamiliar with the principles. Our survey opened with demographic questions Westin's Privacy Segmentation Index to compare the overall privacy attitudes from our sample to previous studies. As indicated by some studies (e.g., [43]), the Westin categories may not accurately infer behavioural intent and responding to demographic questions first could increase the stereotype threat [38]. Our work is focused on users and regulations from Canada; while we broadly think that our findings would generalize, at least to other Western countries, further work is needed to explore the unique attributes present in other parts of the world.

8 Conclusion

Making online privacy decisions is increasingly difficult due to the complexity of information technologies and the variety of activities that consumers engage with online across multiple platforms and devices [3]. Our research adds to the body of literature in understanding individual's privacy preferences and behaviours. Beyond the traditional economic view of individuals engaging in privacy benefit trade-offs, and heuristics and biases that influences behaviour, we suggest that understanding users' privacy ethics could offer rich insights into how they engage in online privacy decision-making.

Acknowledgments

Sonia Chiasson acknowledges funding from NSERC for her Canada Research Chair and Discovery Grants. The authors thank Elisa Kazan for help in data collection and Cassie Cassell for help in qualitative analysis.

References

[1] Eathar Abdul-Ghani. Consumers' online institutional privacy literacy. In *Advances in Digital Marketing and eCommerce*, pages 40–46. Springer, 2020.

[2] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: Examining user scenarios and privacy preferences. In *ACM conference on Electronic commerce*, pages 1–8, 1999.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017.

[4] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[5] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE security & privacy*, 3(1):26–33, 2005.

[6] Irwin Altman. *The environment and social behavior: privacy, personal space, territory, and crowding.* Brooks Cole Publishing, 1975.

[7] Oshrat Ayalon and Eran Toch. Evaluating users' perceptions about a system's privacy: Differentiating social and institutional aspects. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 41–59, 2019.

[8] Paula J Bruening and Mary J Culnan. Through a glass darkly: From privacy notices to effective transparency. *NCJL & Tech.*, 17:515, 2015.

[9] Butter Business Bureau. BBB start with trust, 2021.

[10] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: why, when, & what people want to share. In *SIGCHI conference on Human factors in computing systems*, pages 81–90, 2005.

[11] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[12] Curt J Dommeyer and Barbara L Gross. What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2):34–51, 2003.

[13] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *SIGCHI Conference on Human Factors in Computing Systems*, pages 5228–5239, 2016.

[14] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77:226–261, 2018.

[15] Government of Canada. Canada's digital charter: Trust in a digital world, 2021.

[16] David R Hannah and Brenda A Lautsch. Counting in qualitative research: Why to conduct it, when to avoid it, and when to closet it. *Journal of Management Inquiry*, 20(1):14–22, 2011.

[17] Lesley Jacobs, Barbara Crow, and Kim Sawchuk. Privacy rights mobilization among marginal groups in canada: Fulfilling the mandate of PIPEDA. Technical report, York Centre for Public Policy & Law, York University, 2011. https://ycppl.info.yorku.ca/files/2013/05/Privacy-Rights-PIPEDA-paper.pdf.

[18] Leslie K John, Alessandro Acquisti, and George Loewenstein. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, 37(5):858–873, 2011.

[19] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, 2017.

[20] Klaus Krippendorff. Reliability in content analysis. *Human communication research*, 30(3):411–433, 2004.

[21] Klaus Krippendorff. Computing krippendorff's alpha-reliability. *Departmental Papers (ASC)*, 43, 2011.

[22] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3):709–734, 1995.

[23] Helen Nissenbaum. *Privacy in context*. Stanford University Press, 2009.

[24] Office of the Privacy Commissioner of Canada. PIPEDA interpretation bulletins, 2020.

[25] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *SIGCHI conference on Human factors in computing systems*, pages 129–136, 2003.

[26] Robert W Palmatier and Kelly D Martin. *The intelligent marketer's guide to data privacy: the impact of big data on customer trust*. Springer, 2019.

