Recommendations: Towards a Privacy Code of Conduct for Smart Cities

By Sara Bannerman, David Fewer, Keri Grieman, and Angela Orasch
Draft of 19 March 2019

Contents

Preamble

Privacy is a growing concern as municipalities across the country put in place smart city technologies, from location-tracking technologies in transit and bike sharing, to health and education-related portals and mobile apps. Most Canadians (88 percent, according to our recent survey[1]) are concerned about their privacy in the context of the growing uses of smart city technologies.

These recommendations are intended to guide municipalities as they seek to institute smart city technologies and partnerships.

These recommendations proceed in the following groupings:

1. In Part One, we offer structural recommendations:
    a. we recommend legal and policy actions addressing privacy challenges in Canadian smart cities; and
    b. we recommend that smart city initiatives be undertaken in a manner that recognizes the ways in which data and technology can reaffirm social and economic inequities.
2. In Part Two, we offer recommendations for implementing smart city applications:
    a. we recommend implementing smart city technologies in ways that address privacy concerns at the outset, rather than as a reaction to those concerns; and
    b. we recommend caution in implementing smart city technologies in specific zones informed by existing privacy law and the results of our survey. These are “no go” and “proceed with caution” zones in which citizens express heightened privacy concerns.
3. In Part Three, we conclude by recommending the adoption of a robust set of data rights for individuals, confirmed in both legislation and smart city policies, that includes the right to view, delete, and download personal data.

[1] Bannerman, Sara and Angela Orasch. *Privacy and Smart Cities: A Canadian Survey*. January 15, 2019. Available at https://smartcityprivacy.ca

Part One: Structural Recommendations

Policy and Legal Governance Recommendations

1. **Develop a Smart City Policy.** All levels of government should develop principled policies on the implementation of smart city technologies. These policies should:
    - **Serve the Public Interest.** Smart cities should serve the interests of Canadians and be guided primarily by the needs of Canadians, and the goals and policy agendas of governments, rather than by commercial objectives of technology companies.
    - **Be Open by Default.** Smart cities should be grounded in transparent and responsive governance, open standards, interoperable technologies, open data, meaningful public engagement and democratic control.
    - **Involve Privacy Regulators at the Outset.** Smart city technologies pose difficult challenges to privacy laws and interests. Cities and their partners should develop standards, practices and governance structures in close consultation with privacy regulators. Such consultations will assist with both legal compliance and with the use of privacy regulatory tools.
    - **Develop Processes to Include Privacy Regulatory Tools.** Cities and their partners should develop standards and practices that ensure the astute use of tools such as privacy impact assessments and the inclusion of privacy by design methodologies in the development of city technologies and practices.
2. **Privacy Law Reform.** Smart city initiatives have laid bare the gaps in existing privacy legislation. Privacy law reform is required that will address:
    - **Enforcement Powers.** Grant privacy commissioners robust enforcement and oversight powers, including order-making powers, audit powers, and power to issue fines for violations of the law.
    - **Substantive Reform.** Modernize privacy laws to cover private and public sector dealings with personal information appropriate for a smart city and big data context. Canadian jurisdictions should be home to modern privacy regimes that are on a similar level to Europe's General Data Protection Regulation.
3. **Assume Leadership.** Governments should take the lead role in smart city projects, including the design of the data governance structures.
4. **Assert Privacy Laws and Principles.** Key privacy principles, such as consent, data minimization and identifying purposes must be incorporated in smart city data governance designs.
5. **Data Governance.** Data governance in the smart city is a civic responsibility. Address key decisions about responsibility for the the collection, use, sharing and safe-keeping of the different categories of data generated by smart city technologies in a transparent, principled and coherent fashion rather than in an ad hoc or reactive manner.
6. **Data Localization is Non-Negotiable, and an Opportunity**. Canadians' data should reside in Canada, rather than being exposed to the laws of foreign nations. Data transmitted across the internet should be encrypted, and data should be stored locally.

