Understanding the Information Privacy Concerns of Digital Contact Tracing Application Users

Ashkan Rostami
Concordia University
Ashkan.rostami@mail.concordia.ca

Mohsen Farhadloo
Concordia University
Mohsen.farhadloo@concordia.ca

Rakesh Bishnoi
Concordia University
Rakesh.bishnoi@concordia.ca

Abstract

Given the anticipated instrumentality of digital Contact Tracing Applications (CTAs) in tracing the sources of infectious diseases, such applications have not been widely adopted by the general public. One major barrier to the diffusion of CTAs is public concerns about the privacy of their information. In this study, we first measured the attitudes of Canadians toward the nature of information privacy. We then distinguished and measured general and specific information privacy concerns of Canadians to better understand such concerns in the context of CTAs. Finally, we explored the potential associations between participants' attitudes toward information privacy and their major information privacy concerns. Our results shed light on the relative importance of various types of information privacy concerns in general and in relation to CTAs, and how such concerns might be affected by one's attitudes toward information privacy.

Keywords: Information Privacy Concerns, Contact Tracing Applications, Information Privacy Attitudes, Technology Acceptance

1. Introduction

With the advent of new digital technologies that collect data from users, information privacy has become a social concern in many contexts (e.g., Benigo et al., 2020; Oyibo et al. 2022). Such concerns are particularly prominent when it comes to the collection of highly personal and sensitive data such as health-related information (e.g., Angst & Agarwal, 2009). The outbreak of the Covid-19 pandemic re-surfaced the importance of using digital technologies in the health-care sector but at the same time raised concerns about the privacy of user's personal information (e.g., Kreps et al., 2020; Oyibo et al. 2022).

During the outbreak of infectious diseases, such as the COVID-19 pandemic, digital technologies can be utilized to track the sources of the infection, which in turn can contribute to curbing further spread of the virus. Traditionally, manual contact tracing (i.e., public health agents identifying and contacting those who have been in close proximity of an infected case) has been used in these situations. In the case of the COVID-19 pandemic, however, it was realized that manual contact tracing was not sufficient (e.g., Ferreti et al., 2020) and it should be complemented by digital technologies. Supplemental technologies such as digital Contact Tracing Applications (CTAs) proved useful in this regard. These applications estimate the distance between CTA users and the amount of time they have been in close contact of each other (Walrave et al., 2021). When a CTA user is identified as infected, CTAs can be used to notify other CTA users who have been in the proximity of the infected individual, thus help controlling the transmission of the highly infectious viruses. The outbreak of the COVID-19 pandemic, and the later variants of the virus, spotlighted the importance and instrumentality of CTAs in preventing the further spread of the COVID-19 pandemic (Kreps et al., 2020).

Although during the current COVID-19 pandemic, countries in various parts of the world developed CTAs with the hope of limiting the dissemination of the pandemic, people have not embraced such applications as expected (Oyibo et al., 2022). For instance, statistics show adoption rates to be below 20% in many countries (e.g., Chan, 2020). To reap the potential benefits of using CTAs, a much bigger portion of the population should adopt and regularly use them (Oyibo et al., 2022). Recent reports suggests at least 56% of a country's population need to use CTA technologies to ensure maximal chance of epidemiological control of COVID-19 (Hinch et al., 2020).

A major issue hindering the wide diffusion of CTAs is public concerns about the privacy of their personal information (e.g., Oyibo et al. 2022). It is shown that the public are concerned with privacy-related issues when it comes to digitizing their health-related information (Angst & Agarwal, 2009). Indiscriminate collection of personal information, chronic privacy breaches, and lax attitudes towards individual privacy in the private sector have reduced public trust in digital technologies (Benigo et al., 2020).

Such privacy concerns can, in turn, impede the diffusion of health-related technologies. In particular, Oyibo and colleagues (2022) reviewed the recent empirical literature on the acceptance and use of CTAs.

URI: https://hdl.handle.net/10125/106813
978-0-9981331-7-1

They identified 56 factors, which then were categorized into 10 broader groups that influence people's intentions to use such technologies. Among these factors, privacy concerns were identified as the most prominent barrier in the adoption of CTAs and were shown to negatively affect the intentions to download CTAs, intentions to install CTAs, and intentions to use CTAs.

The success of using contact tracing tools to control the transmission of infectious diseases highly depends on whether or not a large enough portion of the population use them. In order to encourage people to adopt such applications, their concerns over the privacy of their information should be identified and properly addressed. Therefore, we first need to understand how people perceive information privacy when it comes to the uptake of CTAs, and then develop solutions to overcome those concerns.