[27] Yong Jin Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, 2013.

[28] Pew Research Center. The state of privacy in post-snowden america, 2016.

[29] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. Expecting the unexpected: Understanding mismatched privacy expectations online. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 77–96, 2016.

[30] Kate Raynes-Goldie. Aliases, creeping, and wall cleaning: Understanding privacy in the age of facebook. *First Monday*, 15(1):1–14, 2010.

[31] Marshall David Rice and Ekaterina Bogdanov. 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, 2019.

[32] Katharine Sarikakis and Lisa Winter. Social media users' legal consciousness about privacy. *Social Media & Society*, 3(1):1–14, 2017.

[33] Kim Bartel Sheehan. Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1):21–32, 2002.

[34] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, pages 989–1015, 2011.

[35] Daniel J Solove. A taxonomy of privacy. *University of Pennyslvania Law Review*, 154:477, 2005.

[36] State of California Department of Justice. California consumer privacy act (CCPA) opt-out icon, 2021.

[37] Statistics Canada. 2016 census profile, 2017.

[38] Claude M Steele and Joshua Aronson. Stereotype threat and the intellectual test performance of african americans. *Journal of personality and social psychology*, 69(5):797, 1995.

[39] S Shyam Sundar, Jinyoung Kim, Mary Beth Rosson, and Maria D Molina. Online privacy heuristics that predict information disclosure. In *SIGCHI conference on Human factors in computing systems*, pages 1–12, 2020.

[40] TermsFeed. 3 part test for legitimate interests under the GDPR, 2021.

[41] Edward Shih-Tse Wang. Role of privacy legislations and online business brand image in consumer perceptions of online privacy risk. *Journal of theoretical and applied electronic commerce research*, 14(2):0–0, 2019.

[42] Alan F Westin. Privacy and freedom. *Washington and Lee Law Review*, 25(1):166, 1968.

[43] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. Would a privacy fundamentalist sell their DNA for 1000... if nothing bad happened as a result? the westin categories, behavioral intentions, and consequences. In *Symposium On Usable Privacy and Security (SOUPS)*, pages 1–18, 2014.

[44] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12):1, 2011.

APPENDIX

A. Online Survey

The survey choices are formatted differently than what appeared in the Qualtrics survey seen by participants to conserve space.

A1 Demographic Questions

Q1. Which province or territory are you currently living in? (Choices: The thirteen provinces and territories)

(The following questions all include a "Prefer not to answer" choice.)

Q2. Which gender do you identify as? (Choices: Male, Female, Non-binary, Other)

Q3. What age group do you belong to? (Choices: 19 years and under, 20 years to 79 years in five-year intervals, 80 years and above)

Q4. What is your highest level of education? (Choices: Less than a high school degree, High school degree or equivalent, College degree, Bachelor's degree, Master's degree, Doctoral degree, Other professional degree)

Q5. What is the total income of your household per year? (Choices: Less than $15,000, $15,000 to $99,999 in $4,999 intervals, $100,000 to $149,000, $150,000 to $199,999, $200,000 and above)

A2 Westin privacy index Questions

Q6. Participants responded to the following questions with a four-point scale ranging from "Strongly Agree" to "Strongly Disagree"

1. Consumers have lost all control over how personal information is collected and used by businesses.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and business practices provide a reasonable level of protection for consumer privacy today.

A3 Survey questions

Q7. Which, if any, of the following types of Internet-connected device(s) do you have in your household?

