CANADIAN JOURNAL of
URBAN RESEARCH
REVUE CANADIENNE de RECHERCHE URBAINE

Privacy and smart cities: A Canadian survey

Sara Bannerman
Canada Research Chair in Communication Policy and Governance
Department of Communication Studies and Multimedia
McMaster University

Angela Orasch
Department of Political Science
McMaster University

Abstract
This paper reports the results of a national survey of Canadians about smart city privacy. Our research questions were: How concerned are Canadians about smart city privacy? How do these concerns intersect with age, gender, ethnicity, and location? More, what are the expectations of Canadians with regards to their ability to control, use, or opt-out of data collection in smart city context? What rights and privileges do Canadians feel are appropriate with regard to data self-determination, and what types of data are considered more sensitive than others?
In part two of this paper, we review existing literature on privacy and smart cities, particularly in Canada. In part three, we outline the method used in our survey. In part four, we present the findings of our national survey on Canadian attitudes towards privacy in a smart city context. We conclude by summarizing our findings and setting out possible areas for future research.

Keywords: smart city, privacy, urban data, data self-determination

Résumé
Cet article présente les résultats d'un sondage national sur la vie privée dans les villes intelligentes mené auprès des Canadiens et des Canadiennes. Nos questions de recherche étaient les suivantes: à quel point les Canadiens sont-ils préoccupés par la vie privée dans les villes intelligentes? Comment ces préoccupations se recoupent-elles avec l'âge, le sexe, l'ethnicité et le lieu? De plus, quelles sont les attentes des Canadiens et des Canadiennes en ce qui concerne leur capacité à contrôler, utiliser ou de se retirer de la collecte de données dans un contexte de ville intelligente? Quels sont les droits et privilèges que les Canadiens jugent appropriés en ce qui concerne l'autodétermination informationnelle et quels types de données sont considérés plus sensibles que d'autres?
La deuxième section de l'article présente une revue la littérature existante sur la protection de la vie privée et les villes intelligentes, en particulier au Canada. La troisième section décrit la méthode utilisée dans notre sondage. Finalement, la quatrième section consiste en une analyse des résultats du sondage national sur les attitudes des Canadiens et des Canadiennes à l'égard de la protection de la vie privée dans une ville intelligente. Nous concluons en résumant nos conclusions et en définissant les domaines possibles de recherches futures.

Mots-clés: ville intelligente, confidentialité, données urbaines, l'autodétermination informationnelle

Canadian Journal of Urban Research, Summer 2020, Volume 29, Issue 1, pages 17-38.

ISSN: 2371-0292

Introduction

In 2017, a framework agreement was established between Waterfront Toronto, the organization charged with revitalizing Toronto's waterfront, and Sidewalk Labs, parent company of Google, to develop a smart city on Toronto's Eastern waterfront (Sidewalk Toronto 2018). This news was met with a series of questions and concerns from experts in data privacy and the public at large. What was to be included in Sidewalk Lab's smart city vision? How would the overall governance structure function? How were the privacy rights of residents going to be protected, and what mechanisms would ensure that protection?

A 'smart city' adopts digital and data-driven technologies in the planning, management and delivery of municipal services. Information and communications technologies (ICTs), data analytics, and the internet of things (IoT) are some of the main components of these technologies, joined by web design, online marketing campaigns and digital services. Such technologies can include smart utility and transportation infrastructure, smart cards, smart transit, camera and sensor networks, or data collection by businesses to provide customized advertisements or other services. Smart-city technologies "monitor, manage and regulate city flows and processes, often in real-time" (Kitchin 2014, 2).

Smart cities are emerging in different ways in various local contexts, and are the focus of an expanding area of study. Smart city technologies move quickly from development to adoption, often outpacing the social and political deliberations necessary to consider their effects in detail. It is within this climate that social research attempts to uncover the adverse consequences that smart city technologies may produce.

As smart-city projects continue to develop across Canada, social research is necessary to gauge public opinion, to consider legal and legislative options, and to examine the social context in which such technologies operate. Given the emergent status of smart cities, this research comes at an important moment. As best practices and path dependencies emerge, it is important to consider the consequences of incorporating technologies into the fabric of city life.

The Toronto waterfront is just one of numerous examples of smart-city developments. Many municipalities in Canada have begun to develop smart city initiatives. In 2018, the Canadian federal government launched a "Smart City Challenge", offering prizes of $50 million, $10 million, and $5 million dollars to fund Canadian cities' top proposals to apply technological solutions to local governance issues (Infrastructure Canada 2018). This intergovernmental program has encouraged the creation of such projects across the country. As of today, almost all major cities in Canada have adopted some level of smart city planning (Author 1 et al. 2019)

Personal and collective privacy is one of the most salient problems associated with smart city initiatives. In April of 2018, the Privacy Commissioner of Canada sent an open letter to the Canadian Minister of Infrastructure and Communities, calling on the federal government to ensure privacy concerns were seriously considered as part of the winning proposals for the Smart City Challenge Project. This letter was signed by all 13 Provincial and Territorial Privacy Commissioners (Beamish et al. 2018). As a result, privacy was included in the selection criteria of the Smart City Challenge (Information and Privacy Commissioner of Ontario 2019, 16).

Existing attitudinal research on privacy has not examined the Canadian smart city context. For that reason, we undertook to conduct a national survey of Canadians about smart city privacy. Our research questions were: How concerned are Canadians about smart city privacy? How do these concerns intersect with age, gender, ethnicity, and location? More, what are the expectations of Canadians with regards to their ability to control, use, or opt-out of data collection in smart city context? What rights and privileges do Canadians feel are appropriate with regard to data self-determination, and what types of data are considered more sensitive than others?

In part two of this paper, we review existing literature on privacy and smart cities, particularly in Canada. In part three, we outline the method used in our survey. In part four, we present the findings of our national survey on Canadian attitudes towards privacy in a smart city context. We conclude by summarizing our findings and setting out possible areas for future research. Our survey data and the full set of tables are available online at https://smartcityprivacy.ca.

Privacy and smart cities

Privacy

While there are several examinations of Canadians' attitudes towards smart cities, and their attitudes about privacy, there are few current population surveys examining Canadian attitudes towards privacy in the context of smart city technologies. The Toronto Region Board of Trade released a poll suggesting that many Torontonians were unaware

of the Toronto smart city project, but also that 47% of Greater Toronto Residents supported the project (Toronto Region Board of Trade and Environics Research 2019). This study did not ask questions relating to privacy.

Attitudes about privacy in general have been studied more extensively. A recent survey by Ipsos-Reid found that Canadians' concerns about privacy are growing, and four in ten Canadians had changed their social media behaviour following revelations about the Facebook/Cambridge Analytica data breach revealed in March 2018 (Simpson 2018). Statistics Canada's Canadian Internet Use Survey examines Canadians' online privacy practices (Government of Canada 2018). The latest survey, in 2012, found growing levels of misuse of Canadians' personal information (Government of Canada 2017a).

Internationally, survey research about attitudes towards privacy attitudes is extensive. Some of that research draws on Alan Westin's Privacy Segmentation Index, which finds that 55% of Americans are "privacy pragmatists," weighing the value of consenting to particular uses of their personal information against potential privacy risks in deciding whether to agree or disagree with particular information activities; that 25% are "privacy fundamentalists" who place a particularly high value on privacy and favour strong privacy laws; and that 20% are "unconcerned" about privacy (Hoofnagle and Urban 2014). Subsequent research has found flaws in Westin's privacy index, finding that people's level of awareness of actual privacy business practices plays a strong role in influencing Americans' attitudes on privacy; those Westin termed "privacy pragmatists" are not making pragmatic informed decisions as Westin suggested, but rather are often less informed about businesses' use of their personal information and about the laws (or lack thereof) in place to protect their privacy. Those whom Westin termed "privacy fundamentalists" were, on the other hand, significantly more informed (Hoofnagle and Urban 2014; Gandy 1993). Others have continued to use, or have modified, Westin's categorization (Da Veiga 2018; Elueze and Quan-Haase 2018).

Past surveys have found that women are more concerned than men with privacy threats, and that "girls perceive more privacy risks and have a higher level of privacy concerns than boys" (Youn and Hall 2008; Bartel Sheehan 1999; Jensen, Potts, and Jensen 2005). However, frequency of Facebook use and online skills have been shown to be more influential on users' tendency to modify their Facebook privacy settings than gender (Hargittai and others 2010; Marwick and boyd 2014).

While it is sometimes said that young people are less concerned about privacy than their elders, Hoofnagle *et al.* suggest that young people are also concerned about privacy (Hoofnagle et al. 2010). Past research demonstrates that youth and teenagers are concerned about privacy and take steps to protect their privacy online (Agosto and Abbas 2017; see also Jai and King 2016). Older adults are also often concerned about privacy, and for them privacy concerns can be a significant barrier to internet use (Elueze and Quan-Haase 2018). Other studies, such as a poll about banking and insurance privacy, have shown a lower level of concern about privacy among older adults (Advocis and The Financial Advisors Association of Canada 2006). At the same time, older adults, too, have a broad range of attitudes towards privacy (Elueze and Quan-Haase 2018). Where older adults exhibit a lower level of privacy concern, this has been linked to a lower level of awareness about privacy risks (Elueze and Quan-Haase 2018).

Lesbian, gay, bisexual, transgender and queer (LGBTQ) people must often navigate how and whether to out themselves not only in real life but online. A 2013 PEW Research survey of people who are LGBT found that 43 % had revealed their sexual orientation or gender identity on a social networking site, and that 55% used social networking sites to meet new LGBT friends online (Pew Research Center 2013). Privacy settings sometimes facilitate users' ability to choose whether or not to disclose their gender identity or sexual orientation to various different online groups and networks by managing the visibility of their postings to various audiences. However, sometimes such affordances are not available. The requirement to use real names, as on Facebook, can also mitigate against privacy control for LGBT people (York and Kayyali 2014). One study showed that LGBT people (parents, in this case), wished to have greater control of online disclosure to different audiences (Blackwell et al. 2016).

Research on privacy, Arora notes, "disproportionately draws from empirical evidence on privacy attitudes and behaviors of Western-based, white, and middle-class demographics to theorize privacy in this digitally mediated world" (Arora 2018, 3). However, as Virginia Eubanks has shown, poor, working class, racialized and marginalized people are subject to higher levels of surveillance (Eubanks 2018; Gangadharan 2017; Arora and Scheiber 2017; Arora 2018; Maréchal 2015):

> marginalized people are subject to some of the most technologically sophisticated and comprehensive forms of scrutiny and observation in law enforcement, the welfare system, and the low-wage

> workplace. They also endure higher levels of direct forms of surveillance, such as stop-and-frisk in New York City. (Eubanks 2014)

Low-income and marginalized people, Eubanks suggests, may see privacy as a pipedream (Eubanks 2014). After all, privacy laws do little to protect those forms of legal and legitimized surveillance to which low-income and marginalized people are subject. However, as Eubanks argues, those same forms of surveillance to which marginalized people are subject, spawn "repressive political environments" wherever used, and will "eventually be used on everyone" (Eubanks 2014).

Contrary to libertarian hypotheses that Americans are most concerned about *state* incursions into the private realm than they are about the intrusions of private businesses, surveys have shown that they are equally concerned about state and business' uses of their personal information (Hoofnagle and Urban 2014, 278).

While existing research reveals a great deal about attitudes towards privacy, much of the existing research deals with contexts outside Canada, and does not address smart city technologies and applications in particular.