Recommendations Regarding Digital Inequity and Dialogue

1. **Realize that social inequities can be replicated in smart cities**: The smart city promises to produce a more responsive and better-informed municipality through the efficient use of data and technology. However, policymakers should remain cautious regarding the ways in which data and technology can reaffirm social and economic inequities through existing systemic barriers. The process of adopting new technologies within a municipality should should always assess how such technologies may affect the most marginalized.
2. **Foster dialogue on smart cities**: A sound smart city policy should foster a greater understanding of citizens' priorities in the development of smart cities, of what defines a smart city, how they function, and how they affect groups and individuals differently depending on their race, income, and ability. Dialogue and education should include various strategies for public outreach, such as forums, talks, debates, and lectures, as well as age-appropriate inclusions in school curriculum and library programs. Such a campaign should help citizens better understand how to navigate their personal privacy concerns, and empower them to become "smart citizens" in the evolving digital age.[2]
3. **Support affordable and public access to digital devices**: Existing library programs that offer public access and education with digital devices should be expanded to include a focus on the technologies that citizens may encounter in the smart city. Public access to computers and digital devices, often available through public libraries, should remain a priority in future funding decisions of said institutions.

Part Two: Application Recommendations

Technological Recommendations

1. **Privacy by design.** Technology permits or constrains behaviour depending on its implementation. This is what Lawrence Lessig means when he says, "code is law": different implementations of technology will influence behaviour differently, encouraging some activities and discouraging others.[3] In this way, technology can be a more effective regulator than law in achieving certain socially-desirable outcomes, and discouraging others. At its best, deliberation over technological implementations can weigh competing public objectives, minimize harms and recognize and vindicate public values. At its worst, careless implementations can disregard crucial public values, including privacy values. This truth has long been recognized in the privacy space: simply, technology implicates privacy. We can implement technology in ways that maximize respect for privacy, or in ways that disregard privacy interests. "Privacy by Design" is an approach to engineering technology that recognizes this truth, and

[2] Smart citizens are those who are able to navigate the digital landscape and democratically participate within it. See Hemment, Drew, and Anthony Townsend, eds. *Smart Citizens*. Vol. 8. Manchester: FutureEverything, 2013. https://www.scribd.com/document/180718005/Smart-Citizens.

[3] Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

seeks to account for privacy values, and technological security, throughout the development process.[4] The European *General Data Protection Regulation* (GDPR) incorporates privacy by design.[5]

We recommend that cities and their partners incorporate in their smart city policy the requirement that smart city technologies and services be developed in compliance with Privacy by Design framework, ensuring that privacy and security is at the fore throughout the development process.

2. **Data minimization.** The best way to avoid privacy encroachment is to ensure that services gather only that information necessary to provide those services. The temptation to maximize data collection - always present in big data environments - must be resisted.

   We recommend that cities and their partners require data collection be as limited as possible to provide the service in question.

3. **Anonymization at source.** Related to the concept of data minimization is the principle of anonymization at source: if data need not be personal, it should not be identifiable. Anonymization can allow for aggregate data, but the point of collection should not seek out personally identifiable information, and should be alive to the potential for re-identification through cross-referencing 'anonymized' data against other databases.

   We recommend that where cities and their partners collect data about individuals, that data be anonymized at source.

4. **Encryption.** Data security requires appropriate safeguards. The prevalence and ease of use of encryption technologies today mandates the default use of encryption safeguards wherever there is a risk of data breach or interception. However, a surprising number of wireless devices needlessly leave users' personal information exposed.[6]

   We recommend that municipalities and their partners encrypt smart city personal information on data transmission and in storage.