1. Mobile phones
2. Tablets
3. Desktop or laptop computers
4. Smart appliances (e.g., gas/electric meters, refrigerators, thermostats or robotic floor cleaners)
5. Smart media devices (e.g., printers, speakers, TVs)
6. Wearables (e.g., smartwatches, Fitbit)
7. Medical health monitors (e.g., Smart continuous glucose monitoring (CGM) and insulin pens, smart inhalers, smart heart monitors)
8. Home assistants (e.g., Amazon Alexa or Google Assistant)
9. Gaming consoles connected to the Internet (e.g., Xbox, PlayStation 4 or Nintendo Wii U)
10. Home security systems connected to the Internet (e.g., SimplySafe)
11. Toys, baby monitors or GPS child trackers connected to the Internet (e.g., Hello Barbie, Furby Connect, Phillips Avent, Amber Alert)
12. Car with smart system (e.g., Audi Connect, Lexus Enform, Ford SYNC3)

Q8. How would you rate your knowledge of your privacy rights? (Choices were a five-point scale ranging from "Very good" to "Very poor")

Q9. How would you rate your knowledge of how to protect your privacy rights? (Choices were a five-point scale ranging from "Very good" to "Very poor")

Q10. In general, how concerned are you about your personal information held by businesses? (Choices were a five-point scale ranging from "Very concerned" to "Not at all concerned")

Q11. Participants responded to the following questions with a four-point scale ranging from "I am aware for *all* of the services and products that I use" to "I am aware for *none* of the services and products that I use"

1. What personal information is collected and its sensitivity
2. Why my personal information is collected
3. How my personal information collected
4. What my personal information is used for
5. Where my personal information is physically kept
6. How my personal information is protected and secured
7. Who has access to or uses my personal information
8. Who my personal information is shared with
9. after it is no longer needed

Q12. In general, how would you rate your knowledge of how these technologies affect your privacy? (Choices were a five-point scale ranging from "Very good" to "Very poor" with a "Don't know" option)

Q13. Participants rated their knowledge of how to protect their personal information on the following Internet-connected devices using a five-point scale ranging from "Very good" to "Very poor" with a "Don't know" option.

1. Mobile phones
2. Tablets
3. Desktop or laptop computers
4. Smart appliances (e.g., gas/electric meters, refrigerators, thermostats or robotic floor cleaners)
5. Smart media devices (e.g., printers, speakers, TVs)
6. Wearables (e.g., smartwatches, Fitbit)
7. Medical health monitors (e.g., Smart continuous glucose monitoring (CGM) and insulin pens, smart inhalers, smart heart monitors)
8. Home assistants (e.g., Amazon Alexa or Google Assistant)
9. Gaming consoles connected to the Internet (e.g., Xbox, PlayStation 4 or Nintendo Wii U)
10. Home security systems connected to the Internet (e.g., SimplySafe)
11. Toys, baby monitors or GPS child trackers connected to the Internet (e.g., Hello Barbie, Furby Connect, Phillips Avent, Amber Alert)
12. Car with smart system (e.g., Audi Connect, Lexus Enform, Ford SYNC3)

Q14. For each of the statements, how would you rate your knowledge regarding your privacy?
(Choices were a five-point scale ranging from "Very good" to "Very poor" with a "Don't know" option)

1. The basics of Canada's federal privacy laws
2. How the Federal Government handles my personal information
3. A business's obligations concerning my privacy and personal information
4. How to raise a privacy concern with businesses that handles my personal information
5. How to file a privacy complaint with a business to the Office of the Privacy Commissioner of Canada (OPC)

Q15. To what extent do you agree or disagree with the following statements for protecting your privacy? (Choices were a five-point scale ranging from "Always" to "Never")

1. I think about why my personal information is needed, who will use it, and how it would be used before providing it online or in person.
2. I read the privacy policies of the websites and apps I use
3. I raise my concerns with the business if I am worried about the way my personal information is being handled.
4. I refuse to provide optional personal information when a business asks me for it. (e.g., when a business asks you to provide an optional secondary phone number).
5. I remove my personal information when I no longer need the services that I signed up for (e.g., removing yourself from mailing lists).
6. I avoid sharing my Social Insurance Number (SIN) with businesses or individuals (e.g., landlords).