Privacy and smart cities

There are a number of academic studies examining smart city privacy in Canada. Teresa Scassa, Tracy Lauriault, Rachel Bloom, Jean-Noé Landry, and David Murakami Wood have written some of the most prominent commentary and scholarship in this area; Scassa has addressed both the privacy and intellectual property aspects of data in a smart city context; Lauriault, Bloom and Landry have set out five characteristics of "open" smart cities and have conducted Canadian case studies of smart cities in Edmonton, Guelph, Montreal and Ottawa; and Murakami Wood has highlighted the historical links between visions of smart cities and previous visions of information societies and e-government, as well as the centrality of surveillance in these projects (Scassa 2017a; 2017b; Lauriault, Bloom, and Landry 2018; Scassa, Chandler, and Judge 2011; Scassa and Sattler 2011; Murakami Wood 2015; Bloom, Lauriault, and Landry 2018). The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), a partner in this research project, has published a "Frequently Asked Questions" document on "Open Smart Cities" (Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, n.d.) as part of a broader project with OpenNorth on Open Smart Cities (Lauriault, Bloom, and Landry 2018).

Privacy regulators in Canada have also begun to grapple with the privacy practices adopted by municipalities and corporations involved in the implementation of smart city technologies. The Office of the Information and Privacy Commissioner of Ontario has developed a public fact sheet addressing smart cities and an individual's privacy (Information and Privacy Commissioner of Ontario 2018). In 2018, federal, provincial, and territorial privacy protection authorities requested that the federal Minister of Infrastructure and Communities take steps to consider the privacy and security of personal information in the selection, design, and implementation of the winning proposals in the federal government's Smart Cities Challenge (Beamish et al. 2018). The Office of the Privacy Commissioner of Canada has funded research on privacy and the Internet of Things, which includes a number of technologies used in smart cities, such as connected devices and sensors (Office of the Privacy Commissioner of Canada 2016).

Internationally, numerous studies have been published on the privacy issues posed by smart cities (Van Zoonen 2016; Kitchin 2016; Finch and Tene 2013; Hiller and Blanke 2016; Edwards 2016). These studies form part of a growing literature on smart cities (Mosco 2019; Caragliu, Del Bo, and Nijkamp 2011; Campbell 2012; Zanella et al. 2014; Albino, Berardi, and Dangelico 2015; Kitchin 2014; Kitchin, Lauriault, and McArdle 2018; Batty et al. 2012).

Methods

During October 23 to November 1 2018, we conducted an online panel survey of Canadians about their attitudes towards privacy in a smart city context. Participants were recruited to the panel by phone using random digit dialing to a blend of landline and cell phones by EKOS Research Associates, and recruited to participate in our survey using emailed scripts. The panel is based on the socio-demographic statistical parameters of the most recent Canadian census (2016). The survey itself was rim-weighted for province, gender, and age and was conducted in English and French.

The final research sample was 1011 individuals (n = 1011). The sample of people surveyed is considered representative of Canadians as a whole, accurate to within a margin of error (MoE) of +/-3.08, 19 times out of 20. It is representative of demographic subgroups with a reduced level of confidence.[1] Significance testing, run on unweighted data, was done using a multinomal test.[2]

Findings

Overall privacy concern

The survey began by defining smart cities as follows:

> The term "smart city" refers to the municipalities' and private businesses' use of technologies, sensors, networks and data used to manage urban environments. Smart city technologies include things like traffic sensors, licence plate readers, smart utility grids, transit apps, smart cards, and online portals for municipal services.

The preliminary question of the survey asked respondents, "How concerned are you about your privacy in the context of the growing uses of smart-city technologies?" Responses were measured on a 5-point Likert scale, from "Extremely concerned" to "Not at all concerned". The survey found that 88% of Canadians are concerned on some level about their privacy in the smart-city context, with 23% being extremely concerned, 29% saying they are moderately concerned, and 19% somewhat concerned. In general, these responses demonstrate a strong level of concern in the privacy issues surrounding smart cities (see Figure 1).

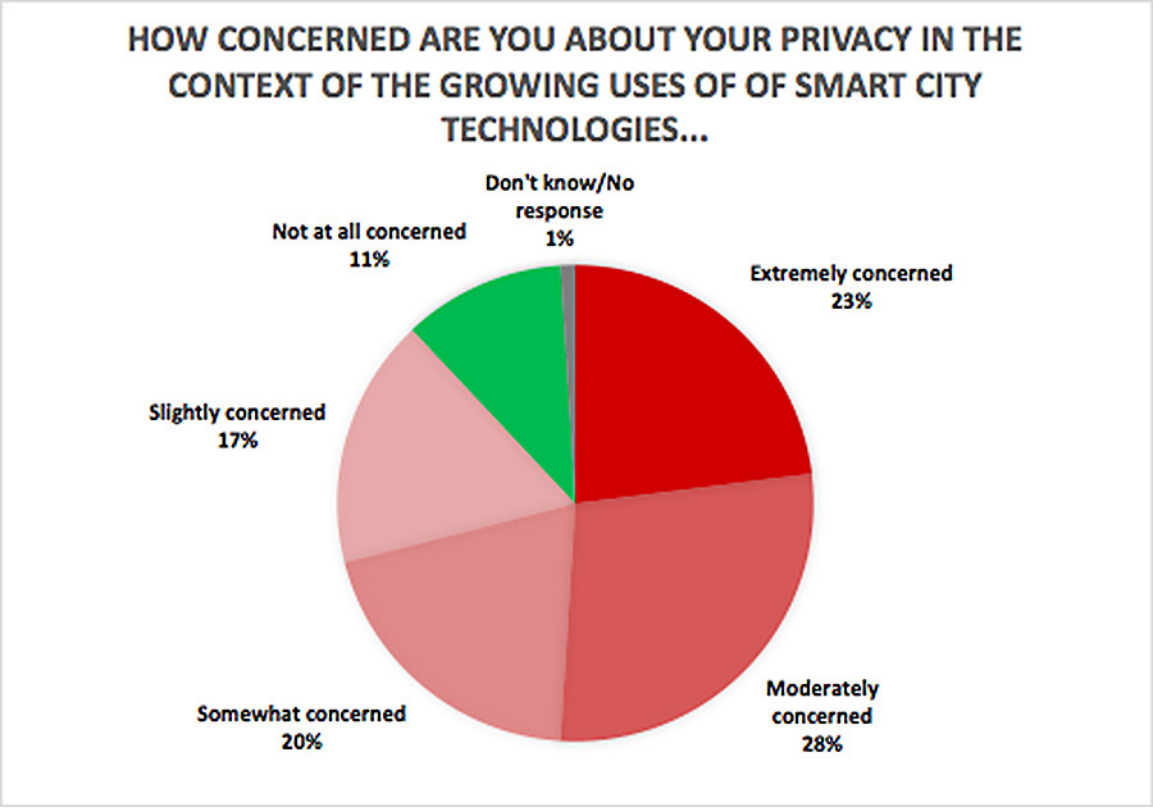

Figure 1

The survey suggests a few interesting demographic findings (Table 1). Participants age 65 and up were less concerned than those from other age groups (35% were "not at all" or "slightly" concerned, compared with 21-30 percent for other age groups). Our finding that older adults are less concerned about smart-city privacy is consistent with some studies that have also shown less concern among older adults about privacy, sometimes due to a lower level of awareness of the privacy risks associated with new technologies (Elueze and Quan-Haase 2018; Advocis and The Financial Advisors Association of Canada 2006).

University-educated Canadians who participated in our survey were also more likely (33%) than high school and college-educated participants to say they were "not at all" or "slightly" concerned. Participants who self-identified

Table 1

How concerned are you about your privacy in the context of the growing uses of smart city technologies?																								
	Total	Province / Territory						Computed age					Gender		Education			Employment status		Minority status				
		BC	AB	SK/MB	ON	QC	Atl	<35	35-44	45-54	55-64	65+	M	F	<HS	Coll	Uni	Emp	Not emp	Non white	Disab	LGBT	None
Total:	1011	127	113	62	383	253	70	250	156	181	184	223	485	512	250	333	420	613	388	99	87	63	753
NOT VERY CONCERNED	28%	29%	31%	21%	30%	23% -	36%	27%	30%	27%	21% --	35% ++	29%	28%	30%	23% --	33% ++	28%	28%	19% --	36% +	22%	29%
SOMEWHAT	20%	20%	21%	25%	19%	21%	18%	21%	22%	21%	21%	18%	19%	21%	20%	23%	17% -	21%	19%	24%	18%	15%	21%
VERY CONCERNED	51%	51%	48%	52%	50%	55%	45%	51%	49%	50%	57% +	48%	51%	50%	49%	54%	50%	50%	52%	54%	46%	60%	50%
Not at all concerned	11%	10%	12%	8%	11%	11%	12%	8%	9%	10%	9%	19%	12%	10%	12%	10%	10%	9%	14%	5%	16%	7%	11%
Slightly concerned	17%	18%	19%	13%	19%	12%	24%	20%	20%	18%	12%	15%	17%	18%	18%	13%	23%	19%	14%	14%	20%	15%	18%
Somewhat concerned	20%	20%	21%	25%	19%	21%	18%	21%	22%	21%	21%	18%	19%	21%	20%	23%	17%	21%	19%	24%	18%	15%	21%
Moderately concerned	28%	29%	24%	31%	29%	27%	23%	30%	21%	29%	30%	30%	26%	30%	28%	26%	31%	27%	30%	31%	25%	40%	28%
Extremely concerned	23%	22%	24%	21%	21%	28%	21%	21%	27%	22%	27%	17%	25%	20%	21%	28%	19%	23%	22%	24%	21%	20%	22%
Don't know/ No response	1%	0%	0%	2%	1%	0%	1%	1%	0%	2%	1%	0%	1%	1%	1%	1%	0%	1%	1%	3%	1%	2%	0%

as visible minorities or Indigenous were more concerned with privacy in the smart city than other groups (just 19 % of visible minorities and Indigenous peoples were "not at all" or "slightly" concerned, as compared with 28 percent of all Canadians).[3]

Past research suggests that visible minorities and Indigenous people, as well as college educated working class people, are subjected to greater levels of surveillance by public or workplace authorities (Eubanks 2018; Gangadharan 2017; Arora and Scheiber 2017; Arora 2018; Maréchal 2015). They may therefore be less likely to be unconcerned about surveillance in a smart-city context.

Uses of data in a smart-city context

Our survey sought to examine Canadians' attitudes towards particular uses of personal information in a smart-city context, focussing on six specific uses of personal information: in targeted advertisements, for behaviour modification, in traffic and transit planning, in policing and crime prevention, the sale of data, and in private businesses. Personal information was defined as "any personally-identifiable information." The survey questions sought to gauge whether certain uses of personal information in a smart-city context were considered more sensitive than others.

Targeted advertisements

Sixty-nine percent of Canadians felt that the use of their personal information to target them with personalized advertisements should not be permitted. A further 27% felt that use of their personal information for targeted advertising should be permitted, but only if they were granted certain rights and protections in their data. Only three percent felt that the collection of data for targeted advertisements should be permitted by default (Figure 2).