Our study contributes to this discussion, and the IS literature, in multiple ways. First, we identify three types of attitudes toward information privacy: information privacy as a human right, information privacy as a commodity, and information privacy as a social norm. We argue that people do not necessarily perceive information privacy in the same way, and the way that people perceive the nature of information privacy has implications for their information privacy-related concerns. Accordingly, we develop scales to measures these attitudes. Our results show that the majority of Canadians believe information privacy to be a human-right rather than a commodity or social norm.

Further, multiple frameworks have been proposed to study information privacy in various contexts. In this study, we argue that integrating these frameworks has value-added beyond any single one of them. Thus, we integrate three of the most widely used information privacy frameworks (CFIP, IUIPC, and MUIPC) to craft a more comprehensive tool to measure Canadians' information privacy-related concerns in general and in relation to the uptake of CTAs. This tool, which is consisted of various types of information privacy concerns, enables us to make novel comparisons. In this regard, and as suggested by Li (2011), we measure both general and specific information privacy concerns which leads to a further nuanced understanding of the information privacy-related concerns of the CTA users. Our results suggest that Canadians' high levels of general information privacy concerns might have inhibited the wide diffusion of CTAs, rather than the particular characteristics of the CTAs themselves.

Finally, we show that one's attitude towards the nature of information privacy has implications for their information privacy-related concerns. For instance, our results suggests that those who believe information privacy is a human right are more concerned with the amount of data collected from them (in general, not limited to the CTAs), than those who believe information privacy is a commodity or social norm. However, our data do not support such distinctions when we limit data collection to the data collected by CTAs.

Overall, our study contributes to the IS research by empirically investigating some of the intricacies in how people perceive information privacy in general, and in relation to the CTAs. Such understanding is a pre-requisite in properly addressing the concerns of the CTA users and facilitating the wide adoption of such applications.

2. Background

2.1. Attitudes about the nature of information privacy

Attitude toward privacy is defined as a set of emotions and beliefs that represent an individual's overall evaluation, perspective, and feeling about privacy (Marcinkowski & Reid, 2019). The literature suggests that people have different attitudes toward the nature of information privacy (e.g., Smith et al, 2011).

Smith, Dinev, and Xu (2011) reviewed multiple literatures to answer the question "what is (and is not) privacy?" They classified one of the definitional approaches to privacy as the value-based approach. Within the value-based approach, some have defined privacy as a human right (e.g., Smith, 1994; Milbrg et al., 2000). For instance, in their seminal work, Warren and Brandies (1989) defined the right to privacy as a natural right, the right to be left alone. Their core argument is an extension of the fundamental right of the individual to full protection in person and property. They emphasize that this principle should be reconfigured in light of political, social and economic changes to preserve individual's right to privacy.

On the other hand, some scholars have defined privacy as a commodity (Smith et al., 2011). When considered as a commodity, privacy is still a value at the individual and societal levels, but it can be considered in cost-benefit calculations as an economic value can be assigned to it (Smith et al., 2011, p. 993).

Finally, some scholars have treated privacy as a social norm. Drawing on Nissenbaum's theory of privacy as contextual integrity (2004), Proferes (2022) explained how we develop, revisit, and negotiate norms around privacy when confronted with new technologies. According to the contextual integrity theory, there are two types of informational norms that affect our privacy evaluations: information appropriateness norms and information flow norms. Information appropriateness norms govern the match between context and the type of information being requested, while the information flow norms govern the movement or transfer of information from one party to another. These norms are

themselves shaped by history, culture, law and convention. Therefore, individuals may have different evaluations about the privacy violation of the same practice, depending on these factors (Proferes, 2022).

As discussed by Xu and Dinev (2022), answering the normative question of "what is privacy" is required to determine and set the privacy rules. Accordingly, in this study, we will first ask participants about their attitudes towards the nature of information privacy. We will use this data to explore the potential associations between individual's attitudes about the nature of information privacy and their major information privacy concerns.

2.2. Types of information privacy concerns

As reviewed by Li (2011), information privacy concerns can be discussed at two levels: general information privacy concerns, and specific information privacy concerns. At the general level, privacy concerns reflect one's overall concerns about information privacy and common practices across different contexts. On the other hand, specific privacy concerns reflect one's privacy concerns in relation to a particular object such as an application, a website, or an organization. This distinction is noteworthy as general privacy concerns can color one's evaluation of privacy concerns in a particular context. Three information privacy frameworks are widely used in the literature.

Smith and colleagues (1996) developed the Concerns For Information Privacy (CFIP) framework. CFIP was developed by focusing on organizational information privacy practices and had four dimensions: collection, unauthorized secondary use, improper access, and error. In this conceptualization, collection refers to an individual's concerns regarding the extensive amount of identifiable information that is gathered and stored from them. Unauthorized secondary use (either internal or external) refers to the concerns that the collected information might be used for purposes other than what was intended when collecting data. Such unauthorized use might be relevant within an organization, or when information might be disclosed to external parties without the consent of information providers. Improper access refers to concerns about the availability of personal data to people who are not properly authorized to have access to the data. Finally, error reflects concerns over the accuracy of the collected and stored information.