5. **Data localization.** Data localization can have one of two meanings. Data *storage* localization refers to a government compelling "content hosts to store data about internet users in their country on servers located within the jurisdiction of [that government]."[7] Data *routing* localization refers to compelling service providers to only route data between parties within the country itself. The *Canada-United States-Mexico Agreement*, or CUSMA, restricts data storage localization, stating that "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[8] The incorporation of the *General Agreement on Trade in Services* (GATS) into CUSMA means that there are a few exceptions to this general prohibition, designed to:

---

[4] Information and Privacy Commissioner of Ontario, and Registratiekamer. "Privacy-Enhancing Technologies: The Path to Anonymity." Toronto: Legislative Assembly of Ontario, 1995. http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf.

[5] *General Data Protection Regulation (EU) 2016/679,* Article 25; European Data Protection Supervisor. "Preliminary Opinion on Privacy by Design," May 31, 2018. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[6] "Fitness Trackers Put Users' Health Data at Risk, Study Suggests | The Star." thestar.com. Accessed January 25, 2019. https://www.thestar.com/news/privacy-blog/2016/02/fitness-trackers-put-users-heath-data-at-risk-study-suggests.html.

[7] John Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?" *International Journal of Law and Information Technology* 25, no. 3, 1:213-232. Available at https://academic.oup.com/ijlit/article/25/3/213/3960261

[8] *Canada-United States-Mexico Agreement* (CUSMA)**,** article 19.12

1. protect public morals or maintain public order;
2. protect human, animal, or plant life or health; and
3. comply with laws and regulations including prevention of deceptive practices, protection of privacy, and safety.[9]

It has been argued that even with these exceptions, the agreement in CUSMA limits the flexibility of the Canadian government to require storage localization to safeguard the public interest.[10] The extent of these exceptions remains ambiguous. While a sweeping general requirement for data localization within a jurisdiction would fall afoul of CUSMA, requirements with respect to specific businesses that fit within the CUSMA exceptions are permitted. At a minimum, existing data localization rules, such as those found in British Columbia regarding healthcare, likely fall under the exceptions. Absent these exceptions, nothing prohibits cities or other actors from storing their own data locally. By extension, if contracting with other actors to provide city services, nothing prohibits cities from requiring data localization in such procurement contracts. However, uncertainty creeps in when such contracts involve third parties. For example, if a city were to build an open data platform, imposing general data storage localization obligation on third parties using the platform would likely raise questions about CUSMA compliance.

There are many points in favour of data sovereignty, both rights-based and economic; data localization means that data will be subject to known local laws, rather than foreign law. This means that Canadians can be assured that their data will be subject to Canadian privacy law alone. The growth of local data and data storage businesses will support local business and expertise without sacrificing individual privacy to foreign interests or standards. While national legislation is subject to the above noted trade agreements, cities may locate their own data services locally, and may contract with private partners to do so in deploying smart city services.

We recommend that smart cities require that all data sent over the internet be encrypted, and that information that is sent through non-internet networks be routed locally where possible. We recommend that cities require of service contracts, both internally and in contract, that data be stored locally in local cloud services or on local servers, and in the case of an open data platform, require that information provided by the platform be stored locally.

6. **Notice.** Canada's personal information protection laws are predicated on providing people with information and control over their personal information. Notice of the purpose for which personal information is being collected, how it is used, and with whom it will be shared provides the foundation for those legal rights. Notice allows people to provide meaningful consent to dealings with their personal information under PIPEDA, and allows for meaningful engagement with public authorities exercising powers consistent with public sector privacy laws. Notice may take a variety of forms, and be more or less closely associated with behaviour that impacts privacy. The speed of transactions online has led many businesses to rely upon privacy policies or similar passive tools to provide notice

[9] Michael Geist, *How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA,* October 10, 2018. Available at http://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/; *General Agreement on Trade in Services*, Article XIV.