Participants under the age of 35 (4%), and Canadians who identified as men (4%), were significantly more likely than other age groups and women respectively to say that the use of their personal information to target them with ads should be permitted by default. Participants under the age of 35 (36%), university-educated Canadians (34 %), Canadians who are employed (31%), and LGBTQ participants (39%), were more likely than other groups (compare with 27% of all Canadians) to say that the use of their personal information to target them with ads should be permitted but "only if I am granted certain rights and protections for my data." Participants age 65 and up (82%), and

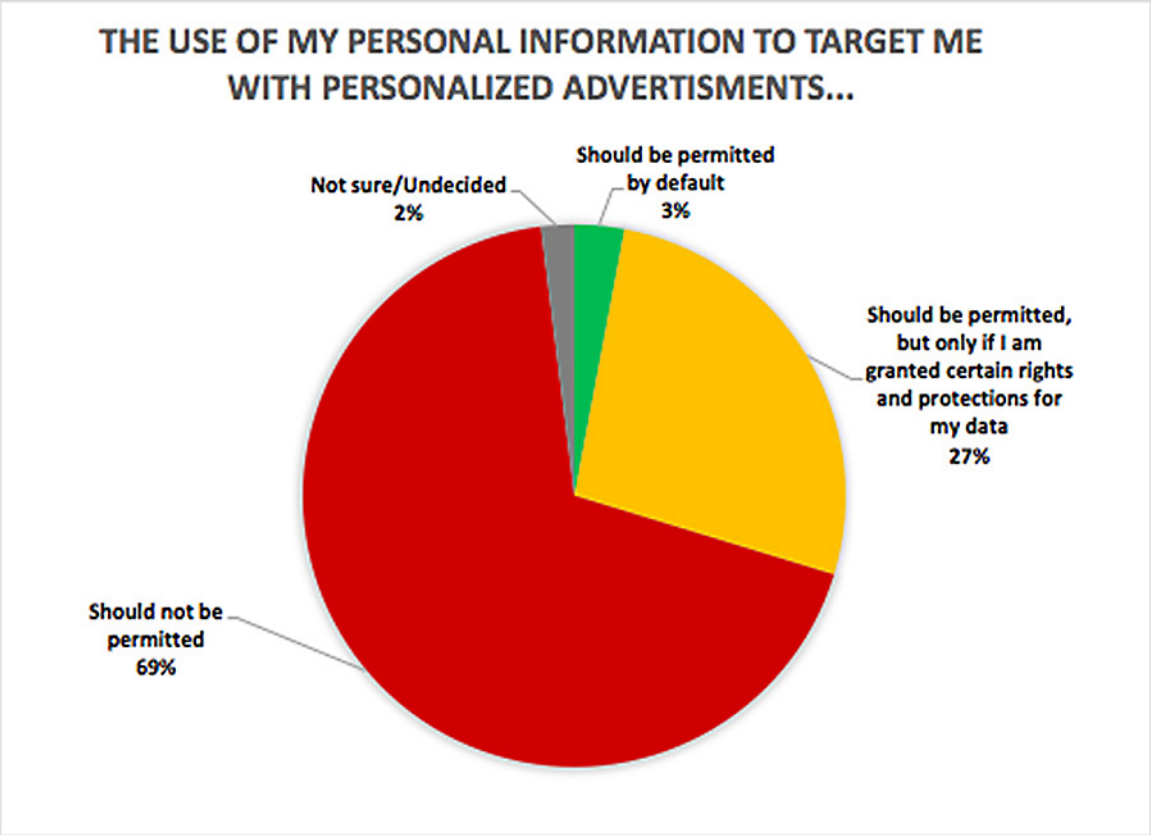

Figure 2:

unemployed Canadians (74%), were more likely than participants in other age categories and employed Canadians, respectively, to say that the use of their personal information to target them with ads should not be permitted (Table 2).

These findings are consistent with previous studies that indicated that young people are more permissive about their personal information, as well as with studies that show young people care about privacy and want to control their personal information (Hoofnagle et al. 2010; Agosto and Abbas 2017; Jai and King 2016).

The stronger level of concern among participants ages 65 and up is consistent with previous studies that show respondents' higher levels of concern about the use of their personal information by banks to sell insurance products (Advocis and The Financial Advisors Association of Canada 2006). While persons over 65 may be less concerned

Table 2

The use of my personal information to target me with personalized advertisements...																						
	Total	Province / Territory						Computed age					Gender		Education			Employment status		Minority status			
		BC	AB	SK/MB	ON	QC	Atl	<35	35-44	45-54	55-64	65+	M	F	<HS	Coll	Uni	Emp	Not emp	Non white	Disab	LGBT	None
Total:	1011	127	113	62	383	253	70	250	156	181	184	223	485	512	250	333	420	613	388	99	87	63	753
...should be permitted by default.	3%	3%	1%	3%	2%	3%	6% +	4% ++	1%	3%	3%	2%	4% ++	2% --	1% -	4%	4%	3%	3%	1%	5%	1%	3%
...should be permitted, but only if I am granted certain rights and protections for my data.	27%	24%	27%	23%	29%	25%	27%	36% ++++	29%	30%	21% -	15% ----	29%	25%	25%	23%	34% +++	31% ++++	21% ---	32%	22%	39% ++	26%
...should not be permitted.	69%	71%	70%	72%	68%	70%	63%	58% ----	68%	66%	74%	82% ++++	66% --	72% ++	71%	72%	61% ---	65% ----	74% +++	66%	69%	57% --	70%
Not sure / undecided	2%	3%	2%	2%	1%	3%	4%	1%	2%	2%	3%	2%	2%	2%	2%	1%	1%	2%	2%	1%	5%	3%	2%

about privacy in general, they may be more concerned about the use of personal information to target them with unscrupulous sales and marketing practices.

Our results are also consistent with studies that have found that women are more concerned about privacy, as compared with men (Youn and Hall 2008; Jensen, Potts, and Jensen 2005; Bartel Sheehan 1999).

Unemployed Canadians were more likely (74%) than those employed (65%) to say that the use of their personal information to target them with ads "should not be permitted," rather than permitting such uses if they are granted certain rights and protections for their data (Table 2). People with lower incomes may have lower confidence that privacy rights and protections will actually serve to protect their privacy (Eubanks 2014; 2018).

Behaviour modification

Second, the survey examined attitudes towards the use of personal information to prompt an individual to modify their behaviour. To demonstrate how personal information could be used to prompt an individual to modify their behaviour, the survey question noted that:

> your transit use or location data could be analyzed, and you could then receive personalized messages prompting you to use transit or to park in less congested areas. Your hydro use data could be analyzed, and you could receive prompts to use less hydro, or to use hydro in off-peak hours. Your activity data could be analyzed, and then you could be prompted to engage in healthier behaviours.

Respondents were asked to complete the sentence "Use of my personal information to prompt me to modify my behaviour…" and were given the options "should be permitted by default," should be permitted, but only if I am granted certain rights and protections for my data," "should not be permitted," and "not sure / undecided."

Forty-eight percent of Canadians felt that the use of their personal information to prompt them to modify their behaviour should be permitted, but only with the granting of certain rights and protections. A further 44% felt that this should not be permitted at all, suggesting there is a strong aversion to the use of personal information for behavior modification, especially if individual rights and access over that data is not granted. Only 5% saw use of personal information for behaviour modification as something that should be permissible by default (Figure 3).

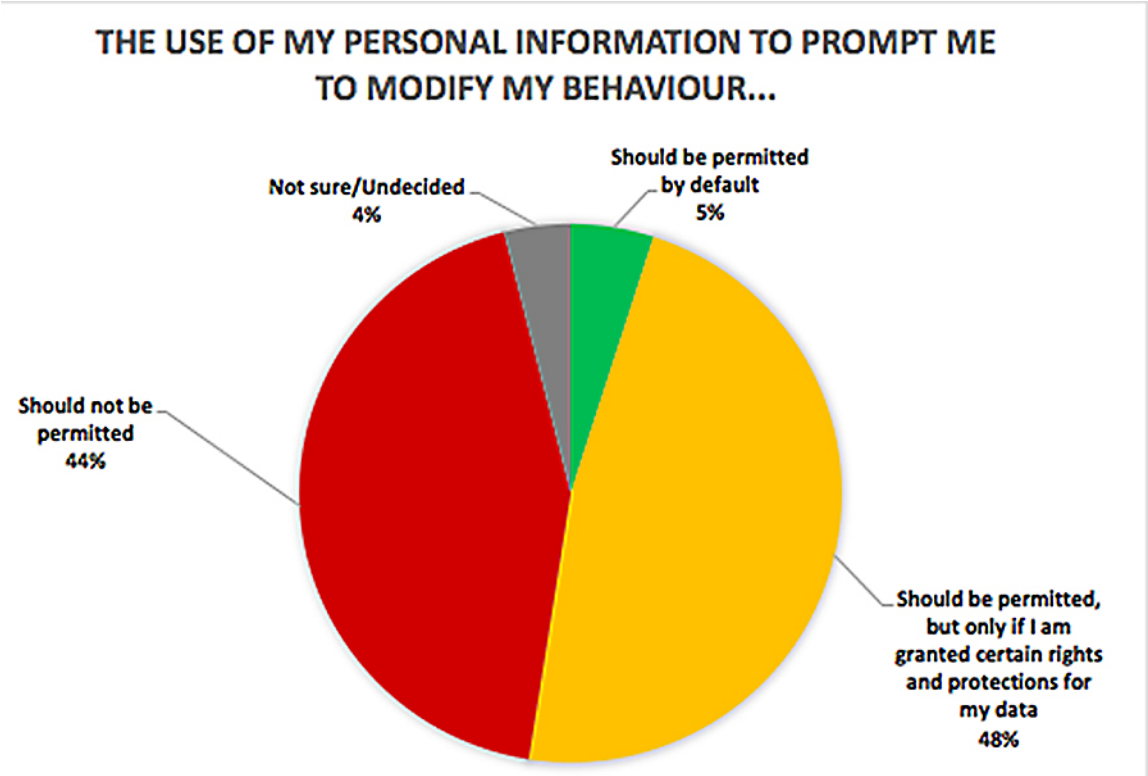

Figure 3:

University educated (58%) and employed Canadians (52%), participants under 35 (56%), and LGBTQ participants (61%) were more likely to say that the use of their personal information for behaviour modification prompting should be permitted only with certain rights and protections than to say that such use should not be permitted outright. College-educated participants (50%), unemployed Canadians (41%), and participants over 65 (49%), were more likely than their counterparts to say that this use should not be permitted at all (Table 3).

Table 3

Use of my personal information to prompt me to modify my behaviour...																						
	Total	Province / Territory						Computed age					Gender		Education			Employment status		Minority status			
		BC	AB	SK/MB	ON	QC	Atl	<35	35-44	45-54	55-64	65+	M	F	<HS	Coll	Uni	Emp	Not emp	Non white	Disab	LGBT	None
Total:	1011	127	113	62	383	253	70	250	156	181	184	223	485	512	250	333	420	613	388	99	87	63	753
...should be permitted by default.	5%	2%	5%	2%	4%	7% +	6%	4%	5%	3%	6%	5%	5%	5%	3%	5%	5%	4%	5%	1% -	6%	8%	5%
...should be permitted, but only if I am granted certain rights and protections for my data.	48%	45%	50%	47%	51%	47%	39%	56% +++	49%	46%	45%	41% --	48%	48%	48%	41% ---	58% ++++	52% +++	43% ---	55%	40%	61% ++	48%
...should not be permitted.	44%	43%	41%	45%	43%	42%	52%	36% ---	42%	46%	47%	49% +	45%	43%	44%	50% +++	34% ----	41% --	47% +	37%	43%	28% --	45%
Not sure / undecided	4%	10%	4%	6%	1%	5%	2%	4%	5%	4%	2%	4%	3%	4%	5%	4%	3%	3%	5%	6%	11%	3%	3%

As with the previous question about targeted advertisements, these results may suggest a stronger level of confidence in privacy rights and protections by younger participants, university-educated and employed Canadians, as compared to college-educated participants and unemployed Canadians. The greater willingness of LGBTQ participants to conditionally permit, rather than outright reject, behaviour-modification uses may reflect greater confidence in rights and protections, and/or a greater dependence on, or familiarity with, technologies for managing identity, disclosure, and personal connections and relationships (Blackwell et al. 2016).

Traffic and transit planning

The survey examined attitudes regarding the use of personal information for traffic, transit, or city planning. The survey question noted that "web, smartphone app or social media activity data could be used to analyze traffic and transit activity, and to predict future trends."

There seemed to be a generally lower level of concern regarding this type of data collection, especially if individuals were granted rights and protections over the personal information collected. The greatest number of Canadians (57%) felt that the use of personal information for traffic, transit, and city planning was permissible with protections and rights granted to them over their data, while 24% felt that such uses should not be permissible at all. However, 17% felt that this kind of use should be permitted by default—a higher number than the previous two categories, suggesting a slightly lower level of privacy concern (Figure 4).