By acknowledging the widespread use of internet, Malhotra and colleagues (2004) adapted CFIP to better reflect concerns in the online context. Accordingly, they proposed the Internet Users Information Privacy Concerns (IUIPC) framework which includes three dimensions: collection (retained from the CFIP framework), control, and awareness. In this conceptualization of information privacy concerns, the amount of control one has over their personal information and how it is going to be used is considered as a major factor. Further, awareness refers to one's concerns over their knowledge and awareness of the information privacy policies and practices.

Further specifying the focus of information privacy concerns, Xu and colleagues (2012) proposed the Mobile User's Information Privacy Concerns (MUIPC) framework. They argued that mobile applications pose new privacy-related concerns as huge volumes of personal information can be collected and transmitted in real-time through smart phones. The MUIPC framework consists of three dimensions: perceived surveillance, perceived intrusion, and secondary use of information. The first two dimensions can be considered as somewhat new dimensions. Perceived surveillance is rooted in the collection dimension from CFIP and IUIPC and refers to user perceptions that their actions are constantly monitored through smartphones. Perceived intrusion refers to issues of co-ownership of the data and if application providers are able to make decisions about the data independent of data providers. Such decisions might be intrusive and create discomfort for data providers.

As each of these frameworks has a particular focus (i.e., organizations, internet users, mobile phone users), we integrate them in the current study to craft a more comprehensive tool to investigate the information privacy concerns of CTA users. Given that some organizations provide CTAs, and that such applications work through mobile phones which enable constant transmission of information through internet, integrating the discussed frameworks enable us to capture much more relevant information compared to using only one framework.

2.3. Empirical evidence on privacy concerns and CTAs.

Although far from conclusive, some aspects of the information privacy-related concerns of CTA users are studied, and suggestions are made to tackle those concerns. For instance, it is suggested that people should be informed about what data will be collected from them and how it will be accessed and used (Sharma et al., 2020). This suggestion seems to focus on raising the awareness of people about the data that is collected and the privacy policies of CTA providers. Further, it is suggested that the amount of collected data should be minimized and the access and evaluation of privacy terms should be simplified (Walrave et al., 2021). This suggestion also highlights the importance of addressing the awareness-related concerns of CTA users (by simplifying the access to privacy policies of CTA providers) and, at the same time, addressing their concerns over collection of too much data. Both of these

factors (i.e., awareness and collection) are discussed in privacy frameworks. However, these are only two of the concerns that are identified in previous studies. Thus, we still need to dig deeper and investigate a wider range of privacy-related concerns of individuals which in turn enables us to provide practical suggestions to curb such concerns.

In the current study, we cast a much wider net by integrating the three most widely used frameworks to craft a more comprehensive tool for investigating such concerns. Our goal is to map out a wider range of information privacy concerns of CTA users. We further surveyed if there is any association between attitudes toward information privacy and privacy concerns. Findings will be informative in understanding one of the major reasons for the low adoption of CTAs. Such understanding can be used to tackle the concerning issues and ensure the widespread adoption of CTAs if needed.

3. This study

This study has three main objectives. The first objective is to investigate the attitudes of Canadians about the nature of information privacy. As discussed above, people might have different beliefs about information privacy either as a human right, a commodity, or a social norm. Such beliefs might, in turn, have implications for people's concerns over the privacy of their information and how such concerns can be addressed. To the best of our knowledge, this is the first study to explore this question in Canada.

The second objective of this study is to capture and explore the relative importance of a variety of individuals' information privacy-related concerns: both general information privacy concerns and specific information privacy concerns regarding CTAs. To this end, we integrate three of the most frequently used information privacy frameworks (CFIP, IUIPC, and MUIPC) and construct a more comprehensive tool to investigate different types and dimensions of information privacy concerns.

Angst & Agarwal (2009) used CFIP to study the uptake of electronic health record technologies. They studied the overall effect of CFIP (i.e., the overall influence of various types of privacy-related issues on the uptake of the new technology). As a future research direction, they suggested further studying the underlying factors that contribute to the overall CFIP as discrete constructs. We integrate this suggestion into our analysis of information privacy concerns and further expand it; we treat different types (dimensions) of privacy concerns as discrete latent variables, and go beyond the CFIP framework by bringing in complementary types of information privacy concerns from other widely used frameworks.

Regarding the dimensionality of information privacy concerns, the literature suggests that it should not be considered as static, and scholars should monitor and investigate the implications of technological changes for privacy-related concerns of individuals (Smith et al., 1996; Xu et al., 2012). Given the rapid technological changes, particularly in the health care industry, it would be informative to investigate the relative importance of different types of information privacy concerns, and their relationships with each other.

