Spatial Knowledge and Information Canada, 2019, 7(5), 1

Pedestrian Curiosity: A Brief Examination of Consent and Privacy in Swath Section Smart City Spaces

KERI GRIEMAN
Canadian Internet Policy and
Public Interest Clinic
University of Ottawa
keri@cippic.ca

ABSTRACT

Smart cities technologies raise concerns for privacy, and our regulatory framework may raise more questions than answers in addressing these concerns. In looking at how smart cities function, legal questions about data collection, jurisdiction over data handling and public-private partnerships, and the function of consent in the smart city are raised.

1. Introduction: Smart Cities – Swath Sections

Sidewalk Toronto has been the target of many a smart-city conversation. Ambitiously, it aims to be as 'smart' as possible – to combine as many possible smart city technologies to create a section of a city that fosters and promotes ideals such as urban growth and innovation; sustainability; affordability; mobility; and economic opportunity.[1] For the purposes of discussion, this type of large-area application of smart city technologies will be referred to as a 'swath section.'

Smart city technologies fall under a broad umbrella, but largely into the definition of technology that analyses large amounts of data in order to improve its services.

Consider a car-sharing service: a management system must know where its cars are, whether they have been paid for, and how to manage user data. The cars will be useless unless they are placed conveniently for customers to use them. Data is analyzed to determine where to purchase parking for the cars, where to replace if necessary, and where to place an allowable 'home area.' For some companies, the data collected is the real product – while services may be free, access to users or their data may in fact be what makes the company profitable, as is the case with technologies like bike-counting detection units. Yet while the types of smart cities technology are boundless, there is one concern fundamental to their discussion, particularly when, as in cases of entire city sections, data can be used for multiple purposes: privacy. Data is useful, marketable, and capable of making cities more efficient, but may do so at the cost of individual privacy.

2. Analysis

2.1 Data Collection in Smart Cities

Smart city technologies run on data. In swath section applications such as Sidewalk Labs' proposed Waterfront Toronto, the data may improve the way the city runs. In fact, the concept of 'open data,' or making as much data broadly available as possible,

1 Sidewalk Labs, "Our Vision", (2018) online: <https://www.sidewalklabs.com/>

does just this, for large swaths of cities down to individual, small areas such as a single intersection. Yet for many private companies, the data itself is a commodity - data can be sold very profitably to parties interested in compiling data profiles, targeting advertising, or analyzing behaviour, to name a few. It doesn't take an active imagination to deduce that an insurance company might be interested in knowing the heart-rate of users of a bike-sharing platform, particularly if they can combine that information with other sources to build an accurate, if not perfectly identifiable, profile of such an individual. While swath section supporters often propose the de-identification of data - stripping it of identifiable characteristics - the risk of re-identification is very real, particularly in cases where multiple data collecting technologies are at play in an individual space. Collection then becomes a balancing act between privacy and profitability - the more anonymous the collected data, the more private to the individual, but the less useful to the company. For example, data that identifies age, gender, habits, and location are much more desirable to companies than that which merely identifies a person's presence. Even a data set that only identifies a singular characteristic can be combined with others: "[s]ophisticated algorithms can be used to match these different data sets to re-identify specific individuals, contributing to widespread practices around profiling individuals.[2] While one individual company operating and/or collecting in a smart city swath space may not use data for a non-consented to purpose, that data might be combined with other information by a third party to do so.

2.2 Jurisdiction of Privacy Law in Canada

Jurisdiction of privacy law in Canada is exceptionally complicated. The *Privacy Act* applies to a distinct, listed set of mostly federal public entities. For other federal works, undertakings, and businesses, as well as where there is commercial activity, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* applies. There are carve-outs of applicability for provinces with 'substantially similar' privacy legislation, which currently includes Quebec, British Columbia, and Alberta. Ontario, New Brunswick, Nova Scotia, and Newfoundland also have their own carve-outs for health-related privacy legislation. So while *PIPEDA* may be the default application in the private sector, it is by no means the given applicable legislation. In terms of *PIPEDA*, application and thus the consent requirement occurs outside of federal works, undertakings, or businesses when there is commercial activity at play. While provincial legislation may not apply exactly the same way, it will be substantially similar for private enterprises. For provincial government entities, provinces have their own legislation, such as Alberta's Freedom of Information and Protection of Privacy Act for public entities, and the Health Information Act for health records.

2.2.a Commercial Activity

Whether or not there is commercial activity is not a straightforward question to answer, particularly in regards to smart cities. The federal Office of the Privacy Commissioner, or OPC, has clarified that for municipalities, educational institutions, and hospitals, the question is not whether a fee is charged, but whether they are engaged in trade and commerce contemplated by the Canadian Constitution.[3] Indicia of this can include whether the institution is dependent on municipal or provincially levied taxes and provincial grants.[4]

2 Teresa Scassa,"Privacy and Open Government", online: (2014) 6 Future Internet 2, at 407

3 Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals" <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/>

4 ibid

Smart city initiatives raise a variety of questions. First: to what extent must an initiative be related to a municipality to fit under this exception? It is clear that, for example, a city-run road repair crew would be considered municipal government activity. Yet it is not clear that a partnership between public and private entities would be, wherein municipal activity and non-municipal activity is found. Metrolinx, for example, is a provincial Crown Corporation that provides transportation in the province of Ontario. Ontario does not have broad private-sector 'substantially similar' legislation, so *PIPEDA* prima facie applies. Metrolinx takes money directly from consumers to perform an optional commercial service, which would fall under most definitions of commercial activity. Yet Metrolinx purports not to be covered by *PIPEDA*, with the rational that they do not undertake commercial activity. Data about users' cards, and their transfers, locations, and habits, thus resides in an unusual governance space. It may be governable under Ontario's provincial privacy laws - the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), but these have not been accepted as on par with *PIPEDA*. The data thus occupies a space lacking governance. In swath sections, private companies are likely to be engaging in activities that are often considered municipal (garbage collection, street cleaning, etc).