Participants over the age of 65 (21%), men (18%), university educated Canadians (19%), and unemployed Canadians (20%), as well as participants from Alberta (23%), were more likely than other groups (for all Canadians, this number was 15%) to say that such use should be permitted by default, whereas participants under the age of 35 (66 %), employed Canadians (61%), and participants in Ontario (60%) were more likely to permit such uses if rights and protections were granted. Participants with high-school education or less (30%) were more likely to say such uses should not be permitted at all (Table 4).

We see here the same lower level of concern and greater confidence in "certain rights and protections" among younger participants and university-educated Canadians as was revealed in previous questions. Interestingly, employed Canadians (61%), as in previous questions, were more willing than those unemployed (49%) to share their data on condition of "certain rights and protections." Here, this corresponds with a *lower* level of permissiveness—a lower willingness to share this data by default (as opposed to a lower likelihood of saying that such use should not be permitted, as was the case with previous questions). In other words, employed Canadians are significantly less permissive than unemployed Canadians, with a higher expectation or desire for data rights and protections when it comes to the use of their data for public services like traffic, transit and city planning.

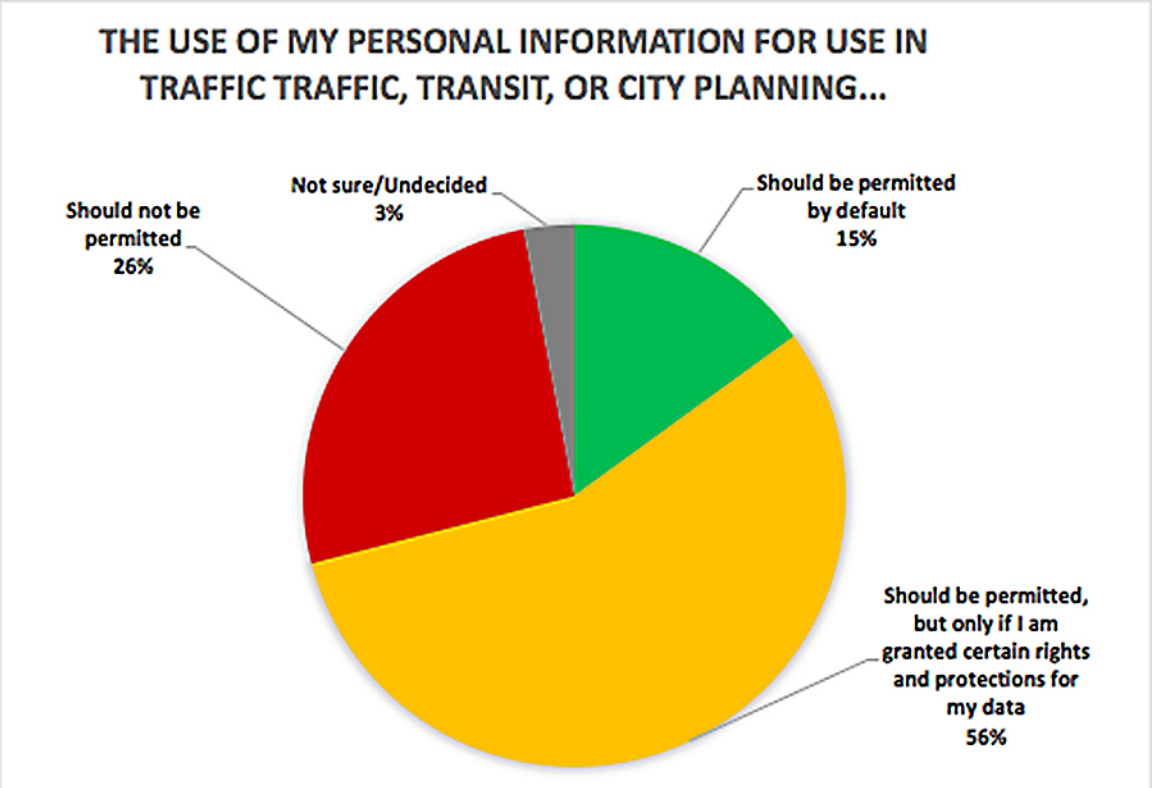

Figure 4

Table 4

Use of my personal information for use in traffic, transit, or city planning...	Total	Province / Territory						Computed age					Gender		Education			Employment status		Minority status			
		BC	AB	SK/MB	ON	QC	Atl	<35	35-44	45-54	55-64	65+	M	F	<HS	Coll	Uni	Emp	Not emp	Non white	Disab	LGBT	None
Q7AC																							
Weighted Total:	1011	138	113	65	387	234	70	276	162	178	171	208	483	514	403	345	255	607	393	108	105	69	723
Total:	1011	127	113	62	383	253	70	250	156	181	184	223	485	512	250	333	420	613	388	99	87	63	753
...should be permitted by default.	15%	15%	23% ++	11%	15%	14%	14%	14%	12%	13%	18%	21% ++	18% ++	13% --	14%	15%	19% ++	12% ----	20% ++++	15%	19%	20%	15%
...should be permitted, but only if I am granted certain rights and protections for my data.	56%	59%	53%	58%	60% ++	53%	41% ---	66% ++++	54%	54%	49% --	53%	54%	58%	52% --	58%	61% ++	61% ++++	49% ----	51%	53%	63%	57%
...should not be permitted.	26%	22%	24%	29%	23%	29%	35% +	19% ---	31% +	30%	30%	21% -	25%	27%	30% ++	26%	18% ----	25%	26%	31%	23%	14% --	26%
Not sure / undecided	3%	4%	0%	3%	1%	3%	10%	1%	2%	3%	3%	5%	2%	3%	4%	1%	2%	2%	4%	3%	5%	2%	3%

Unemployed Canadians were more likely than those employed to say that use of their personal information for traffic, transit and city planning should be permitted by default, also a change from previous questions, on which they were more likely to say that uses should not be permitted. This may represent a greater trust in public authorities, a greater reliance on public services and transit and thus a stronger interest in the use of data to improve public services, a habituation to surveillance by public authorities, or lower confidence that rights and protections would useful to protect individual privacy.

Policing

Noting that "police services can use personal data collected via web, smartphone app or social media activity to predict future behaviours of individuals or groups, and to take actions to prevent crime," the survey asked respondents to complete the sentence "Use of my personal information by police in crime prevention…" Again, respondents were given the options "should be permitted by default," should be permitted, but only if I am granted certain rights and protections for my data," "should not be permitted," and "not sure / undecided."

The majority of Canadians felt that their personal information should either not be collected by police for use in crime prevention (32%), or should only be collected if certain rights and privileges were afforded to individuals over this data (44%). The number of Canadians who felt that default permission was acceptable totaled only 19% (Figure 5). This suggests a strong level of concern regarding this type of data collection in the smart-city context.

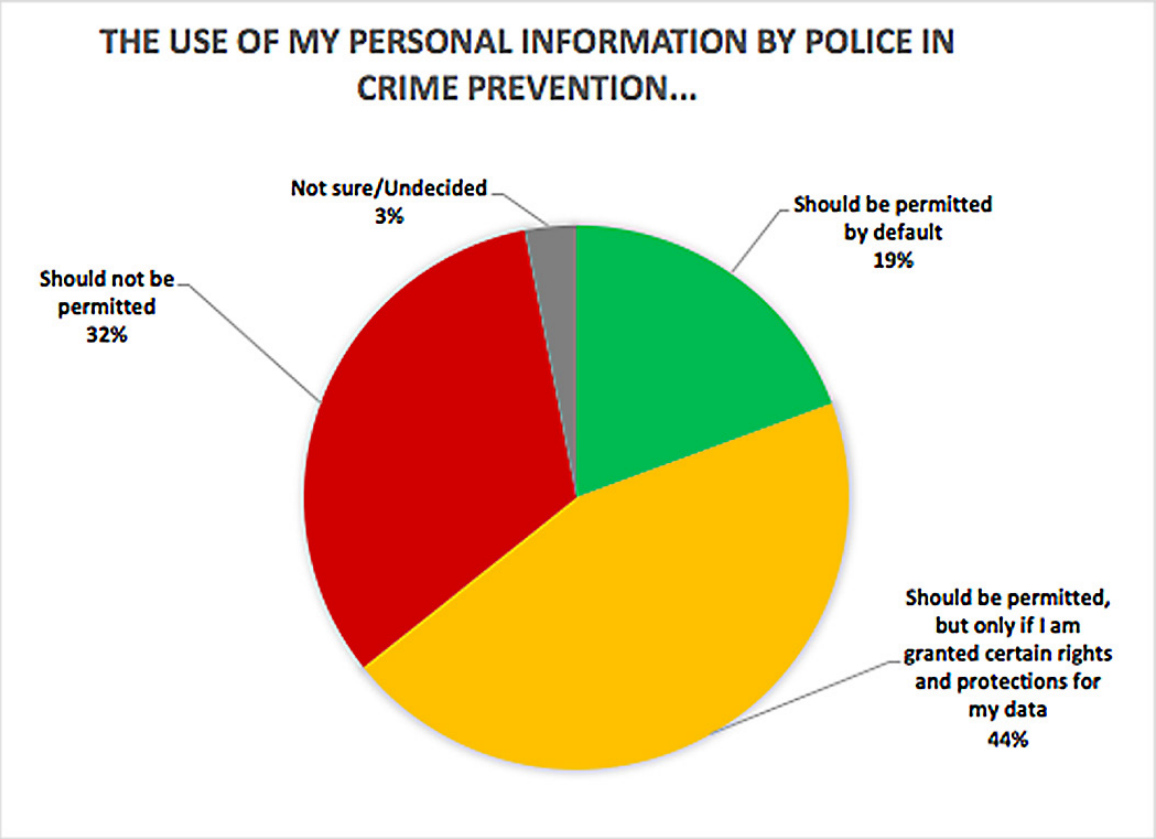

Figure 5

Participants who identified as visible minorities and Indigenous people respondents objected in greater number (together, 42%) to the collection of personal information for policing.[4] Men objected to this type of data collection significantly more than women; 40% of men, compared to 25% of women, said that that the use of personal information by police in crime prevention "should not be permitted." Women were more likely to say that such uses should be permitted by default (22%), or should be permitted if certain rights and protections were granted (46%) as compared with 17% and 41% of men respectively.

This result is interesting because it contrasts with research that shows that women, in most contexts, are more concerned about privacy than men (Youn and Hall 2008; Jensen, Potts, and Jensen 2005; Bartel Sheehan 1999). It also indicates possible strong objections of visible minorities and Indigenous peoples to over-surveillance and targeting by police services, though further research is necessary to verify this finding.

Sale of data

Ninety-one percent of our sample, a clear majority, felt that the sale of their personal information should not be permitted. The survey explained that, "For example, your personal information could be sold by government or businesses to other businesses or data brokers." Only 8% felt that the sale of their personal information should be permitted with certain rights and privileges afforded to the individual (Figure 6). This demonstrates a high degree of public concern over data sales.

Men (9%) were slightly more likely that women (6%) to accept the sale of their data with certain rights and privileges, as were university educated participants (14%) as compared to participants with other levels of education (8% for all levels of education).