Finally, the third objective of this study is to investigate the potential associations between individuals' attitudes toward the nature of information privacy, their general information privacy concerns, and their specific information privacy concerns regarding CTAs. We aim to answer questions such as "are the concerns of those who believe information privacy is a human right different from those who believe information privacy is a commodity?"

4. Methodology

4.1. Attitude towards information privacy

We developed new scales to investigate public attitudes toward information privacy. As discussed above, our review of the relevant literature identified three main perspectives on information privacy: privacy as a human right, privacy as a social norm, and privacy as a commodity. To measure such attitudes, a questionnaire was developed that contained 3 items for each of the identified privacy attitudes. To discover discernible patterns of privacy attitudes, we conducted exploratory factor analysis (EFA). Further, we examined the reliability, convergent validity, and discriminant validity of the scale.

4.2. The framework for measuring information privacy concerns

To serve the objectives of this study, we borrow from Smith and colleagues (1996), Malhotra and colleagues (2004), and Xu and colleagues (2012) conceptualizations of information privacy concerns to craft a more comprehensive tool to investigate information privacy. Accordingly, the following types of information privacy concerns will be measured in this study:

1. General privacy concerns: to measure general privacy concerns we use the existing validated dimensions of collection, unauthorized secondary use, improper access, and error from CFIP as well as control and awareness from IUIPC.
2. Specific privacy concerns: Considering the existence of multiple instruments in the literature to measure privacy concerns, and taking into account the recommendations provided by Xu and Dinev (2022), we

adapted 5 dimensions of collection, unauthorized secondary use, improper access, control and awareness to measure the specific privacy concerns in the context of CTAs. Since the perceived surveillance and perceived intrusion dimensions from MUIPC are rooted in collection, and unauthorized use/improper access, we have integrated their respective items into those dimensions. The adapted dimensions now include items that reflect the concerns regarding massive data collections and the ability of current learning algorithms to extract information from the data of other users who are similar to a target user. This list of information privacy concerns is more comprehensive than any of the original scales and, thus, can provide more information on the main privacy-related concerns of CTA users.

4.3. Impact of privacy attitudes on privacy concerns

To study the impact of privacy attitudes on various types of privacy concerns, we investigated the differences that privacy attitudes make on various types of privacy concerns (Figure 1). To this end, we identified participants with each of the particular privacy attitudes using their perceptions along each of the scales of the privacy attitudes (privacy-as-a-right scale, privacy-as-a-norm scale, and privacy-as-a-commodity scale). We split the participants into four categories according to their privacy attitudes: privacy-as-a-right category (if they scored higher on the right scale), privacy-as-a-norm category (if they scored higher on the norm scale), privacy-as-a-commodity category (if they scored higher on the commodity scale), and indifferent category (if there was not a difference among at least two privacy attitude scales). Then, we performed an analysis of variance (ANOVA) to investigate whether there is any significant difference among the first three categories (we discarded the indifferent category from further analysis) along each dimension of privacy concerns.

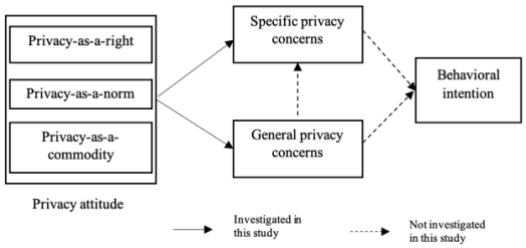

Figure 1. Conceptual Framework

4.4. Data

We used prolific to collect a sample of the Canadian population. Our sample consists of 356 participants and their usable responses. The demographic profile of participants is listed in Table 1. Women (51%) and men were well-presented in the sample, the majority of participants aged between 25-54 years old, and 68% of respondents holds bachelor's degree or higher. Further, the sample included people with various ethnicities with the majority (56%) being Caucasian. Compared to the Canadian population, the minority communities are well represented in our sample.