[10] Michael Geist, *How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA,* October 10, 2018. Available at http://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/

of personal information practices. Smart city applications may share this approach given the difficulty involved in providing "on the fly" notices in the bustle of urban settings. However, we caution against this approach. While it is excellent practice to consolidate privacy practices in a single easy-to-access place, failing to highlight issues at key decision points where people actually pay attention and avail themselves of useful guidance will undermine people's ability to exercise meaningful control over their personal information. "Just in time" notices that highlight information about dealings with personal information within the context of the dealing itself are a much more effective way of providing transparency in informational practices and accordingly also of obtaining meaningful consent. Notices that allow people to interact with clear options supported by useful information make privacy choices meaningful. Notices that reflect these principles should be obvious, easily accessed, and clear.

We recommend that smart cities use privacy notices that are contextual, obvious, easily accessible, and clear. Notices should support privacy decisions with clear options that permit meaningful privacy decisions at the time those choices are relevant.

7. **Minimize Surveillance.** Surveillance is antithetical to liberty. We behave differently when watched. We are more likely to express agreement with majority opinion, and less likely to explore minority views, lifestyles and beliefs. A free and democratic society should therefore strive to minimize the use of surveillance to that necessary to achieve discrete, proportionate and legitimate objectives. A smart city can descend into surveillance city; smart cities by definition observe, count, measure and sense. Canadian smart cities should therefore exercise caution in their distribution of cameras, sensors and counters.

   We recommend that smart cities minimize the use of surveillance technologies such as cameras, audio recording, voice-recognition, and tracking. Tools should be appropriate to the task, placed with a sensitivity to personal liberty and privacy, and collect only that data necessary to the task.

Caution Zones: Recommendations

a) No-Go Zones

1. **Children and Youth.** The Federal Office of the Privacy Commission takes the position that "in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians."[11] From ages 13 to 18, the required meaningful consent is only obtained "if organizations have taken into account their level of maturity in developing their consent processes and adapting them accordingly."[12] In the United States, the *Children's Online Privacy Protection Act* applies to the collection of personal information for those under 13 and imposes restrictions on websites or online services collecting information when they have actual knowledge that the user is under 13. These requirements are a recognition of the importance of protecting children and youth privacy, and an acknowledgment that they lack the same capacity that

[11] Office of the Privacy Commissioner of Canada, *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (Ottawa: OPC, 2017), p. 21. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1-3-3
[12] *Ibid.*

adults have to make meaningful decisions about their private information. This is a distinction worth preserving, and steps must be taken to protect a distinctly vulnerable sector of society.

We recommend that the collection of personal information about youth as part of smart city projects mirror current legislation in requiring parental consent in all but exceptional cases for ages 12 and under, requiring organizations to take into account maturity in obtaining meaningful consent form ages 13 to 18. These conditions should only be departed from in exceptional cases, for example in cases involving time-sensitive health information.

2. **No Sale of Data.** Our smart city privacy survey suggests that 91 percent of Canadians object to the sale of their data, saying that the sale of their data should not be permitted. Private parties selling data that includes personal information inherently engages either PIPEDA or substantially similar legislation. Consent is therefore required before personal information can be sold.

   Because Canadians' objections to the sale of their data is so strong, we recommend that the sale of personal information collected as a part of smart city projects be prohibited, with very limited exceptions for special cases that are publicly disclosed, subjected to rigorous scrutiny, and subject to explicit consent.

3. **No Ad Targeting**. Our smart city privacy survey suggests that 69 percent of Canadians object to the use of their personal information to target them with personalized advertisements. A further twenty-seven percent feel that use of personal information for ad targeting should be permitted, but only if they are granted certain rights and protections for their data.[13] PIPEDA requires that personal information collected be appropriate, that the specifics of the collection be pointed out to the individual, and that the the collection be consented to.[14] The Office of the Privacy Commissioner "is concerned about the potential privacy infringements presented by [targeted advertising], particularly the lack of transparency with which they are conducted.[15] The Office of the Privacy Commissioner has called on the advertising industry to "better explain what behavioural advertising involves," to allow individuals to opt out, and to ensure that informed consent is obtained before collection.[16] The Office has taken the position that tracking and targeting of individuals places limits on companies' ability to use opt-out or implied consent methods.[17]