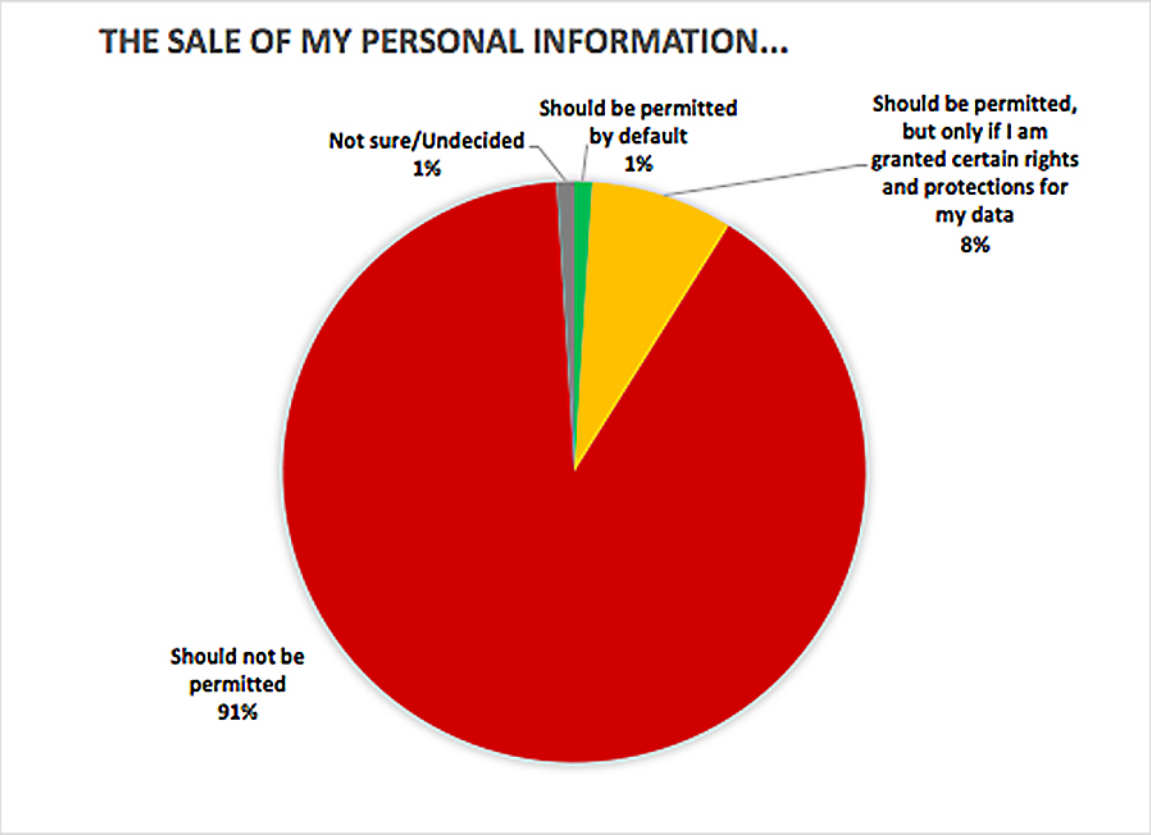

Figure 6

These findings are consistent with studies generally showing a higher level of concern about privacy among women (Youn and Hall 2008; Jensen, Potts, and Jensen 2005; Bartel Sheehan 1999), and possibly a higher level of awareness of the risks associated with the sale of personal information among university-educated Canadians.

Private business use

Survey respondents were asked to complete the sentence, "Use of my personal information to plan and refine private businesses to make them more profitable should be permitted, as long as…." "For example," the survey explained, "your taxi usage data could be analyzed to adjust services or prices." Fifty-five percent of respondents felt this type of data collection should not be permissible. By contrast, 37% felt that is should be permissible but with rights and protections, while only four percent felt it should be permissible by default (Figure 7). Similar to the sale of data, these results demonstrate a substantial degree of concern over the usage of data to service private business interests.

Surprisingly, participants aged 35–44 were more likely (65%) than other age groups to be unwilling to permit use of personal data for profit (compare with 55% of all Canadians). University educated Canadians were more permissive, and more likely to allow their personal data to be used with certain rights and protections (42%, versus 37% for all education levels). Unemployed Canadians were more willing to allow their data to be used in this manner by default (six percent, compared to three percent for those unemployed).

It is possible that university-educated Canadians were, again, more confident in the protection that could be provided by "certain rights and protections" than their high school and college-educated counterparts. It is also possible that unemployed Canadians hoped or believed that permitting uses of personal data to make businesses more profitable might improve employment opportunities.

Data control

Following the initial questions, those who agreed that their data should be used for the given purpose (i.e. for targeting ads, behavior modification, traffic and transit planning, policing and crime prevention, sale, or profitability) "only

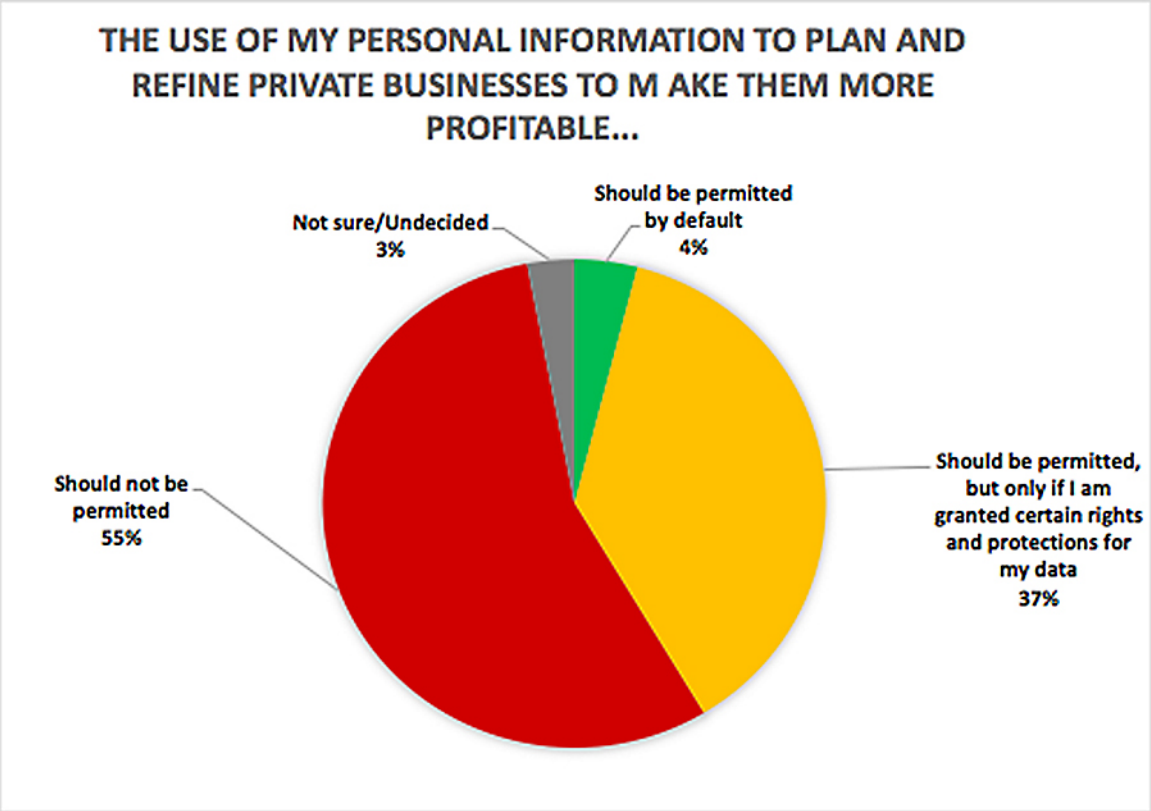

Figure 7

if I am granted certain rights and protections for my data," were given a subset of questions, with order randomized, where they could indicate what specific rights and privileges should be provided the use should be permitted.[5] The response field offered the following provisions within which respondents could indicate what they felt were appropriate measures to ensure appropriate collection of personal data. They were instructed to select all of the conditions that should apply:

- I'm notified somewhere in the fine print when I agree to use a service;
- I can opt in;
- I can opt out;
- I can view my data;
- I can correct my data;
- I can delete my data;
- I can download my data for my own use;
- My data is aggregated with other data or masked such that my identity is not revealed; and/or
- Don't know/ No response.

Our survey results suggested that the aggregation and masking of personal information is the most desired type of data control, with 55–72% of respondents selecting this option in every category. Opting out was also frequently selected, especially in the context of targeted advertisements (67%), behaviour prompting (61%), and sale of personal data (58%). Notification in the fine print was the least-selected option (24–34%)(Table 5). These results suggest a high level of concern for data anonymity among survey participants, as well as a preference for opting in and out of the collection of personal information. They also suggest that nominal consent, where one is notified somewhere in the fine print that one's personal information will be used in a particular way, is prompted to click on "I agree," is not sufficient in the eyes of many participants.

Participants wished to see greater levels of control over private uses of their data. In the case of targeted ads, 69% of respondents thought that the use of their personal information "should not be permitted." Of the 27% of

participants who would permit targeted advertising if certain rights and protections were granted, 67% wished to be able to opt out, 58% to be able to opt in, and 50% to be able to delete their data.

Fewer participants expected to have such control over their data for public uses such as crime prevention and traffic planning, but many participants (42–44%) still wished to be able to view their information in those contexts, and some also wished to have other types of controls, such as the ability to opt out, opt in, delete their data, correct their data, and download their data.

Table 5

	Crime	Traffic	Ads	Sale	Business	Behavior	Total
My data is aggregated with other data or masked such that my identity is not revealed	61%	72%	55%	58%	61%	58%	61%
I can opt out	34%	52%	67%	58%	51%	61%	54%
I opt in	32%	46%	58%	59%	51%	58%	51%
I can view my data	42%	44%	49%	45%	40%	55%	46%
I can delete my data	25%	38%	50%	40%	42%	47%	40%
I can correct my data	30%	31%	41%	36%	28%	40%	34%
I can download my data for my own use	26%	31%	30%	28%	30%	43%	31%
I'm notified somewhere in the fine print when I agree to use a service	24%	25%	34%	35%	26%	30%	29%
Don't know/ No response	5%	1%	1%	0%	3%	1%	2%

Targeted advertisements

With regards to personalized advertisements, a total of 27% of survey respondents were promoted into this question series—fewer than for other types of uses. This is indicative of a greater aversion to targeted advertisements; most respondents had indicated that they did not want their personal information collected for targeted advertising, and thus were not promoted into this question series. However, most respondents who indicated their willingness to share their data on the condition that certain rights and privileges were afforded to them, wanted to be able to "opt out", "opt in", have their data aggregated and/or be able to delete their data. According to the survey, these four provisions held the highest selection rate.

The highest number or responses, 67%, agreed to sharing personal information if they could "opt out"; 58% agreed on condition that they can "opt in"; 55% agreed on the condition that their data is aggregated with others; 50% on condition that they can delete their data; 49% on condition that they can view their data; 41% on condition that they can view their data; 34% agreed to the sharing of personal data as long as they are notified in the fine print; and 30% wanted to be able to download their data for their own use (Figure 8).

Participants under the age of 35 were more likely than other age groups to make the use of their personal information for targeting ads conditional on the protections and rights indicated. This may indicate greater comfort among young people in navigating the processes of data management, possibly due to greater familiarity with targeted ad systems on social media platforms or a higher level of digital literacy among young people.

Behaviour modification

Forty-nine percent of respondents answered that they would permit the use of their personal information for behaviour modification on condition that certain rights and privileges were granted, and were thus promoted into the survey question asking which rights and privileges they would require. A majority of these respondents wanted to be able to "opt out"/"opt in", have their data aggregated, and to be able to view their data. Sixty-one percent of respondents wanted to be able to opt out; 58% to opt in; 58% agreed to sharting their data if it is aggregated or masked; and 55% if they could view their data. Forty-seven percent of respondents wanted to be able to delete their data; 43 % to download their data; 40% to correct their data; and 30% agreed to collection as long as they were able to view the fine print (Figure 9).

Again, there was a significant relationship between age and employment and the conditions participants placed on the use of their personal information for behaviour modification, with younger and employed respondents requiring data rights and protections more than their counterparts in other age groups and those unemployed respectively.