Table 1. Respondent's profiles (demographics)

Age	%	Income (CAD)	%
18-24	18	$200,000 or more	1
25-34	36	$160,000 - $199,999	2
35-44	28	$100,000 - $159,999	18
45-54	10	$75,000 - $99,999	18
55-64	6	$50,000 - $74,999	19
65+	2	$25,000 - $ 49,999	19
		Under $25,000	22
Sex		Employment Status	
Female	51	Employed	79
Male	49	Not in labor force	8
		Unemployed	12
Highest Education		Marital Status	
Bachelor's degree	51	Single/ never married	54.2
Some college	22	Married/ common law	41.0
Advanced graduate degree	17	Divorced	2.5
High school	5	I prefer not to answer	1.1
Some graduate work	4	Separated	0.8
Less than high school	1	Widowed	0.3
Race/ Ethnicity			
Caucasian/ White	56		
East Asian	21		
Others (mixed race)	8		
South Asian	6		
African/Black	5		
Hispanic/Latino	3		
Native/Aboriginal	1		

5. Results

5.1. Attitude towards information privacy

We first investigated the factorial structure of attitudes toward the nature of information privacy. To this end, and following Xu and colleagues (2012), we conducted an exploratory factor analysis (EFA). EFA was conducted by using the Principal Component

Analysis technique with Orthogonal Varimax as the rotation method using SAS Enterprise Guide (7.15). The results are provided in Table 2. As the results suggest, all the items were loaded on their respective attitude type and there was no cross-loading. Except for one item that was used to measure social norms, all items loaded higher than 0.7 on their expected factor and lower than 0.4 on the other factors. These results confirm the three-factor structure of our data.

The convergent validity for each factor in the EFA was conducted by examining the reliability measure, Cronbach's alpha, provided in Table 2. The analysis shows the reliabilities of the three dimensions to be equal to or above the 0.7 criteria suggested in the literature (Nunnally, 1978). To assess the convergent validity of the scale, it is suggested that all the item loadings should be above the 0.6 cutoff (e.g., Chin et al., 1997; Malhotra et al., 2004). As Table 2 suggests, all the items (except one) loaded higher than 0.6, and the only one below 0.6 is very close to the cut-off (0.599). Thus, the measure shows an acceptable level of convergent validity. Discriminant validity is the extent to which an item does not relate to the measures of other constructs and was established by having all the cross loadings below 0.3.

Table 2. EFA for attitudes toward information privacy

Factor	Items	Component			Cronbach's Alpha
		1	**2**	**3**	
Privacy-as-a-right	PB Q1	**0.850**	0.021	-0.030	0.8
	PB Q2	**0.859**	0.042	-0.005	
	PB Q3	**0.775**	-0.013	0.124	
Privacy-as-a-commodity	PB Q4	0.115	**0.778**	0.047	0.7
	PB Q5	0.049	**0.847**	0.151	
	PB Q6	-0.125	**0.733**	0.214	
Privacy-as-a-norm	PB Q7	0.177	0.036	**0.599**	0.7
	PB Q8	-0.105	0.220	**0.855**	
	PB Q9	-0.018	0.165	**0.816**	

Further, our results show that the majority of our participants (62.9%) perceive privacy as a right, rather than a social norm (14.3%) or commodity (3.4%). The remaining (19.4%) were not categorized as belonging to any of these categories as they scored equally on at least two types of attitudes. This group of participants is not considered for further analysis. These findings show that a considerable portion of Canadian society believes information privacy is a human right and should be treated as such. The implications of such attitudes towards information privacy will be discussed.

5.2. Measuring the relative importance of general and specific privacy concerns

In this study, we distinguished between general information privacy concerns and specific information privacy concerns in the context of CTAs. We investigated the relative importance of various types of information privacy concerns. This was done for both general information privacy concerns (Figure 2) and specific information privacy concerns in the context of CTAs (Figure 3).

In general, as evident in Figure 2, unauthorized secondary use, improper access, lack of awareness about privacy practices as well as lack of control over data and data over-collection concern our Canadian participants. Participants were more concerned over unauthorized secondary use, improper access, and awareness. However, participants are less concerned about the inaccuracy of the collected data (the error dimension).

In the context of CTAs (Figure 3), control and improper access were the main concerns of participants when it comes to the uptake of CTAs. Such concerns are followed by awareness, data over-collection, and unauthorized secondary use respectively. It is interesting to note that, overall, our Canadian participants were more concerned with the privacy of their information in general rather than in relation to CTAs.

