Privacy and Smart Cities: A Canadian Survey

By Sara Bannerman and Angela Orasch[1]

Introduction

This report presents the findings of a national survey of Canadians about smart-city privacy conducted in October and November 2018. Our research questions were: How concerned are Canadians about smart-city privacy? How do these concerns intersect with age, gender, ethnicity, and location? Moreover, 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?

What is a smart city?

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).

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 questions and concerns from experts in data privacy and the public at large regarding 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, if any, would ensure that protection?

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 (Bannerman et al. 2019).

[1] 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 Keri Greiman, David Fewer, Teresa Scassa, Nicole Goodman, Blayne Haggart, Clifton van der Linden, Earl Washburn, Maureen Smith, Natasha Tusikov, Chranjot Shokar, Emmanuel Appiah, Sumana Naidu, Ian Steinberg, Peck Sangiambut, and Jean-Noé Landry. Any errors are our own.

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 that 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).

Smart-city technologies move quickly from development to adoption, often outpacing the social and political deliberations necessary to consider their effects in detail. 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.

Method

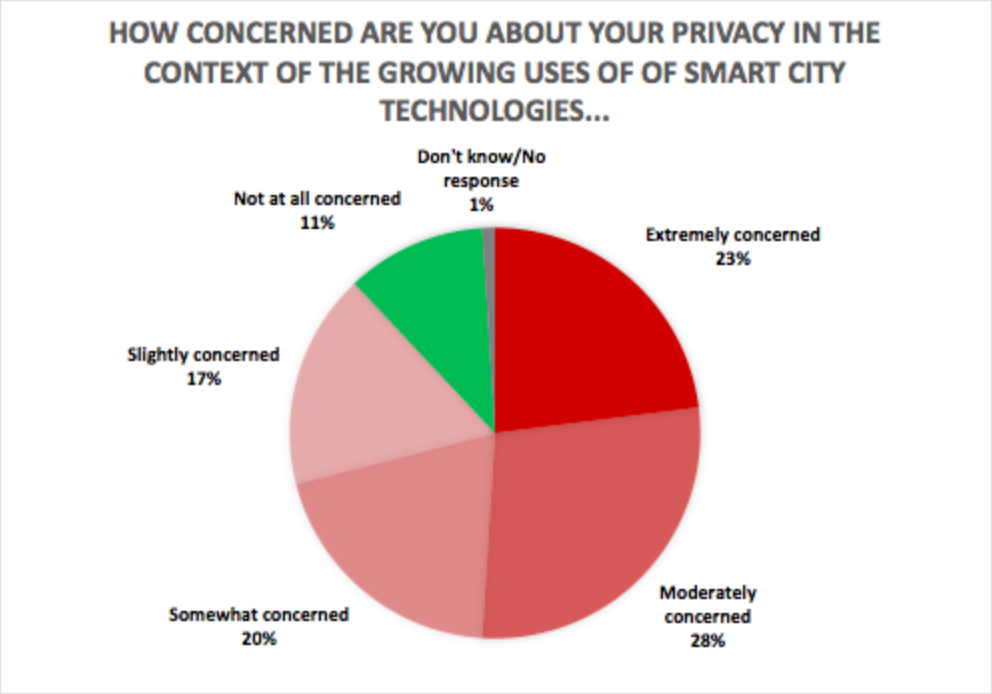
During October 23 to November 1 2018, we conducted an online survey of Canadians about their attitudes towards privacy in a smart-city context. Participants were recruited by EKOS Research Associates, drawn as a random stratified sample from a probability panel database and recruited using emailing scripts. The panel is based on the socio-demographic statistical parameters of the most recent Canadian census (2016). The survey itself was rim-weighted for location, 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 of +/-3.08, 19 times out of 20. It is representative of demographic subgroups with a reduced level of confidence. The margin of error is within 5 or less, 19 times out of 20, for Canadians identifying as men and women; for university-educated Canadians; for Canadians who are employed or unemployed; and for Canadians not identifying as a visible minority or Indigenous person, as a person with disabilities, or as an LGBT Canadian. The margin of error for Canadians from any province, any age group, for high-school-educated Canadians, and for college-educated Canadians ranges from +/- 5.01 to +/-12.45 19 times out of 20.