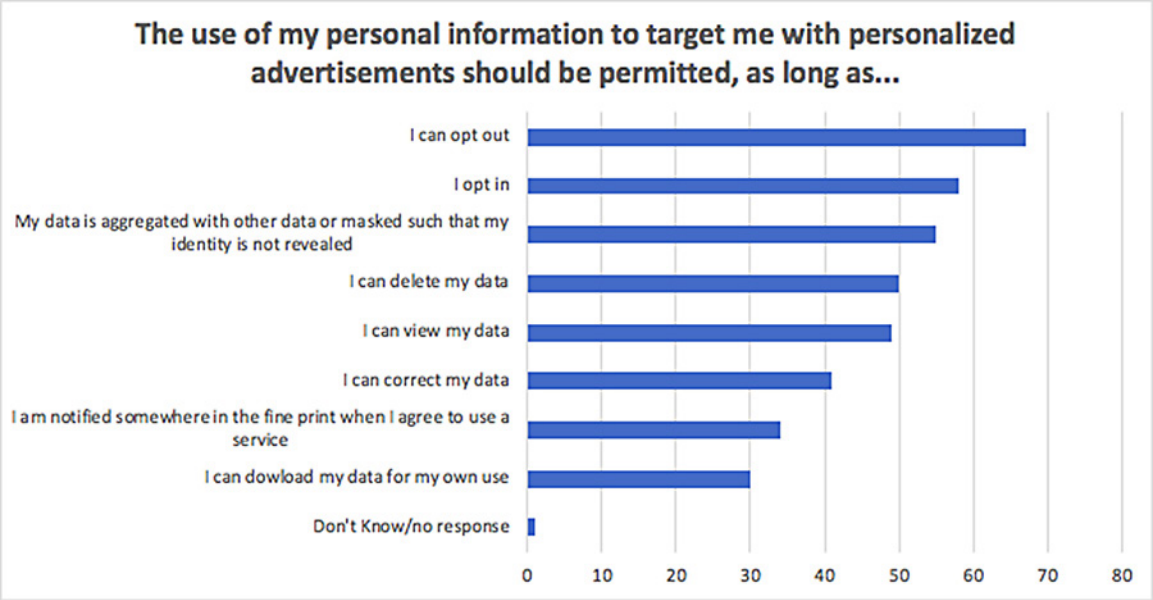

Figure 8

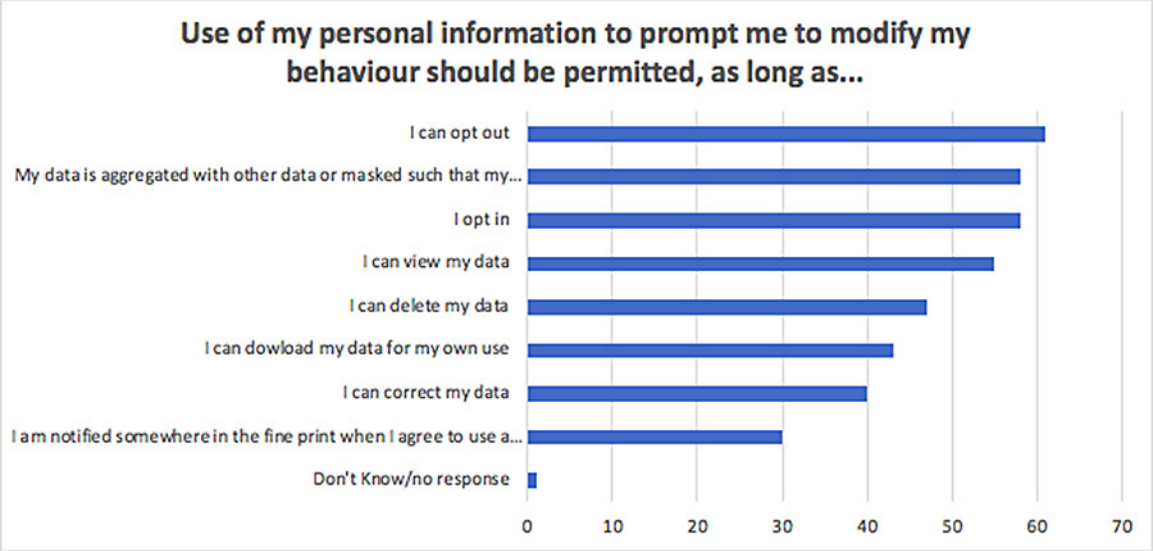

Figure 9

Traffic and transit planning

Fifty-six percent of respondents indicated their willingness to share personal data for traffic and transit planning as long as they were granted certain rights and privileges. Seventy-two percent of respondents agreed to the collection of their personal data for traffic and transit as long as this data was aggregated or masked. Fifty-two percent wanted to be able to opt out; 46% to opt in; 44% wanted to view the data; 38% to be able to delete their data; 31% to download their data for personal use; 31% to correct their data; and 25% wanted to be able to view the fine print (Figure 10).

Again, there was a significant positive correlation with age and with being employed and wishing to see rights and privileges as a condition of using personal information for traffic and transit planning.

Policing

Forty-four percent of respondents indicated they would allow their data to be gathered for use by police in crime prevention only condition that rights and protections be afforded to them. Of those rights and protections, a majority

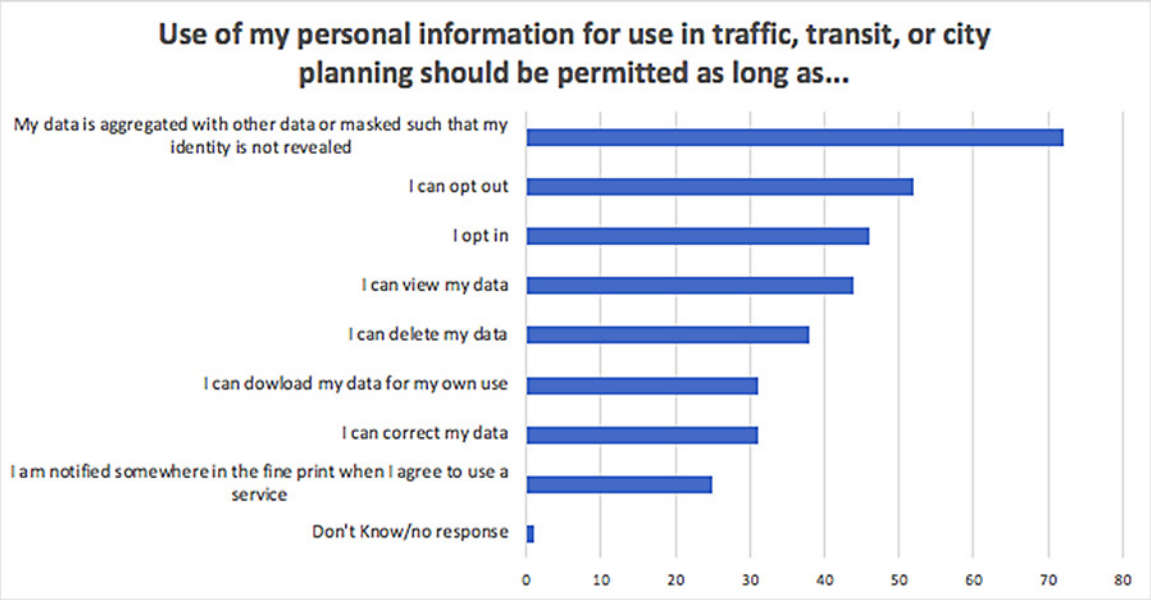

Figure 10

of 61% wanted their data to be aggregated and masked. A further 42% wanted to view their data; 34% wanted to be able to opt out; 32% to opt in; 30% wanted to be able to correct their data; 26% to download it for personal use; 25% wanted to be able to delete their data; and 24% wanted to be notified in the fine print (Figure 11).

Once again, a significant positive correlation with age is noted. Again, this could be indicative of a higher degree of comfort with data management among younger respondents.

Sale of Data

Only nine percent of survey participants were comfortable with the sale of their data, even with certain rights and privileges afforded to them. This is indicative of the high degree of discomfort with the sale of personal information; most respondents did not want their data collected for the purpose of selling it regardless of what rights or privileges they might be granted. Of those few that would permit the sale of their personal information on the condition that

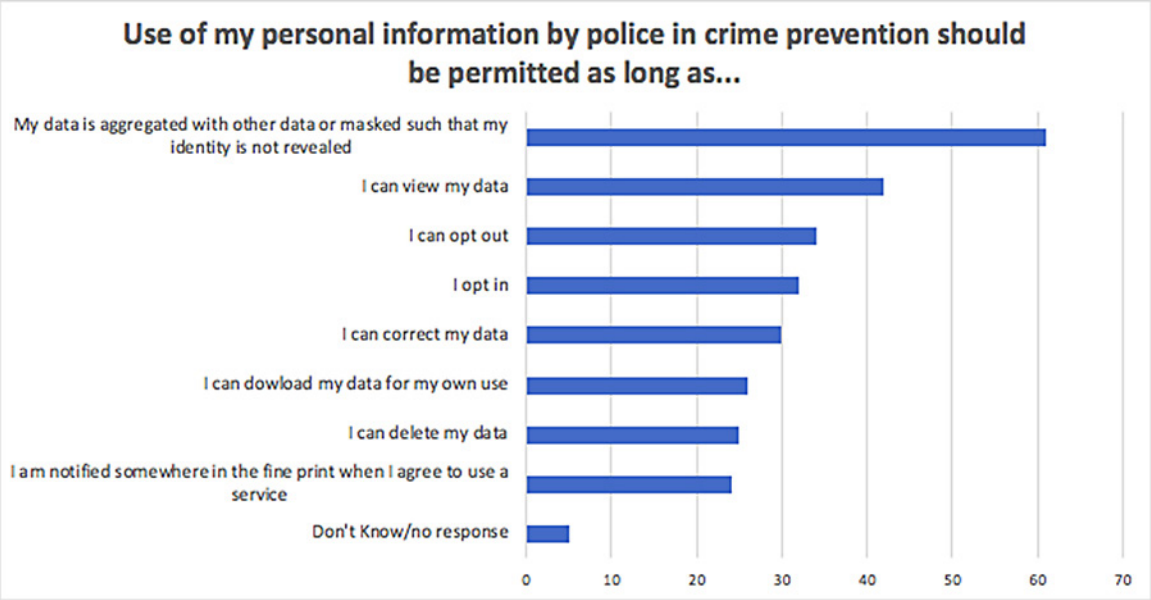

Figure 11

certain rights and privileges were granted, 59% wanted to be able to opt in; 58% opt out; 58% wanted their data to be aggregated with others; 45% wanted to be able to view their data; 40% to delete their data; 36% to correct their data; 35% to be notified in the fine print; and 28% to download their data (Figure 12).