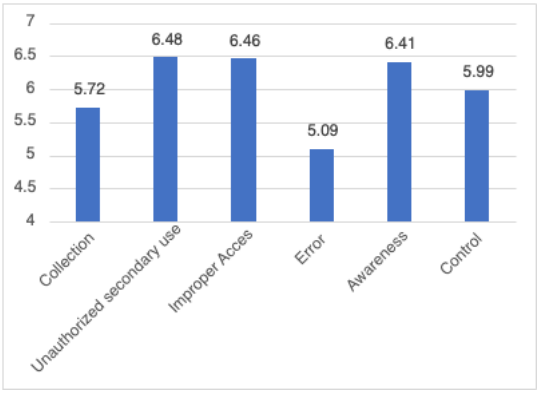

Figure 2. General Information Privacy Concerns

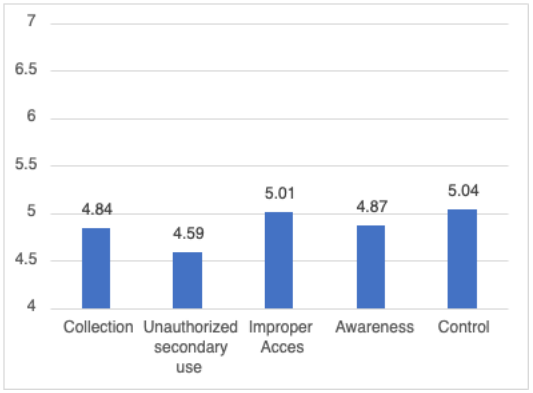

Figure 3. Specific Information Privacy Concerns

5.3. Impact of privacy attitudes on privacy concerns

To investigate if the attitudes toward information privacy have any impact on the types of privacy concerns of participants, we conducted analysis of variance (ANOVA). The analysis was conducted once for the general privacy concerns and once for the specific privacy concerns. The results are shown in Table 3 and Table 4.

Table 3. ANOVA for the general information privacy constructs comparing three different attitudes to information privacy (we have bolded the results with P-value < 0.01)

Construct	Average group concern	F value	P value	Pairwise difference
Collection	Right: 5.84 Norm: 5.24 Commodity: 4.83	8.67	**0.0002**	Rights > Norms, Rights > Commodity
Unauthorized Secondary use	Right: 6.51 Norm: 6.27 Commodity: 6.20	3.59	0.0289	
Improper Access	Right: 6.52 Norm: 6.20 Commodity: 6.11	4.99	**0.0074**	Rights > Norms
Error	Right: 4.97 Norm: 4.78 Commodity: 5.50	1.29	0.2756	
Awareness	Right: 6.42 Norm: 6.32 Commodity: 6.11	1.3	0.2731	
Control	Right: 6.00 Norm: 5.76 Commodity: 5.75	2.49	0.0846	

For general privacy concerns, the results in Table 3 suggest that one's attitudes toward the nature of information privacy significantly affect their concerns over two types of privacy concerns: collection, and improper access. The results of the analysis suggest that those who believe information privacy is a human right are more concerned over the collection dimension than both of the other groups. Regarding improper access, the results suggest that those who believe information privacy is a human right, are more concerned than those who believe information privacy is a social norm.

Regarding specific privacy concerns, the results suggest that one's attitudes toward the nature of information privacy significantly affect their concerns over all types of privacy concerns, but collection, when it comes to the uptake of CTAs. For unauthorized secondary use, improper access, awareness, and control, the results suggest that those who believe information privacy is a human right are more concerned about the privacy of their information than those who believe information privacy is a social norm.

Table 4. ANOVA for the specific information privacy constructs (CTAs) comparing three different attitudes to information privacy (we have bolded the results with P-value < 0.01)

Construct	Average group concern	F value	P value	Pairwise difference
Collection	Right: 5.00 Norm: 4.43 Commodity: 4.03	4.11	0.0175	
Unauthorized Secondary use	Right: 4.71 Norm: 3.82 Commodity: 4.14	5.97	**0.0029**	Rights > Norms
Improper Access	Right: 5.19 Norm: 4.46 Commodity: 4.28	5.32	**0.0054**	Rights > Norms
Awareness	Right: 5.06 Norm: 4.06 Commodity: 4.36	8.35	**0.0003**	Rights > Norms
Control	Right: 5.23 Norm: 4.30 Commodity: 4.04	7.57	**0.0006**	Rights > Norms

6. Discussion

We measured and analyzed Canadians' attitudes toward information privacy. Our data suggest that 62.9% of our participants perceive information privacy as a right, while only 3.4% perceive it as a commodity. In other words, the majority of our participants do not perceive information privacy as something that they would like to assign an economic value to or be willing to consider it in a cost-benefit calculation. Further analysis revealed that this majority group is significantly

more concerned with the privacy of their information (either in general or specific to the use of CTAs) than those who perceive information privacy as a commodity or social norm.

If the majority of people believe that information privacy is a human right (which is the case in our Canadian sample) and not something to be traded, this might be, in fact, a factor that have contributed to the low diffusion of CTAs and other health-related technologies that collect highly personal information. Our findings suggest that this group of the population seems to be the most difficult to encourage to uptake CTAs. We need to highlight the importance of context in generalizing our findings. Li's (2011) review showed that information privacy has social and cultural antecedents and thus we should be cautious in generalizing our findings to other countries. We therefore call for further research about attitudes toward information privacy in other countries.

Further, we aimed at measuring various types of information privacy concerns of Canadians in the context of digital contact tracing applications. To better understand such concerns, we distinguished between general information privacy concerns and specific information privacy concerns in relation to CTAs. Our results reveal that the Canadian general public is highly concerned about the privacy of their information in general. However, such concerns seem to be at a lower level when it comes to the uptake of CTAs.