7. I ensure my computer, smartphone and other mobile devices are password protected.
8. On my devices, I download from reputable sources.
9. On my devices, I install the latest software updates.
10. On my devices, I encrypt sensitive data.
11. On my devices, I disable Wi-Fi and Bluetooth if I'm not using it.
12. On my devices, I disable Wi-Fi and Bluetooth when passing through public spaces with open wireless networks.
13. I create passwords that are sufficiently complex using character combinations that are only meaningful to me.
14. I use different passwords for different websites, accounts and devices.

Q16. To what extent do you agree or disagree with the following statements for protecting your privacy? (Choices were a five-point scale ranging from "Strongly agree" to "Strongly disagree")

1. I regularly review and adjust the privacy settings on my devices to limit the sharing of my personal information with businesses.
2. In general, I believe Canadian privacy laws effectively protect my privacy.

A4.1 Privacy Scenarios

(Each participant was randomly assigned to five out of ten scenarios. The order was randomized. One scenario was displayed per page).

Q17. There are privacy principles for businesses to comply with the law regarding how they collect, use and disclose individuals' personal information. The next 5 questions will include various scenarios about the privacy practises of businesses. Imagine yourself in each of the following scenarios and indicate to what extent do you agree or disagree with each statement. (Choices were a five-point scale ranging from "Strongly Agree" to "Don't know" with a "Don't know" option)

1. I think scenarios like this are likely to happen.
2. I would be concerned about my privacy in this scenario.
3. I think the business acted appropriately in a lawful manner based on the situation described.
4. Which of the privacy principles do you think apply in this situation? (The principles were displayed as a checklist)
    a. **Accountability:** A business is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these privacy principles.
    b. **Identifying Purposes:** The purposes for which the personal information is being collected must be identified by the business before or at the time of collection.
    c. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
    d. **Limiting Collection:** The collection of personal information must be limited to that which is needed for the purposes identified by the business. Information must be collected by fair and lawful means.
    e. **Limiting Use, Disclosure, and Retention:** Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
    f. **Accuracy:** Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
    g. **Safeguards**: Personal information must be protected by appropriate security relative to the sensitivity of the information.
    h. **Openness:** A business must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
    i. **Individual Access:** Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
    j. **Challenging Compliance:** An individual shall be able to challenge a business's compliance with the above principles.

A4.2 Scenario description

All scenarios are based on real reported findings from OPC's Interpretation Bulletins, linked at the end of each scenario. We shortened the case summaries and retained only the essential information in a standard format to maintain consistency and improve readability.