   Because Canadians' objections to the use of their personal information to target them with personalized advertisements is so strong, we recommend that the use of personal information to target individuals with ads as a part of smart city project be permitted only

[13] An April 2018 survey by Ipsos-Reid also found that "While most (85%) also agree (46% strongly/39% somewhat) that they think that internet advertising is annoying, a majority (67%) also agree (26% strongly/41% somewhat) that **i**t's an invasion of privacy." Simpson, Sean. 2018. "Four in Ten (39%) Canadians Changed Their Social Media Behaviour (28%) or Stopped Using Some Platforms (11%) Over Data Privacy Concerns." Ipsos. April 10, 2018. A ailable at https://www.ipsos.com/en-ca/news-polls/Global-News-Data-Privacy-and-Social-Media-Poll-April-2018.

[14] Office of the Privacy Commissioner of Canada, *Online Behavioural Advertising in Brief* (Ottawa: OPC, 2011). Available at https://www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/02_05_d_52_ba_02/

[15] *Ibid.*

[16] *Ibid.*

[17] *Ibid.*

on an opt-in basis, with very limited exceptions in special cases that are publicly disclosed and subject to rigorous scrutiny.

4. **No Collection of Certain Types of Private and Sensitive Data.** Our smart city privacy survey suggests that over 90 percent of Canadians consider their face recognition / image data, their IP address, their web surfing history, their purchase history, their device identification number, and their location data to be private and/or sensitive. A majority of Canadians consider all of these types of information to be "very private and/or sensitive."

   We therefore recommend that the collection of the following types of personal information be prohibited as a part of smart city projects, with very limited exceptions for special cases that have the express permission of the privacy commissioner and explicit consent from the individual involved:

   - **biometric data, including individuals' face recognition / image data;**
   - **IP addresses;**
   - **device identification numbers;**
   - **web surfing histories;**
   - **purchase histories; and**
   - **location data.**

b) Proceed with Caution Zones

Our survey suggests that Canadians wish to have control over their data when it is used for-profit, and when it is used in behavioral modification prompting.

1. **For-Profit Uses by Businesses.** Our smart city privacy survey suggests that 55 percent of Canadians object to the use of their personal information to plan and refine private businesses to make them more profitable. Thirty-seven percent feel that use of personal information for business planning should be permitted, but only if they are granted certain rights and protections for their data, while only four percent believe such uses of personal information should be permitted by default.

   PIPEDA or substantially similar legislation applies to use, collection, and disclosure of personal information where there is commercial activity. This restricts businesses from unilaterally collecting personal information, but does allow businesses to collect and use personal information with individuals' consent.

   Fewer than half of Canadians agreed or strongly agreed 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," and 38 percent of Canadians disagreed with the statement. This suggests that the model of consent used by many businesses--where individuals are required to agree to a unilateral privacy policy or terms of use--is not satisfactory, and that this problem is particularly pronounced in the context of use of personal information by businesses.

   We recommend that the collection and use of personal information for-profit purposes as a part of smart city projects by businesses be permitted on an opt-in-only basis. Citizens should not be excluded from using services on the basis that

they do not consent to the collection, use, or disclosure of their personal information for for-profit purposes. There should be only very limited and rare exceptions to this rule.

2. **Behavioural Modification Prompting.** Smart City technologies can be used to shape or "nudge" people's behaviour towards particular outcomes. For example, smart city technologies can be used to monitor individuals' use of public transit and location data, and then to send personalized messages prompting individuals to use transit or to park in less congested areas. Similarly, hydro use data can be analyzed and used to send individuals prompts to use less hydro, or to use hydro in off-peak hours. Individuals' activity data can be analyzed and used to prompt them to engage in healthier behaviours. Other versions of this strategy rely upon setting default options that favour particular outcomes. This is particularly common in commercial settings, where, for example, a service might set defaults that favour greater openness with personal information over those favouring privacy.