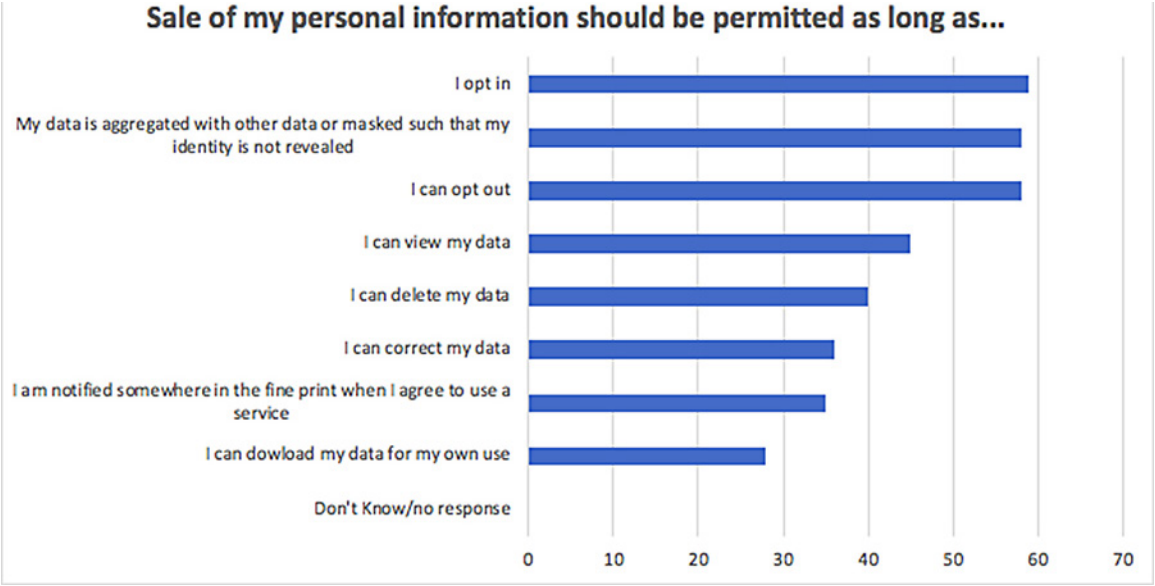

Figure 12

Private business use

Thirty-nine of survey participants were comfortable with the use of their personal data for use in private business if certain rights and privileges were granted. Of those, 61% would require that their data be aggregated; 51% would want to be able to opt in, and 51% wanted to be able to opt out. A further 42 wanted to be able to delete their data; 40% wanted to be able to view their data; 30% to download their data; 28% to correct their data; and 26% wanted to be notified of data collection in the fine print (Figure 13). Canadians under the age of 35 and employed Canadians were significantly more likely than those of other age groups and those employed respectively to permit such uses on condition that certain rights and privileges were granted.

Rights and privileges

With regards to the kinds of rights and privileges expected over personal data collection, the survey suggested specific data control mechanisms and asked respondents to gauge their agreement on a five-point Likert scale, from "Strongly Agree" to "Strongly Disagree." A strong majority of Canadians strongly agreed that they should have the right to view the personal information that has been collected on them (80%). A majority of Canadians also strongly agreed that they should be able to delete that data (66%), as well as download it (65%). Interestingly, many Canadians (37%) did not agree with the statement "if I do not want to share my personal information in the way that a service provider sets out in their privacy policy, I should simply not use the service" (Figure 14). Not using the service is currently, in many cases, the only option available to Canadians who do not agree with a company or service provider's privacy policy. This survey finding suggests that Canadians are not satisfied with the current model of notice and consent which often provides only the options of agreeing with a privacy policy or not using a service.

Privacy of particular types of data

The survey asked respondents to rate "how private/sensitive" they felt the following types of personal information were on a three-point Likert scale: from "very private or sensitive," to "somewhat private or sensitive," to "not private or sensitive."

Face recognition and image data, device identification numbers, IP addresses, web surfing histories, and location data were all viewed as less sensitive than pieces of personal information that are traditionally treated as very

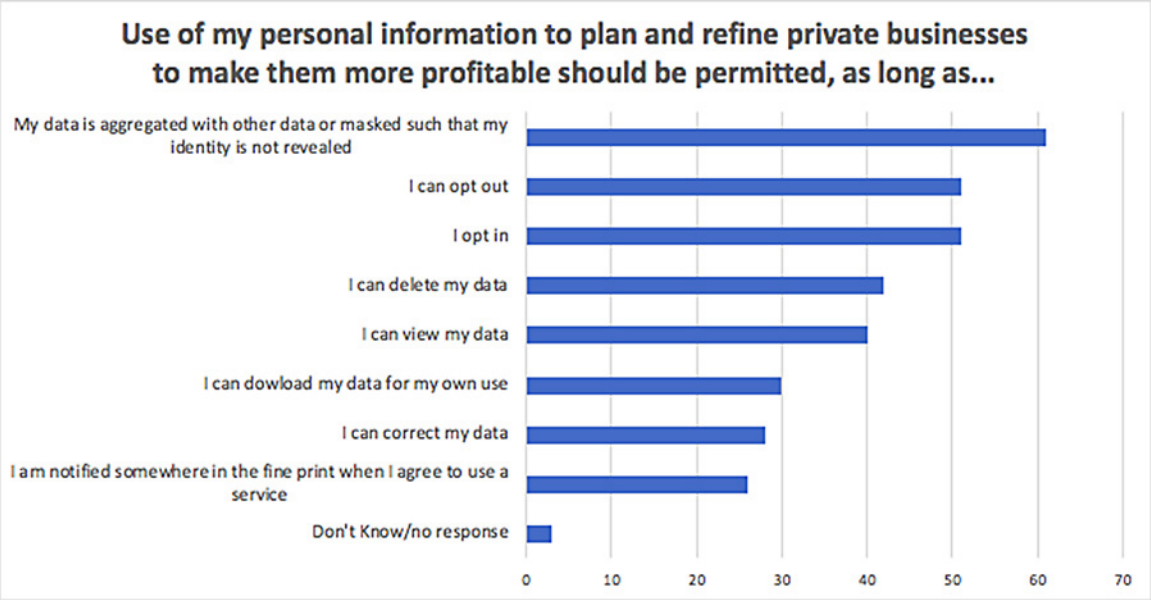

Figure 13

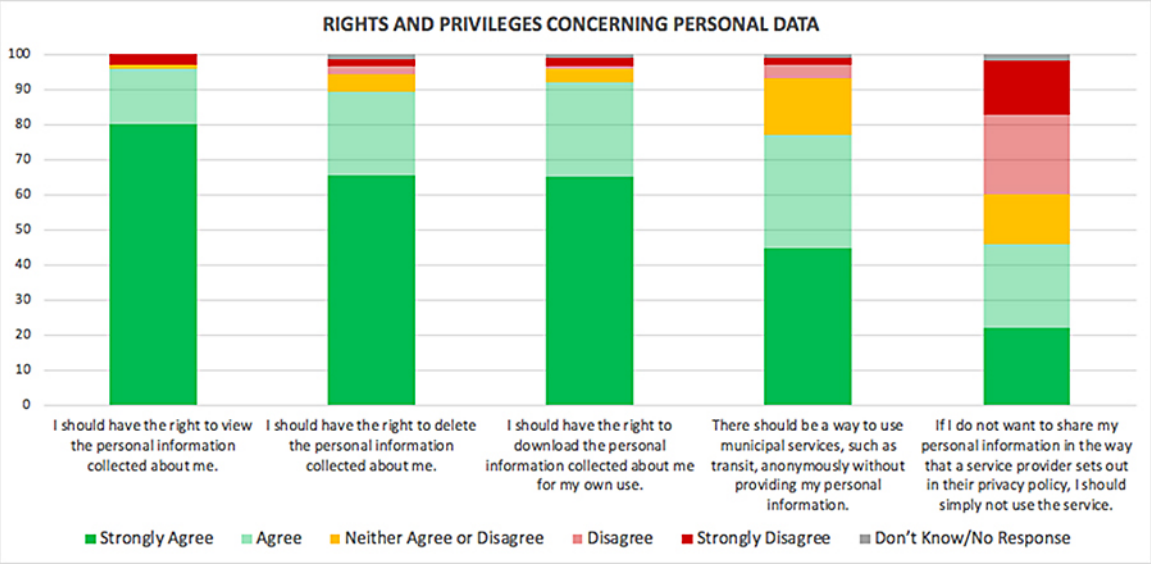

Figure 14

private: Social Insurance Numbers and Credit Card numbers (Figure 15). This may indicate that Canadians are slow to realize the possible sensitivities of these types of data and the uses to which they could be put. At the same time, Canadians recognized these types of data as more sensitive than a person's address, name, or phone number. Email addresses were viewed as less sensitive than physical addresses. There was little recognition among Canadians of the sensitivity or privacy of hydro use and transit data; there were rated the least private of all the types of data listed.

Conclusions

Overall, our survey findings suggest that Canadians are concerned about their privacy in the development of smart cities. Other findings indicate that many Canadians desire broader protection and control over their personal data. While many did not want to have their personal information collected at all, those who would permit the use of their personal information wished to have levels of control over that data that are, often, not currently available, such as the ability to opt out, view, correct, download and delete their data. This was particularly true regarding data use by private businesses, as opposed to public data uses, but many Canadians wished to see greater levels of control in a public context as well.

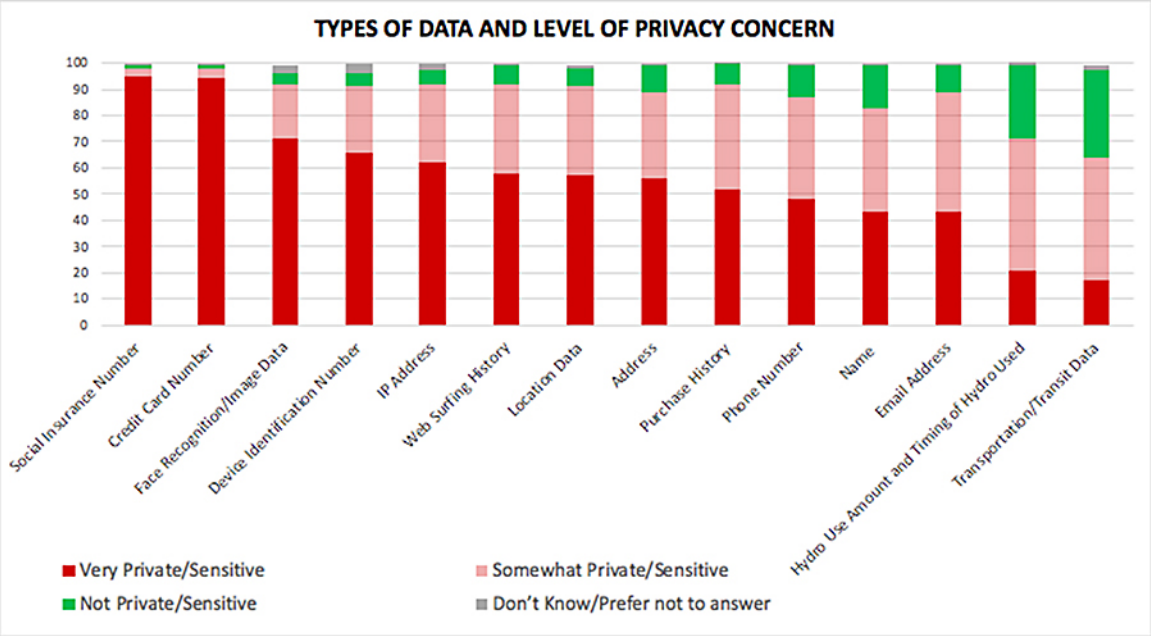

Figure 15

The survey also demonstrates that the intended purpose and use of data gathering influences respondents' attitudes towards its collection. The sale of personal data is the most strongly opposed use that we examined. Canadians also objected strongly to the use of personal data for targeted advertising and behaviour modification, while data collection for public uses such as transit and city planning is not as strongly opposed.

With respect to demographic characteristics, adults age 55-64 may be less concerned about smart-city privacy, possibly due to a lower awareness of privacy risks (Elueze and Quan-Haase 2018; Advocis and The Financial Advisors Association of Canada 2006). College-educated working-class people, may be less concerned about smart-city privacy, possibly due to habituation to higher levels of surveillance by workplace authorities or lower levels of awareness about privacy risks (Eubanks 2018) or the privacy risks associated with smart-city technologies in particular.[6] Awareness-raising about the privacy risks associated with smart-city technologies may be worthwhile among these groups. However, in the context of policing, the potential privacy risks associated with smart-city technologies may be more apparent to those often affected by surveillance; visible minorities and Indigenous groups, as well as men in general, may be more concerned about data collection in the context of policing and crime prevention.[7]

Our survey results were limited in that Aboriginal and visible minorities, LGBTQ people, and people with disabilities were underrepresented in the survey as a true percentage of the Canadian population. As critical data studies scholars recognize, is important to recognize what (and who) is missing in data sets, and further quantitative or qualitative studies could weight and include minority groups appropriately (Dalton, Taylor, and Thatcher 2016; Hawkins and Burns 2018). As well, our survey could be biased by the online format of the survey instrument, as participants who are unwilling or unable to participate in an online survey might have different attitudes towards privacy and technology than those willing to take part in online surveys; inclusion of other survey formats might permit more representative results.