1. You received an email from your Canadian email provider notifying you that your email services would be operated by a business based in the U.S from now on. The email provider is informing you that your data will be used and stored in the U.S., which is subject to the laws of that country. The email states that upon logging into your new account, you will be asked to accept or decline the new services. If you decline, your email account and all its contents will be permanently deleted. *Based on PIPEDA Case Summary #2008-394*
2. You are an employee of a telecommunications company that does installation and repairs. Your employer notifies you that they are installing Global Positioning Systems (GPS) on all work vehicles to manage workforce productivity, ensure safety and development, and protect and manage assets. The GPS data will be used to locate, dispatch, and route employees to job sites. Your employer will be able to view and track the location of your vehicle in real-time and to produce reports using historical data. *Based on PIPEDA Case Summary #2006-351*
3. You receive a privacy brochure as an insert in your monthly cellular telephone bill. The brochure outlines the business's intended practices regarding the collection, use, and disclosure of customers' personal information for secondary purposes of marketing, and lists all parties concerned. The brochure also indicates that you could have your name removed from marketing lists by calling a toll-free number, sending an email, or using the business's website. If you do not notify the business of your intention to withdraw, it will assume your consent to the continued collection, use, and disclosure of personal information for the identified purposes. *Based on PIPEDA Case Summary #2003-207*
4. A business is offering you a free $10 Grocery Card to purchase items sold in their grocery stores. While registering for the Grocery Card, the business notifies you that to confirm that they are issuing a $10 Grocery Card to a single eligible person, you are required to provide a scanned copy or photo of either: (i) a current utility bill or (ii) a valid driver's licence to finish processing your registration. You are told that the information will not be used for any purpose other than to verify your eligibility and will be destroyed as soon as the verification is complete. *Based on PIPEDA Case Summary #2019-003*
5. You receive a notice from your bank that it is amending its personal information consent clause for its credit and deposit agreements. The notice explains that the amendment is to notify customers that the bank intends to use their personal information for the secondary purpose of marketing new products and services. It also includes a note about who would have access to customers' personal information. The form indicates that customers can withdraw consent by contacting the bank, although it warned that doing so might restrict the bank's ability to effectively provide products and services. *Based on PIPEDA Case Summary #2003-192*
6. You found out that a fraudster had opened a store credit card account with your bank using your personal information. The bank stated that the applicant presented false identification and completed the application form. The form included name, date of birth and SIN, which appear to have been yours. In addition, the address provided was very similar to your address. The bank's credit representative was suspicious and alerted its security department about the account. The security department of the bank made attempts to contact you by telephone using the information on file, but the attempts were unsuccessful. The fraudster used your information to obtain a store credit card and bought $9,000 worth of goods. You contacted your bank to initiate an investigation and to flag the charges as fraudulent. Your bank assumed the financial loss for the account balance. *Based on PIPEDA Case Summary #2007-381*
7. You receive an email notifying you that the server of a web-enabled toy manufacturer, in which you are a customer, was hacked. As a result, there was unauthorized access to account-related information, potentially including your and your children's personal information. The toy manufacturer undertook steps to contain the breach, mitigate the risks to individuals whose information had been compromised, and improve safeguards to minimize the risk of a future breach. *Based on PIPEDA Case Summary #2018-001*
8. You download a free app on your mobile device from a well-known technology company. You are asked to create a User ID for accessing online services before downloading the free application. The registration process includes entering your credit card information. To provide customers with instructions about how to download free applications without having to provide their payment information, the business posted the

information in the website's support section. The information could also be found by using the search term "credit card" in its website's search engine. *Based on PIPEDA Case Summary #2014-007*

9. You attempt to log on to your email account, but your password does not work and you have to reset it. This is the second time it has happened in less than a month and you are suspicious that someone is changing the password to gain access to your account. You contact the business by email, informing them of the problem and requesting access to the date, time, and IP address of the computer being used to change the password. The business replied saying that it cannot grant you access to password information because it is typically law enforcement officials or lawyers who request this information and not clients. The business informed you that if you want information regarding password changes, you would need to provide a subpoena or court order. *Based on PIPEDA Case Summary #2005-315*
10. You contact your doctor asking for a copy of a report that your doctor sent to your insurance company after a medical examination and the written notes that he took during the examination. Your doctor provided you with a copy of the report but refused to provide his notes, indicating that in his view, they did not form part of your medical record, and were therefore not your personal information. The doctor stated he would rely on two exceptions under the law to refuse access: 1) a business is not required to give access to personal information only if the information is protected by solicitor-client privilege; and 2), a business may not give access only if the information was generated in the course of a formal dispute resolution process. *Based on PIPEDA Case Summary #2005-306*

Q18. We are interviewing people about their privacy awareness and experiences. Selected participants can expect the interview to take one hour to complete via a video chat platform (e.g., Skype), and be compensated for their time. If you agree to be contacted about the interview, you will be asked to provide your Prolific ID for sending you study information. Your decision will not impact your payment for the current survey. (Choices: Yes, please email me more information about the follow-up interview, No, I do not wish to be contacted.)