   Our smart city privacy survey asked about such possibilities, and found that forty-four percent of Canadians say that the use of their personal information to prompt them to modify their behavior in these ways should not be permitted. Forty-eight percent feel that use of personal information for behavioral modification prompting should be permitted, but only if they are granted certain rights and protections for their data, while only five percent believe such uses of personal information should be permitted by default.

   PIPEDA does not address "nudging" strategies directly. Rather, PIPEDA requires meaningful consent to the collection, use and sharing of personal information. The more sensitive the information, the greater the risk of harm, and the more unexpected the dealing with personal information in the circumstances, the more "active" the form of consent PIPEDA requires. In such circumstances, "opt-out" strategies for managing consent requirements may fail to obtain meaningful consent and fall afoul PIPEDA.

   The requirements of meaningful consent must accordingly guide smart city nudging strategies. The unexpected privacy implications of many smart city applications suggest caution in relying on opt-out strategies for obtaining consent to dealings with personal information. Simply, many smart city applications will be novel and will gather information on human movement and activity in ways and places that city residents may not expect. Where behavioral modification prompting involving dealings with personal information relies upon default "opt-out" strategies for obtaining consent, these strategies may fall afoul PIPEDA where they involve sensitive information, are outside individuals' reasonable expectations, and/or create a meaningful risk of significant harm.

   We recommend that the uses of personal information collected as a part of smart city projects to prompt people towards particular behaviour should be permitted on an opt-in-only basis, with very limited exceptions.

Part Three: Smart City Data Rights

Canadians, according to our recent survey, expect to have the right to view, delete, and download the personal information collected about them.[18] Ninety-six percent of Canadians "agree" or "strongly agree" that they should be able to view the personal information collected about them; 89 percent agree that they should be able to delete it; and 92 percent that they should be able to download their personal information.

Under PIPEDA, Canadians have a right of access to their personal information, and a right to correct that information if it is incorrect.[19] Researchers have investigated the extent to which companies comply with such requests. Researchers in Canada and Hong Kong found many companies failed to comply with requests for access to personal information.[20]

> **We recommend that the rights to view, delete, and download personal data should be recognized and affirmed not only in legislation at all levels, but also in municipal smart city policies. Smart city technology partners should implement technologies to facilitate direct viewing, deletion, downloading, and correction of personal data by individuals.**

Seventy-seven percent of Canadians agree or strongly agree that "there should be a way to use municipal services, such as transit, anonymously without providing my personal information."

> **We recommend that municipalities and municipal partners ensure that it is always possible to utilize municipal services, such as transit, anonymously.**

[18] Bannerman, Sara and Angela Orasch. *Privacy and Smart Cities: A Canadian Survey*. January 15, 2019. Available at https://smartcityprivacy.ca

[19] "PIPEDA Fair Information Principle 9 – Individual Access." Office of the Privacy Commissioner of Canada. Accessed January 25, 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_access/.

[20] Hilts, Andrew, Christopher Parsons, and Masashi Crete-Nishihata. "Approaching Access: A Look at Consumer Personal Data Requests in Canada." The Citizen Lab, February 12, 2018. https://citizenlab.ca/2018/02/approaching-access-look-consumer-personal-data-requests-canada/; Parsons, Christopher, Andrew Hilts, and Masashi Crete-Nishihata. "Approaching Access: A Comparative Analysis of Company Responses to Data Access Requests in Canada." Citizen Lab Research Briefs. Toronto: Citizen Lab, 2018. https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf; "Access My Info." Open Effect, June 21, 2016. https://openeffect.ca/access-my-info/; Cheng, Kris. "Telecom Companies Fail to Provide Sufficient Responses to Personal Data Requests, Transparency Advocates Say." *Hong Kong Free Press HKFP* (blog), May 6, 2016. https://www.hongkongfp.com/2016/05/06/telecom-companies-fail-to-provide-sufficient-responses-to-personal-data-requests-transparency-advocates-say/.