We explored the relative importance of general and specific privacy concerns in Canada. Findings can be used to propose a better balance between privacy and effectiveness in relation to CTAs for the Canadian population. As discussed above, many different types of concerns about information privacy are identified. Addressing each of these categories requires some concrete yet distinct steps to be taken. We should, however, realize that addressing all of the privacy-related concerns of CTA users might not be possible as certain amounts and types of data have to be collected in order to serve the purpose of such applications. In this regard, Oyibo and colleagues (2022) argued for a balance between privacy and effectiveness. In other words, addressing the privacy-related concerns of people should not be at the cost of reducing the effectiveness of using such CTAs. Thus, it is important to understand the major concerns of societies in this regard and to craft the optimum solutions to minimize their concerns while still managing to collect the necessary data. In order to identify the most (privacy-related) problematic aspects of CTAs from potential users' perspectives, we integrated three widely used frameworks and created a more comprehensive tool than those used in previous studies. Such integration enabled us to make novel comparisons.

For instance, our results suggest that, in general, Canadians are more concerned about unauthorized secondary use, improper access, and awareness. In other words, they are concerned about their data being used for purposes other than what the data was collected for, and the data being accessible to parties other than those to whom they have granted access. Further, concerns over their awareness of how the data will be used, who will have access to it, and what are the privacy-related policies and practices of those organizations who have the data were salient among participants. As discussed before, improper access and unauthorized secondary use are highlighted in the CFIP framework, while awareness is introduced from the IUIPC framework. This finding supports the integration of multiple frameworks in measuring information privacy concerns.

Further, these findings provide initial evidence for Xu & Dinev's (2022) insights that, compared to the last decades, today, people are more concerned with the knowledge that might be extracted from the data rather than the data itself. In other words, now that companies have accumulated huge amounts of data, people might no longer be concerned about their own data as long as companies have data from others who are similar to them in some way.

However, some discrepancies can be observed between the relative importance of general and specific privacy concerns. One notable observation is that the specific privacy concerns are lower than the general privacy concerns. From this observation, it might be reasonable to infer that the privacy-related concerns of Canadians toward CTAs do not necessarily stem from the characteristics of these applications per se. The literature suggests that general privacy concerns affect specific privacy concerns (Li, 2011). It seems like the specific characteristics of CTAs have not aggravated the privacy-related concerns of participants. But, the general information privacy concerns of the general public might have inhibited the wide adoption of CTAs.

However, it does not mean that we should not care about the specific concerns; the lower the concerns, the higher the adoption rate. One argument for the low levels of specific information privacy concerns in the context of CTAs could be made using the low familiarity and low adoption of such technologies. In our sample, the average familiarity with the CTAs was 2.90 on a 7-point scale (1: not familiar at all) and the majority of the participants had not much experience with them. However, it is also possible to argue that given that there are CTAs with high information privacy protection, the low adoption of such technologies arises from the general concerns about information privacy.

Another notable observation is the relative importance of unauthorized secondary use among general and specific information privacy concerns. As

the data suggest, unauthorized secondary use is the main privacy concern among the participants in general, while it is the least concern about CTAs. It means that people are generally less concerned about how the information gathered by CTAs might be used by the organization that has their consent to use the data. However, they are highly concerned about the possibility that other entities might get access to their data, and about the amount of control that they have over their data.

Previous research has shown that the health-related information privacy concerns of individuals can be managed, and individuals can be persuaded to change their attitudes about technologies that keep and track their medical information (for instance by manipulating the framing of the information and arguments provided to them; Angst & Angrawal, 2009). According to the findings of the current study, concerns about improper access and control over data can be among the main obstacles to the wider adoption of CTAs. Managing individuals' privacy-related concerns by addressing these factors would potentially contribute to a higher adoption rate of CTAs.

By addressing such concerns, CTA developers would be able to encourage people to use such applications while managing to collect enough information to serve the purpose of CTAs. Previous studies (e.g., Sharma et al., 2020; Walrave et al., 2021) highlighted the importance of addressing CTA users' concerns over awareness and collection dimensions of information privacy. While confirming the importance of such concerns at the general level, our results suggest that potential CTA users are more concerned with the improper access and control dimensions of information privacy.

Finally, our results suggest that those who believe information privacy is a human right (i.e., the majority of our Canadian participants) are more concerned about who will have access to their data and how such data will be used rather than about the amount of information that CTAs collect. This is a promising finding pointing to the importance of privacy-related concerns other than collection when it comes to the uptake of CTAs in Canada. For such applications to perform effectively, collecting enough data is necessary and our findings suggest that collection is not the major concern of potential Canadian CTA users. In short, if the unauthorized secondary use, improper access, and awareness-related concerns be addressed, there is a higher probability that Canadians adopt CTAs as expected.