Survey findings

Overall privacy concern

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 percent of Canadians are concerned on some level about their privacy in the smart-city context, with 23 percent being extremely concerned, 29 percent saying they are moderately concerned, and 19 percent somewhat concerned. In general, these responses demonstrate a strong level of concern in the privacy issues surrounding smart cities.

The findings also suggest a few interesting demographic findings. Participants age 65 and up were less concerned than those from other age groups (35 percent were "not at all" or "slightly" concerned, compared with 28 percent on average). Our finding that older participants 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 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 percent) than average (28 percent) to say they were "not at all" or "slightly" concerned, while college-educated participants were less likely (23 percent) than the average Canadian (28 percent) to say they were ""not at all" or "slightly" concerned. Participants who self-identified as visible minorities or Indigenous were more concerned with privacy in the smart city than average (19 percent were "not at all" or "slightly" concerned, compared with 28 percent on average).[2]

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.

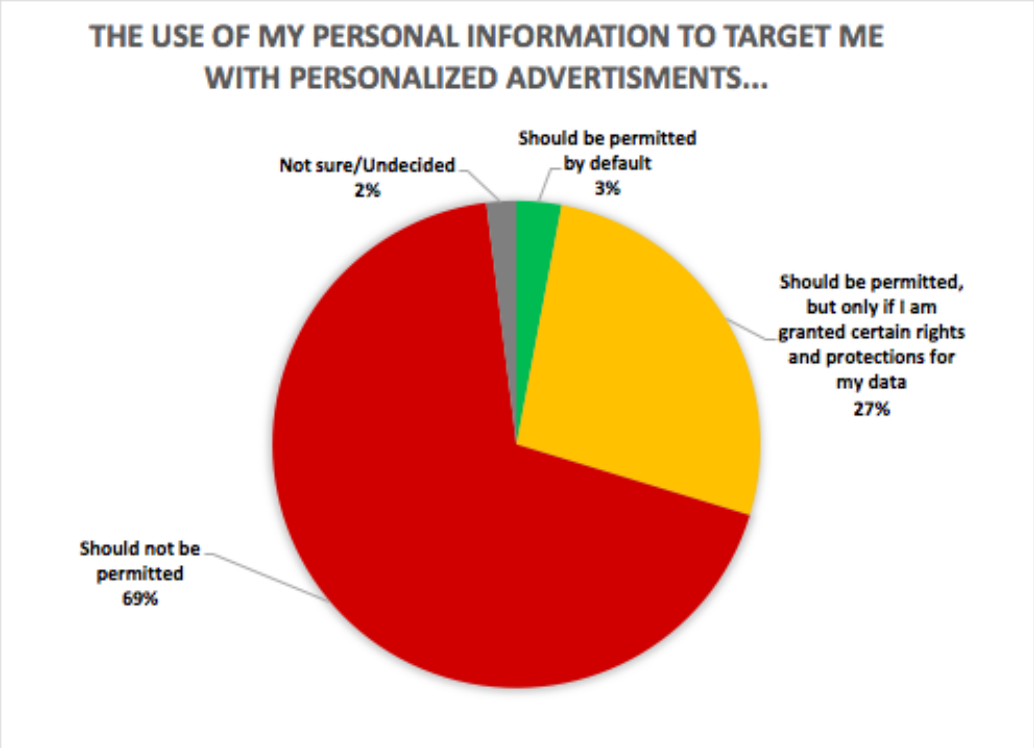
[2] Results are not considered representative of Canadians who are visible minorities or Indigenous people as a whole; the margin of error is +/- 9.85 for this group 19 times out of 20.

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 percent 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.

Participants under the age of 35 (4 percent), and Canadians who identified as men (4 percent), were significantly more likely than average (3 percent) 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 percent), university-educated Canadians (34 percent), Canadians who are employed (31 percent), and LGBTQ participants (39 percent), were significantly more likely than average (27 percent) 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 percent), and unemployed Canadians (74 percent), were more likely than average (69 percent) to say that the use of their personal information to target them with ads should not be permitted.

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).



The stronger level of concern among participants age 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 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).