B. Interview

B1 General questions

Q1. What is your definition of "personal information"?
Q2. How do Canadian privacy laws protect the rights and privacy of consumers regarding the collection, usage, and disclosure of their personal information by companies?
Q3. In general, do companies provide reasonable protection for consumers' privacy? Why or why not?
Q4. In general, do existing laws provide reasonable protection for consumers' privacy? Why or why not? Are there any extra protections that you think should exist?
Q5. How did you learn about Canadian privacy protections? Have you ever gone looking for more information about privacy protections? If yes, why did you decide to do this? Did you find what you needed?
Q6. Whose responsibility is it to report privacy concerns/complaints against a company? Who should it be reported to?
Q7. Have you ever had a privacy concern or complaint against a company? If so, what happened? What did you do? What would you do if you had a concern/complaint tomorrow?
Q8. What are the biggest challenges with protecting consumers' privacy?

B2 Privacy Scenarios

The participants were read the same scenarios they responded to in the survey. See Section A.4.2 Scenarios for the description.

- Do you think the company acted appropriately under the law based on the situation described? Why or why not?
- Would you be concerned about your privacy in this scenario? Why or why not?

The participants also answered the following questions corresponding to the scenarios.

- **Scenario 1**. Do you have an example of a time when a company stored your data outside of Canada (e.g., in the US or another country)?
    a. Were you concerned? Why or why not?

- **Scenario 2**. Can you think of a time when a company did not provide a clear explanation about why they were collecting your personal information?
    a. Can you describe what happened?
    b. Did you provide the information anyway? Why or why not?
- **Scenario 3.** Can you think of a time when you felt concerned about the way that a company is obtaining your consent for the collection of your personal information?
    a. Can you describe what happened?
- **Scenario 4.** Can you think of a time when you felt that a company collected more information about you than it was necessary?
    a. Can you describe what happened?
    b. Did you provide the information anyway? Why or why not?
- **Scenario 5.** Can you think of a time when you felt concerned about a company changing its privacy policies to something different than what you initially consented to?
    a. Can you describe what happened?
- **Scenario 6.** Can you think of a time when a company used inaccurate or outdated information about you?
    a. Can you describe what happened?
    b. Were there consequences?
    c. What did you do to improve the situation?
- **Scenario 7**. Can you think of a time when your personal information held by a company was potentially compromised due to a security breach?
    a. Can you describe what happened?
    b. Were there consequences?
    c. What did you do to improve the situation?
- **Scenario 8.** Can you think of a time when you had difficulties finding certain information about a company's privacy practices relating to your personal information?
    a. Can you describe what happened?
- **Scenario 9.** Can you think of a time when you had difficulties accessing your personal information held by a company?
    a. Can you describe what happened?
- **Scenario 10.** Can you think of a time when you raised a privacy concern with a company?
    a. Can you describe what happened?
    b. Did the company address your privacy concern?

C. Supplementary Results

We first identified five salient descriptions of personal information:

1. **Something that I am:** A group of participants described their biological, intellectual, and cultural makeup as their personal information. This included demographic, health, and medical information. Some stated personal beliefs and interests (e.g., political/religious beliefs, hobbies). Few mentioned biometric information.
2. **Something that I use:** Others believed that personal information is extracted from documents issued to a person. It included government-issued ID, contact information, and financial information (e.g., credit card). A person's name, username, and passwords also fall into this category. Participants believe they should carefully protect *this* information against identify theft and fraud.
3. **Something that I have done:** Some described information gathered through online behavioural tracking methods (e.g., browsing history, location data) as their personal information. Participants with this model were aware that organizations use this information to create tailored content like targeted ads.
4. **My "private" information:** Some equated "personal to "private" and included any information that is not disclosed publicly by choice. It is described as "anything pertaining to myself that's not obvious or publicly available" (P5); "things that normal people can't just look up [on Google]" (P6); "anything that happens… in my house" (P21), and "something you wouldn't know unless you were me or a close family member" (P23).
5. **Like a montage:** A few participants believed that seemingly insignificant details about a person could become personal information when pieced together. For example, "a male in a particular setting who makes a certain amount of money\dots and those individual pieces may not be\dots strictly personal information, but all placed together, they become identifiable" (P7).