7. Conclusion

We propose and provide initial support for a relationship between attitudes toward information privacy and one's major information privacy concerns. Our results show that 62.9% of our Canadian participants perceive information privacy as a right. Furthermore, this group of participants were generally more concerned about the privacy of their information than the others who believed information privacy is a norm (14.3%) or a commodity (3.4%).

In addition, we distinguished general information privacy concerns from specific information privacy concerns about CTAs to better understand such concerns in relation to CTAs and to shed light on the intricacies of the information privacy-related concerns of potential CTA users in Canada. We integrated the most frequently used information privacy frameworks. Our results suggest that using this integrated tool can be more informative than using any single framework. From a practical perspective, our results can be used to encourage a wider diffusion of CTAs. Findings suggest that Canadians are more concerned about some particular aspects of their information privacy when pondering upon using CTAs, and addressing such concerns would encourage them to use such applications.

8. References

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, 339-370.

Bengio, Y., Janda, R., Yu, Y.W., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S. and Sharma, A., 2020. The need for privacy with public digital contact tracing during the COVID-19 pandemic. *The Lancet Digital Health*, *2*(7), pp.e342-e344.

Buck, C., Dinev, T., & Anaraky, R. G. (2022). Revisiting apco. In Modern Socio-Technical Perspectives on Privacy (pp. 43-60). Cham: Springer International Publishing.

Chan, S. (2020). COVID-19 Contact Tracing Apps Reach 9% Adoption In Most Populous Countries. Sensor Tower Blog (2020). Available online at: https://web.archive.org/web/20201126160643/https://sensortower.com/blog/contact-tracing-app-adoption (accessed March 27, 2021).

Chin, W. W., A. Gopal, W. D. Salisbury. 1997. Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. Inform. Systems Res. 8(4)
342–367

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. and Fraser, C., 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, *368*(6491).

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., Lythgoe, K., Cruz, A.B., Zhao, L., Stewart, A. and Ferretti, L., 2020. Effective configurations of a

digital contact tracing app: a report to NHSX. *Retrieved July*, *23*, p.2020.
Kreps S, Zhang B, McMurry N. Contact-Tracing Apps Face Serious Adoption Obstacles. Tech Stream. Brookings (2020).
Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 28.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.
Marcinkowski, T., & Reid, A. (2019). Reviews of research on the attitude–behavior relationship and their implications for future environmental education research. *Environmental Education Research*, *25*(4), 459-471
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization science*, *11*(1), 35-57.
Nissenbaum, H. 2004. Privacy as contextual integrity. Washington Law Review 79 (1): 119157
Nunnally, J.C. 1978. Psychometric Theory, (2nd ed.). New York: McGraw-Hill.
Oyibo, K., Sahu, K. S., Oetomo, A., & Morita, P. P. (2022). Factors influencing the adoption of contact tracing applications: systematic review and recommendations. *Frontiers in Digital Health*, 54.
Proferes, N. (2022). The development of privacy norms. In *Modern Socio-Technical Perspectives on Privacy* (pp. 79-90). Cham: Springer International Publishing.
Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. _IEEE Transactions on Engineering Management.
Smith, H. J. (1994). *Managing privacy: Information technology and corporate America*. UNC Press Books.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.
Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, *68*(3), 459.
Walrave, M., Waeterloos, C., & Ponnet, K. (2021). Ready or not for contact tracing? Investigating the adoption intention of COVID-19 contact-tracing technology using an extended unified theory of acceptance and use of technology model. _Cyberpsychology, Behavior, and Social Networking_, _24_(6), 377-383.
Warren, S., & Brandeis, L. (1989). The right to privacy. In Killing the Messenger (pp. 1-21). Columbia University Press.
Xu, H., & Dinev, T. (2022). Guest Editorial: Reflections on the 2021 Impact Award: Why Privacy Still Matters. Management Information Systems Quarterly, 46(4), xx-xxxii
Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

9. Appendix. Attitudes toward nature of privacy measure

Human Right

(PB_1) I believe privacy is a human right that everybody should have.

(PB_2) I believe that violation of privacy is a violation of human rights.

(PB_3) I believe privacy violation is unethical.

Commodity

(PB_4) I believe privacy is a commodity that organizations should offer to individuals who use their services.

(PB_5) I believe that like other commodities, the market sets the regulations related to privacy.

(PB_6) I believe privacy should be preserved as long as the costs of preserving privacy is less than its benefits.

Social Norms

(PB_7) I believe privacy is a social norm.

(PB_8) I believe privacy norms are socially constructed and evolve overtime.

(PB_9) I believe privacy norms may vary culturally and may change, even within a culture.