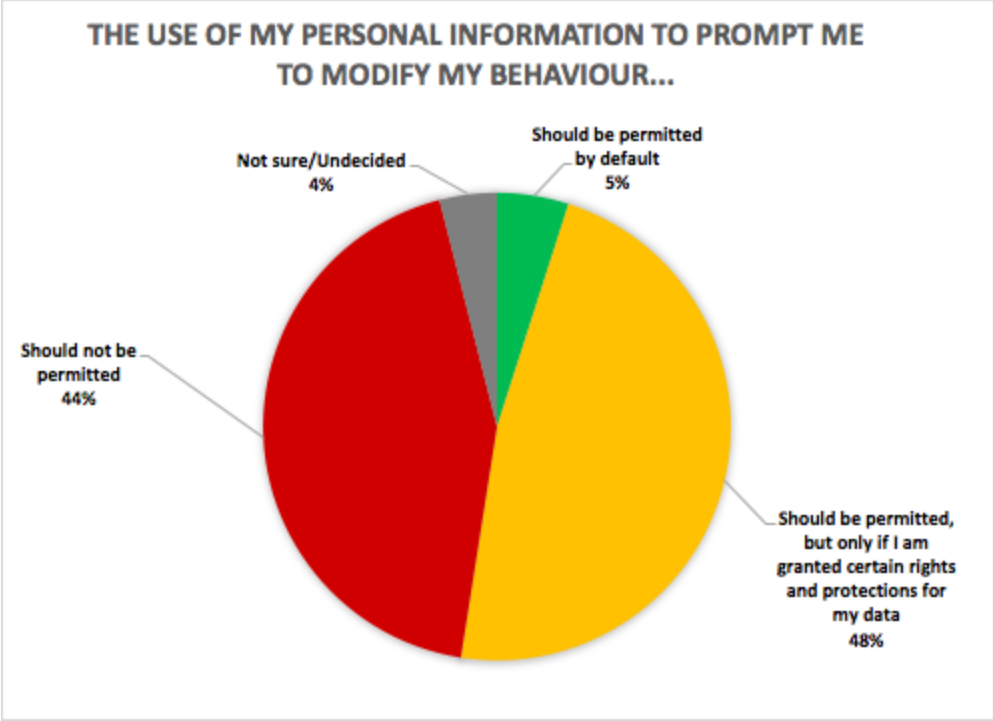
Unemployed Canadians were more likely (74 percent) than average (69 percent) to say that the use of their personal information to target them with ads "should not be permitted," rather than permitting such uses if they are granted certain rights and protections for their data. People with lower incomes 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."



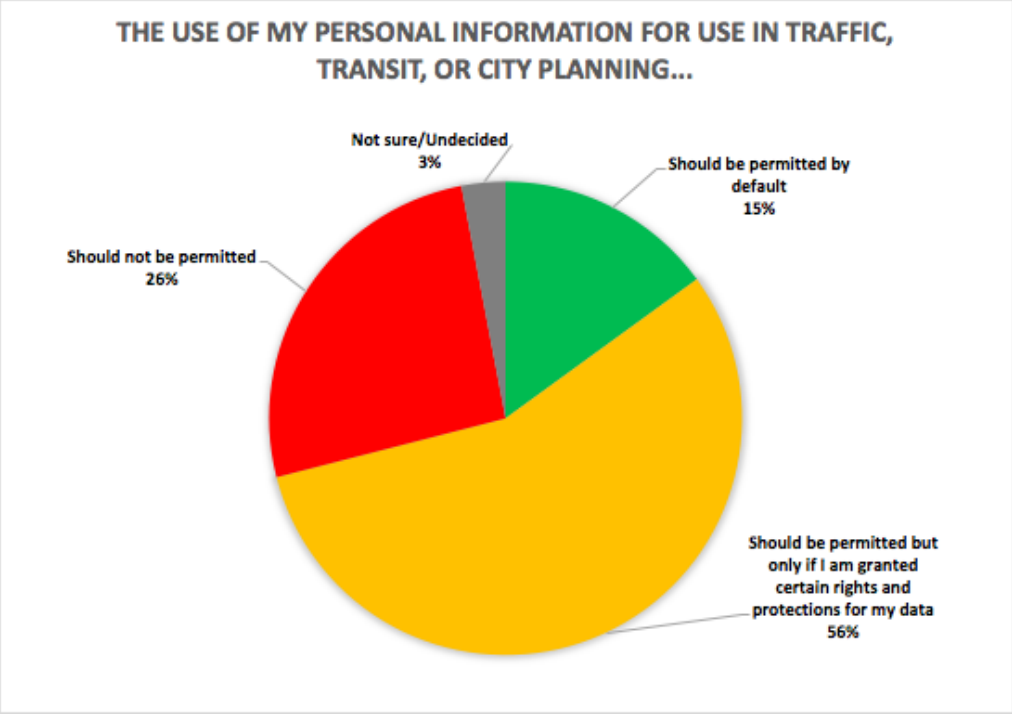
Forty-eight percent of Canadians felt that the use of their personal information to prompt them to modify their behaviour should be permitted, but only with the granting of certain rights and protections. A further 44 percent felt that this should not be permitted at all, suggesting there is a strong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