Other quasi-governmental initiatives are likely to encounter similar problems. Where cities have partnerships with private actors, the private actors actors are likely to argue that they are not engaged in commercial activity - that where they engage in activity that is typically undertaken by cities, they are instead engaged in municipal activity and thus not covered by *PIPEDA*.

Whether or not *PIPEDA* or substantially similar legislation is engaged is important as it determines how personal information is collected, used, or disclosed. While there are exceptions, the general rule is that in order to collect personal information, *PIPEDA*-governed organizations are required to obtain meaningful consent.[5] Meaningful consent involves more than just ticking a box. The entity seeking consent must emphasize key elements of what is being consented to; allow individuals to control the level of detail they get and when; provide individuals with clear options to say 'yes' or 'no,'; be innovative and creative in adopting the methods seeking consent specific to context; consider the consumer's perspective; make consent a dynamic and ongoing process; and be ready to demonstrate compliance.[6]

2.3 Why is consent so important?

Consent is important for many reasons. It is the way individuals decide how their data is used, and whether or not they will allow other entities to use it. PIPEDA requires that the "knowledge and consent of the individual are required for the collection, use, or disclosure of personal data," and provides only strictly limited exceptions for legal, medical, and security reasons.[7] While there are bare-minimum governance requirements, such as for tax purposes, individuals technically have control over the vast majority of their personal data, and whether or not they decide to allow it to be collected, used, or disclosed. Or, rather, they should - but companies may or may not adhere to legal responsibilities. The OPC notes that meaningful consent should include emphasizing the following:[8]

5 Office of the Privacy Commissioner of Canada "Guidelines for obtaining meaningful consent" <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>

6 ibid

7 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, <http://canlii.ca/t/52hmg> 4.3

8 ibid

- What personal information is being collected
- With which parties personal information is being shared
- For what purposes personal information is collected, used or disclosed
- Risk of harm and other consequences

Furthermore, companies must have consent to collect, use, or disclose any personal information. While many companies interpret 'personal information' to mean any information that can identify a person, the legal interpretation is actually much broader. Personal information includes any information *about* an identifiable individual - "not just the subject of something but also relates to or concerns the subject."[9] Exceptions do apply, such as to business contact information, but in general application a "broad and expansive interpretation" is appropriate.[10]

2.4 The ultimate issue - the requirement of consent for sharing personal information in a smart city context

Swath section smart city areas increase the level of concern for privacy and consent. First, the type of data that qualifies as personal information may be broader than companies are prepared to address. For example, in sparsely populated areas, even bike counting data can count as personal information as it could easily be matched to individuals. Second, current legal definitions of commercial activity may be insufficiently specific to hold quasi-municipal entities to task on data protection to the standard required by *PIPEDA*. Third, consent is not only an important tool in management of personal information, but one which, in the context of privacy, must be held to a high standard. Passive, assumed consent is insufficient. Smart city swath sections propose to create a part of the city that permits collection of a vast amount of data. Even in the face of de-identification, there should be a great deal of concern over the combination of data available in a definable geographic section, maximizing the likelihood of combination of datasets. Consent must be meaningfully obtained for each and every collection. Swath section companies have failed to address what consent might look like on a granular level. It is insufficient to assume meaningful consent when it rests on the assumption that the individual is aware that the swath section collects information: “[c]onsent is only valid where the individual can understand that to which they are consenting.”[11] Consider a sign noting such collection. The individual must be told what personal information is being collected (possible); with which parties personal information is being shared (difficult); for what purposes personal information is being collected, used, or disclosed (exceedingly difficult to fit on a billboard); and, most importantly - risk of harm or consequences (exceedingly unlikely). Business models based on data collection, either internally or externally, thrive because individuals do not realize what their information could be used to do: the consequential loss of privacy to simply entering such a section of the city may be higher than citizens wish to contemplate.

4. Conclusion

9 Office of the Privacy Commissioner of Canada "Personal Information" <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/>

10 ibid

11 Office of the Privacy Commissioner of Canada "Guidelines for obtaining meaningful consent" <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>; Personal Information Protection and Electronic Documents Act, SC 2000, c 5, <http://canlii.ca/t/52hmg> 6.1

There are a great deal of unknowns in the governance of data collection in the smart cities space. Privacy is a commodity, and whether it is being begged, bartered, or sold, the smart city swath sections will become a particular battleground. There are issues of jurisdiction, governance of data, and handling of consent that must be addressed, lest the swath section be ungovernable by current privacy legislation. Ultimately, there must be a call to fill the blind spot of how meaningful consent in the smart city swath space will be filled.

References

Personal Information Protection and Electronic Documents Act, SC 2000, c 5, <http://canlii.ca/t/52hmg>

Sidewalk Labs, "Our Vision", (2018) online: <https://www.sidewalklabs.com/>

Teresa Scassa, “Privacy and Open Government”, online: (2014) 6 Future Internet 2’

Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals" <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/>

Office of the Privacy Commissioner of Canada "Guidelines for obtaining meaningful consent" <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>

Office of the Privacy Commissioner of Canada "Personal Information" <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02>