Our findings suggest privacy and digital literacy are important factors to consider as smart-city technologies roll out. Moreover, due to the high degree of concern over the privacy, data collection in the smart-city context should look beyond de-identification measures as a first strategy, towards data control and self-management mechanisms baked into the technologies themselves. Self-management can include granting to users the ability to opt in, opt out, delete, download, correct, and manage their data. Canadians want control of their data that goes beyond simple notice of how their data is used somewhere in the fine print. They want the options to opt out, opt in, view, delete, correct, and download their data.

As the Sidewalk Labs project continued to unfold and criticisms continued to mount, the company retracted some of their original proposals. For example, they scrapped plans for an urban data trust, instead transferring the governance of all collected data to Waterfront Toronto (Vincent 2019). Such changes were prompted by broad-based

criticisms of Sidewalk Lab's original approach to data privacy. Reading this alongside our survey findings, it appears that Sidewalk Labs, and some other corporate-led smart city projects, do not begin with a citizen-focused approach to data policy development, but rather may respond to concerns raised by experts and community organizations piecemeal and after the fact.

This research demonstrates that Canadians are wary of smart cities, as well as of the collection and use of their personal information more broadly. It appears that that some current frameworks within which smart cities operate are not citizen-focused approaches. Canadians are more open to government uses of information such as in traffic and city planning, especially if they are granted rights and protections in their data. They object strongly to private business uses of their personal information, such as the sale of their personal information, its use to target them with ads, and even to its use to make businesses more profitable. Our findings demonstrate that the quasi-governance roles being taken up by private companies may not be in tune with the desires of Canadians. This should cause municipalities to think twice about instituting smart-city projects that are profit-motivated or business-led. Municipalities should tread carefully and engage in as much public consultation as possible as they re-conceptualize and remodel infrastructures around digital platforms.

Acknowledgements

This study was funded by the Office of the Privacy Commissioner of Canada (OPC). The views expressed herein are those of the project researchers and do not necessarily reflect those of the OPC. This research was undertaken, in part, thanks to funding from the Canada Research Chairs program and McMaster University. The authors wish to thank Emmanuel Appiah, Charles Breton, Michelle Dion, David Fewer, Nicole Goodman, Keri Greiman, Blayne Haggart, Jean-Noé Landry, Sumana Naidu, Peck Sangiambut, Teresa Scassa, Chranjot Shokar, Maureen Smith, Ian Steinberg, Natasha Tusikov, Clifton van der Linden, and Earl Washburn. Any errors are our own.

Notes

[1] Percentages have been rounded for ease of reading and may therefore not sum to 100. MoEs for provinces: British Columbia:8.7; Alberta: 9.22; Saskatchewan and Manitoba: 12.45; Ontario: 5.01; Quebec: 6.16; Atlantic provinces: 11.71. MoEs for computed ages: <35 6.2; 35-44:7.85; 45-54: 7.28; 55-64:7.22; 65+: 6.56. MoEs for gender: male: 4.45; female; 4.33. MoEs for education level: high school or less: 6.2; college: 5.37; university: 4.78. MoEs for employment status: employed: 3.96; unemployed: 4.98. MoE for minority status: Non white: 9.85; Persons with disabilities: 10.51; LGBT:12.35; none: 3.57.

[2] The tables that follow bear the indications of significance level indicated as follows: Significance level 0.999: ++++; 0.99:+++; 0.95:++; 0.9:+; -0.999: ----; -0.99:---; -0.95:--; -0.9:-.

[3] Results are not considered representative of Canadians who are visible minorities or Indigenous people as a whole; the margin of error is +/- 9.85 for this group 19 times out of 20.

[4] Results are not considered representative of Canadians who are visible minorities or Indigenous people as a whole; the margin of error is +/- 9.85 19 thes out of 20 for this group.

[5] The findings in this section are not considered representative of all Canadians; the margin of error is +/- 5.94 19 times out of 20.

[6] Results are not considered representative of Canadians who are visible minorities or Indigenous people as a whole; the margin of error is +/- 9.85 for this group. The margin of error for college-educated Canadians is +/- 5.37.

[7] Again, results are not considered representative of Canadians who are visible minorities or Indigenous people as a whole; the margin of error is +/- 9.85 for this group.

References

Advocis, and The Financial Advisors Association of Canada. 2006. *POLLARA Report on Canadians' views of banks and life and health insurance*. https://insurance-journal.ca/media/docs/advocispollara.pdf.

Agosto, D. E., and J. Abbas. 2017. 'Don't be dumb—that's the rule I try to live by': A closer look at older teens' online privacy and safety attitudes. *New Media & Society* 19 (3): 347–365.

Albino, V., U. Berardi, and R. M. Dangelico. 2015. Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology* 22 (1): 3–21.

Arora, P. 2018. Decolonizing privacy studies. *Television and new media*, 1527476418806092.

Arora, P., and L. Scheiber. 2017. Slumdog romance: Facebook love and digital privacy at the margins. *Media, Culture & Society* 39 (3): 408–422.

Author 1, Author 2, Author 3, and Author 4. 2019. *Map*. Web Site Title Withend for Blind Review. 2019. http://www.witheldforblindreview.com.

Bartel Sheehan, K. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13 (4): 24–38.

Batty, M., K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali. 2012. Smart cities of the future. *The European Physical Journal Special Topics* 214 (1): 481–518.

Beamish, B., D. Therrien, J. Chartier, C. Tully, C. Paquin, M. McEvoy, K. Rose, et al. 2018. *Smart cities challenge.* April 24, 2018. https://oipc.sk.ca/assets/joint-letter-smart-cities-challenge.pdf.

Blackwell, L., J. Hardy, T. Ammari, T. Veinot, C. Lampe, and S. Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 610–622. ACM.

Bloom, R., T. P. Lauriault, and J-N. Landry. 2018. *Open smart cities in Canada: Assessment report*. Open North. https://www.opennorth.ca/open-smart-cities-guide.

Campbell, T. 2012. *Beyond smart cities: How cities network, learn and innovate*. Abingdon, Oxon ; New York, NY: Earthscan.

Caragliu, A., C. Del Bo, and P. Nijkamp. 2011. Smart cities in Europe. *Journal of Urban Technology* 18 (2): 65–82.

Dalton, C. M., L. Taylor, and J. Thatcher. 2016. Critical data studies: A dialog on data and space. *Big Data & Society* 3 (1): 2053951716648346.

Edwards, L. 2016. Privacy, security and data protection in smart cities: A critical EU law perspective. *European Data Protection Law Review* 2: 28.

Elueze, I., and A. Quan-Haase. 2018. Privacy attitudes and concerns in the digital lives of older adults: Westin's Privacy Attitude Typology revisited. *ArXiv Preprint ArXiv:1801.05047*.

Eubanks, V.. 2014. Want to predict the future of surveillance? Ask poor communities. *The American Prospect*, January 15, 2014. https://prospect.org/article/want-predict-future-surveillance-ask-poor-communities.

———. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor*. First edition. New York, NY: St. Martin's Press.

Finch, K., and O. Tene. 2013. Welcome to the metropticon: Protecting privacy in a hyperconnected town. *Fordham Urb. LJ* 41: 1581.

Gangadharan, S. P. 2017. The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal internet ssers. *New Media & Society* 19 (4): 597–615.

Hawkins, B. W., and R. Burns. 2018. Queering (meta) data ontologies. In *Proceedings of the 4th Conference on Gender and IT*, 233–234. ACM.

Hiller, J. S., and J. M. Blanke. 2016. Smart cities, big data, and the resilience of privacy. *Hastings Law Journal* 68: 309–56.

Hoofnagle, C. J., J. King, S. Li, and J. Turow. 2010. *How different are young adults from older adults when it comes to information privacy attitudes and policies?* https://repository.upenn.edu/cgi/viewcontent.cgi?article=1413&context=asc_papers.

Information and Privacy Commissioner of Ontario. 2018. *Smart cities and your privacy rights: Technology fact sheet*. https://www.ipc.on.ca/wp-content/uploads/2018/04/fs-tech-smart-cities.pdf.

———. 2019. *2018 Annual Report*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/2019/06/ar-2018-e.pdf.

Infrastructure Canada. 2018. *Smart cities challenge*. Infrastructure Canada. November 19, 2018. https://www.infrastructure.gc.ca/cities-villes/index-eng.html.

Jai, T-M. C., and N. J. King. 2016. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers?" *Journal of Retailing and Consumer Services* 28: 296–303.

Jensen, C., C. Potts, and C. Jensen. 2005. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63 (1–2): 203–227.

Kitchin, R.. 2014. The real-time city? Big data and smart urbanism. *GeoJournal* 79 (1): 1–14.

———. 2016. Getting smarter about smart cities: Improving data privacy and data security. Kitchin, R., T. P. Lauriault, and G. McArdle, eds. 2018. *Data and the City*. Routledge.

Lauriault, T., R. Bloom, and J-N. Landry. 2018. *Open smart cities guide V1*. Open North. https://www.opennorth.ca/open-smart-cities-guide.

Maréchal, N. 2015. First they came for the poor: Surveillance of welfare recipients as an uncontested practice. *Media and Communication* 3 (3): 56–67.

Mosco, V. 2019. *Smart city in a digital world*. S.l.: Emerald Group.

Murakami Wood, D. 2015. Smart city, surveillance city. *SCL: Tech Law for Everyone* (blog). July 1, 2015. https://www.scl.org/articles/3405-smart-city-surveillance-city.

Office of the Privacy Commissioner of Canada. 2016. *The internet of things: An introduction to privacy issues with a focus on the retail and home environments*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/.

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. n.d. *Open smart cities FAQ*. https://cippic.ca/en/Open_Smart_Cities.

Scassa, T. 2017a. *Smart cities: Data ownership and privacy issues*. Teresa Scassa's Blog. February 14, 2017. https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=241:smart-cities-data-ownership-and-privacy-issues&Itemid=81.

———. 2017b. Who owns all the data collected by 'Smart Cities'? *The Star*. November 23, 2017. https://www.thestar.com/opinion/contributors/2017/11/23/who-owns-all-the-data-collected-by-smart-cities.html.

Scassa, T., J. A. Chandler, and E. F. Judge. 2011. Privacy by the wayside: The new information superhighway, data privacy, and intelligent transportation systems. *Saskatchewan Law Review* 74 (1): 87–135.

Scassa, T., and A. Sattler. 2011. Location-based services and privacy. *Canadian Journal of Law and Technology* 9 (1 & 2).

Sidewalk Toronto. 2018. *Plan development agreement between Toronto Waterfront Revitalization Corporation and Sidewalk Labs LLC.* https://sidewalktoronto.ca/wp-content/uploads/2018/07/Plan-Development-Agreement_July312018_Fully-Executed.pdf.

Toronto Region Board of Trade, and Environics Research. 2019. *Quayside GTA survey report*. https://www.bot.com/Portals/0/NewsDocuments/Environics%20-%20Board%20of%20Trade%20-%20Polling%20FGTA2019%20-%20Report.pdf.

Van Zoonen, L. 2016. Privacy concerns in smart cities. *Government Information Quarterly* 33 (3): 472–480.

Vincent, D. 2019. "Sidewalk labs set to release details of all the data it wants to collect at Quayside." *The Star* (blog). November 1, 2019. https://www.thestar.com/news/gta/2019/11/01/sidewalk-labs-set-to-release-details-of-all-the-data-it-wants-to-collect-at-quayside.html.

Youn, S., and K. Hall. 2008. Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior* 11 (6): 763–765.

Zanella, A., N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. 2014. Internet of things for smart cities. *IEEE Internet of Things Journal* 1 (1): 22–32.