University educated (58 percent) and employed Canadians (52 percent), participants under 35 (56 percent), and LGBTQ participants (61 percent) 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 percent), unemployed Canadians (41 percent), and participants over 65 (49 percent), were more likely to say that this use should not be permitted at all.

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 percent) 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 percent felt that such uses should not be permissible at all. However, 17 percent 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.

Participants over the age of 65 (21 percent), men (18 percent), university educated Canadians (19 percent), and unemployed Canadians (20 percent), as well as participants from Alberta (23 percent), were more likely than average (15 percent) to say that such use should be permitted by default, whereas participants under the age of 35 (66 percent), employed Canadians (61 percent), and participants in Ontario (60 percent) were more likely to permit such uses if rights and protections were granted. High school-educated participants (30 percent) were more likely to say such uses should not be permitted at all.

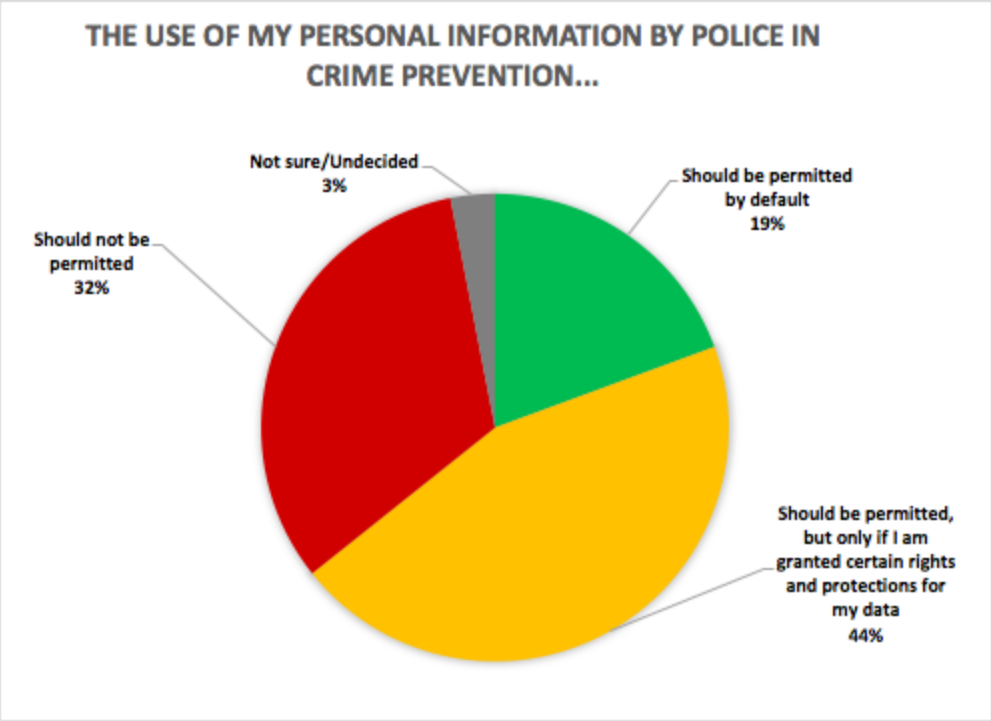
We see here the same lower level of concern and greater confidence in "certain rights and protections" among younger participants and university-educated Canadians as was revealed in previous questions. Interestingly, while employed Canadians, as in previous questions, were more willing to share their data on condition of "certain rights and protections," here, this corresponds with a *lower* level of permissiveness than the average Canadian--a lower willingness than average to share this data by default (as opposed to a lower likelihood of saying that such use should not be permitted, as compared with average Canadians, as was the case with previous questions). In other words, employed Canadians are less permissive than average, 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.

Unemployed Canadians were more likely than average 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 such uses should not be permitted. This may represent a greater trust in public authorities, or to a habituation to surveillance by public authorities, and lower confidence that rights and protections would useful to protect individual privacy.

Policing

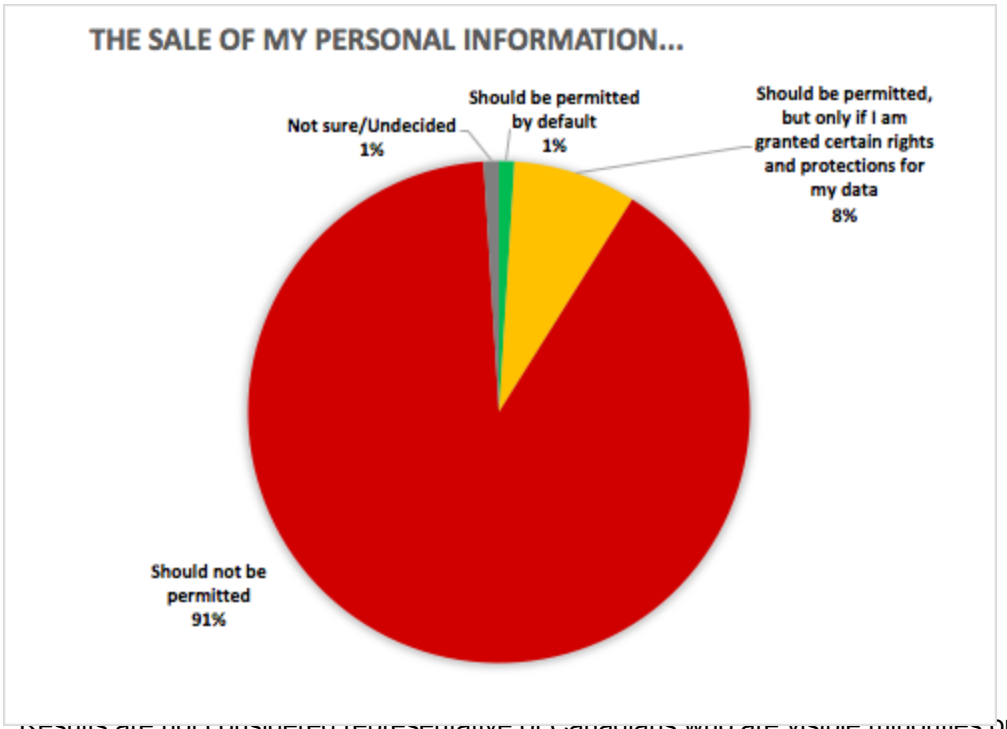
Noting that "police services can use personal data collected via web, smartphone app or social media activity to predict future behaviours of individuals or groups, and to take actions to prevent crime," the survey asked respondents to complete the sentence "Use of my personal information by police in 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 percent), or should only be collected if certain rights and privileges were afforded to individuals over this data (44 percent). The number of Canadians who felt that default permission was acceptable totalled only 19 percent. This suggests a strong level of concern regarding this type of data collection in the smart-city context.



Participants who identified as visible minorities and Indigenous people objected in greater number (together, 42 percent) to the collection of personal information for policing.[3] Men objected to this type of data collection more than women; forty percent of men (compared to 25 percent of women) said it "should not be permitted." Women were more likely to say that such uses should be permitted by default (22 percent), or should be permitted if certain rights and protections were granted (46 percent).

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 eight percent felt that the sale of their personal information should be permitted with certain rights and privileges afforded to the individual. This demonstrates a

[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 19 thes out of 20 for this group.

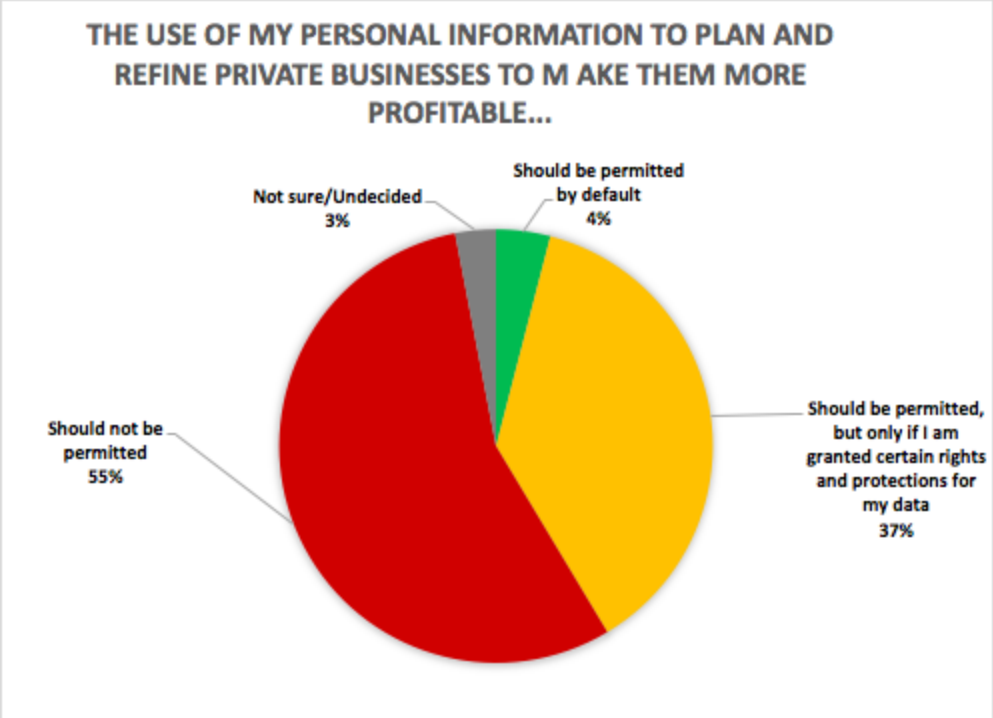
high degree of public concern over data sales.

Men (9 percent) were slightly more likely that women (6 percent) to accept the sale of their data with certain rights and privileges, as were university educated participants (14 percent) as compared to participants with high school or less (6 percent) or the average Canadian (8 percent).

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 percent felt that is should be permissible but with rights and protections, while only four percent felt it should be permissible by default. 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 percent) than the average (55 percent) to be unwilling to permit use of personal data for profit. University educated Canadians were more permissive, and more likely to allow their personal data to be used with certain rights and protections (42 percent, versus 37 percent on average). Unemployed Canadians were more willing to allow their data to be used in this manner by default (six percent, compared to four percent on average).

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 could be collected with certain rights, restrictions, and privileges for the purposes of targeted ads, behavior modification, traffic and transit planning, policing, sale, or profitability, were given a subset of questions to measure *under what conditions* this should be permitted.[4] 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.

	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%**

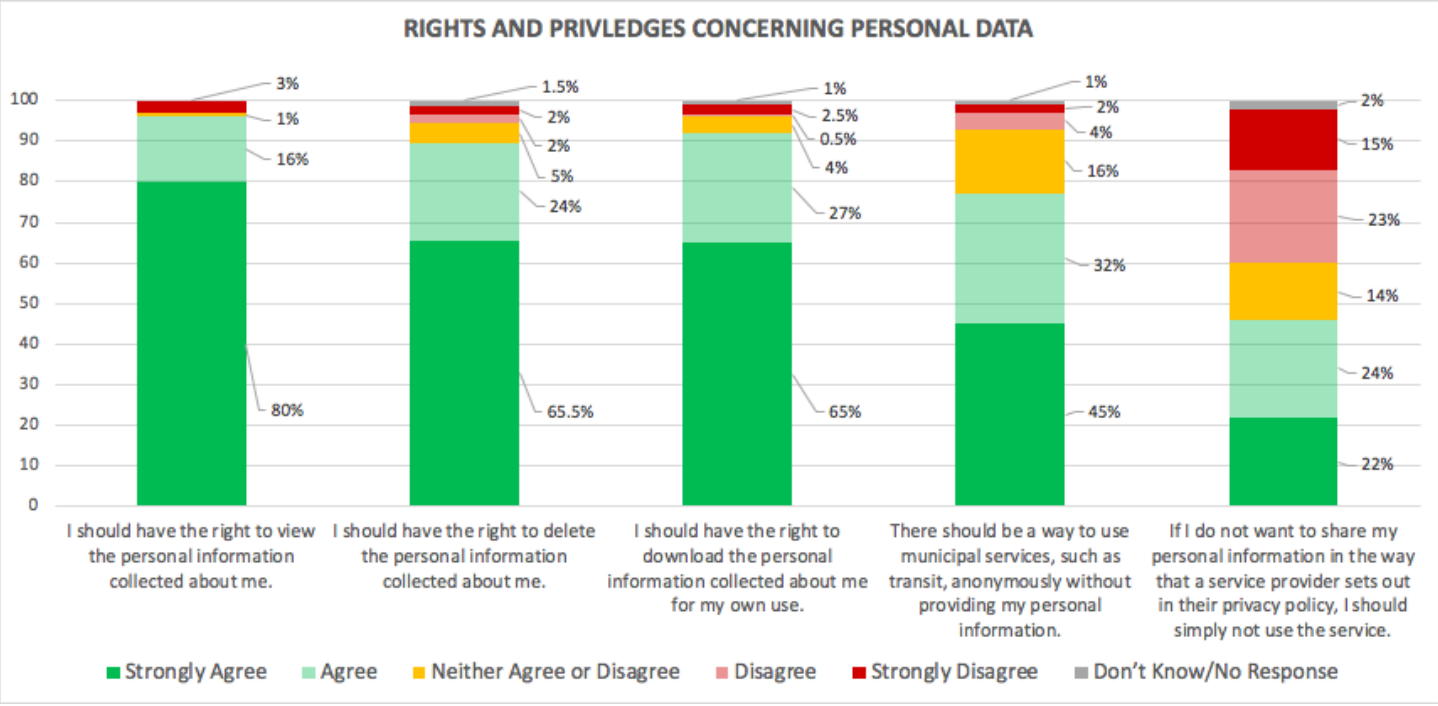
Our survey results suggest that the aggregation and masking of personal information is the most desired type of data control, with 55-72 percent of respondents selecting this option in every category. Opting out was also frequently selected, mostly in the context of targeted advertisements (67 percent), behaviour prompting (61 percent), and sale of personal data (58 percent). Notification in the fine print was the least-selected option (24-34 percent). 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.

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

Participants wished to see greater levels of control over private uses of their data. In the case of targeted ads, 69 percent of respondents thought that the use of their personal information "should not be permitted." Of the 27 percent of participants who would permit targeted advertising if certain rights and protections were granted, 67 percent wished to be able to opt out, 58 percent to be able to opt in, and 50 percent 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 percent) still wished to be able to view their information, 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.

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 percent). A majority of Canadians also strongly agreed that they should be able to delete that data (66 percent), as well as download it (65 percent). Interestingly, many Canadians (37 percent) 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." 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.



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.

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, older adults 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). Visible minority and Indigenous people, and college-educated working-class people, may be less concerned about smart-city privacy, possibly due to habituation to higher levels of surveillance by public and workplace authorities or lower levels of awareness about privacy risks (Eubanks 2018) or the privacy risks associated with smart-city technologies in particular.[5] 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.[6]

These 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.

This research demonstrates that Canadians are wary of smart cities, as well as of the collection and use of their personal information more broadly. 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

[5] 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.
[6] 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.

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. 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.

Bibliography

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, Denise E, and June 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.

Bannerman, Sara, Angela Orasch, David Fewer, and Keri Greiman. 2019. “Map.” Smart City Privacy. 2019. https://smartcityprivacy.ca/about/.

Bartel Sheehan, Kim. 1999. “An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors.” *Journal of Interactive Marketing* 13 (4): 24–38.

Elueze, Isioma, and Anabel 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, Virginia. 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.

Hoofnagle, Chris Jay, Jennifer King, Su Li, and Joseph 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.

Infrastructure Canada. 2018. “Smart Cities Challenge.” Infrastructure Canada. November 19, 2018. https://www.infrastructure.gc.ca/cities-villes/index-eng.html.

Jensen, Carlos, Colin Potts, and Christian Jensen. 2005. “Privacy Practices of Internet Users: Self-Reports versus Observed Behavior.” *International Journal of Human-Computer Studies* 63 (1–2): 203–227.

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.

Youn, Seounmi, and Kimberly Hall. 2008. “Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors.” *Cyberpsychology & Behavior* 11 (6): 763–765.