

Jun 20, 2019

## Smart Cities: An Opportunity for Engagement on Big Data Governance

By Steve J. Tenai

Quayside, a proposed “smart city” on Toronto’s waterfront,<sup>1</sup> has garnered a lot of attention about big data initiatives relative to privacy and data governance. Smart city proposals underscore the importance of balancing the benefits of data analytics with privacy rights. A reactive, complaints-based model has been shown to be inadequate to generate the necessary trust and transparency to meet privacy concerns. At the same time, certain privacy principles, such as individual consent, do not necessarily translate to certain smart city initiatives.

Smart city initiatives provide an opportunity for public engagement about data governance and privacy. This is a welcome opportunity. Public discourse about privacy happens too often after the roll out of big data ventures and, worse yet, after high profile “breaches of trust” that have challenged confidence in data governance. Quayside allows for both “privacy by design” principles to be applied to a new venture and also for a broader public discourse on privacy and big data before the initiative proceeds. The recent announcement of both a federal Digital Charter and other municipal and provincial reviews into data strategies will hopefully provide a robust opportunity for such public discourse and, in the process, arrive at a refreshed big data governance framework that fosters innovation while also increasing public trust and confidence in adherence to privacy concerns.

### Smart Cities

The term “smart city” covers a wide spectrum of initiatives that use internet connected technology and data to allow urban centres and cities to operate more efficiently. Smart city technology is already being used in many urban centres (e.g. streetlights with smart sensors and traffic management systems that use data to improve traffic flows.) There are scores of smart city projects throughout the world that vary widely in their application of technology to different goals, including public WiFi networks, traffic flow, parking, energy, resource and waste management, public transit allocation, environmental monitoring and security.<sup>2</sup>

Google’s Sidewalk Labs, along with Waterfront Toronto, has formed Sidewalk Toronto to develop Quayside. Quayside envisions a new community with an array of sensors measuring all aspects of activity with the stated goal of learning how to better design streets, buildings and transportation systems. It will not be the first development to use internet connected sensors on a large scale to collect large volumes of data to manage municipal services. Songdo, a brand-new development outside of Seoul, South Korea, is one of the first large scale real estate communities designed from the ground up as a smart city. However, existing cities such as Barcelona, Amsterdam and Stockholm have also adopted smart city technologies within existing municipal infrastructure and neighborhoods. A 2017 report from the National League of Cities cites 66% of US cities reporting that they are investing in smart city technology, and 25% of those without any smart city systems are exploring how to implement it.<sup>3</sup>

It is not contentious that smart city technologies offer significant benefits to managing resources and services. Privacy advocates acknowledge that smart city technologies, “Allow communities to more effectively address challenges of urbanization and allocate resources accordingly.”<sup>4</sup>

Barcelona is frequently cited for the benefits smart city technology can yield. For example, the city installed thousands of smart meters that monitor and optimize energy consumption in targeted areas of the city. Lampposts sense when the streets are empty, automatically dimming lights to conserve energy. The lampposts are also part of the city’s WiFi network, providing free Internet access throughout the city. Moreover, they are equipped with sensors that collect data on air quality, relaying that information to city agencies and to the public. Using sensors to monitor rain and humidity, city workers can determine how much irrigation is needed in municipal park areas and, through a system of electronic valves, can remotely

control the delivery of necessary water across the city. In waste management, households deposit waste in municipal smart bins that monitor waste levels and optimize collection routes. For drivers, Barcelona has implemented a sensor system that guides them to available parking spaces. The sensors, embedded in the asphalt, can direct drivers to open spaces thereby reducing congestion and emissions. These various systems generate data that can be used by both city agencies and citizens.<sup>5</sup>

Governments have embraced smart city technology. The Government of Canada's Ministry of Infrastructure and Communities recently announced successful proposals to its competition that invited communities across Canada to develop proposals for "innovative solutions to their most pressing challenges using data and connected technologies."<sup>6</sup> The City of Toronto has begun work on a digital infrastructure and smart city framework.<sup>7</sup>

## Privacy Controls

Smart city technology is based on collecting large quantities of data about how persons interact within their urban environment. Invariably, the data collected will include personal information, and the potential use of this data raises privacy concerns. Mistrust that information may be used to enable privacy-invasive activities, such as surveillance and profiling, or other purposes that are inconsistent with the originally stated purposes are fueled by revelations such as Cambridge Analytica's access to Facebook users' account information. One need only consider the current debate about facial recognition technology that has prompted San Francisco taking the step to ban the use of facial recognition by police and other municipal authorities.<sup>8</sup>

The Office of the Privacy Commission and other privacy authorities have identified six categories of privacy and securities measures<sup>9</sup> that should be incorporated into any smart city initiative:

1. Data-minimization – systems must not collect, use or disclose personal information unless it is necessary to do so to achieve the outcomes of the initiatives. In all cases, where the goals can be achieved using less privacy invasive alternatives, those alternatives should be pursued.
2. De-identification – systems must endeavour to de-identify personal information at the earliest opportunity and include measures to mitigate the risk of de-identification that is inherent with connected devices. As well, systems should only retain, use and disclose de-identified information. The Information and Privacy Commission of Ontario, "De-identification Guidelines for Structured Data" outlines basic concepts and techniques of de-identification and provides a step-by-step protocol for de-identifying structured data.
3. Data governance and Privacy Management program – initiatives must be supported by policies that address privacy and security requirements including appointing a privacy lead, monitoring and auditing for compliance, and breach response. There must also be contractual protections and accountability for all of the diverse parties involved in the initiative.
4. Privacy impact assessments and threat risk assessments – these are widely recognized as important tools to help ensure that privacy and securities risks are identified and adequately addressed in the design of new technologies and programs. In some jurisdictions, they are required.
5. Community engagement and project transparency – communities must ensure full transparency or the information practices of their initiatives to help community members understand how they might be affected. Transparency is reflected in Canadian provincial and federal access and privacy laws.
6. Consent – systems must ensure individuals' meaningful consent where required by law, including the opportunity to opt out of participation, where feasible. Consent encompasses four elements in privacy notices: (1) What personal information is being collected, (2) With whom is the collected personal information being shared; (3) What purpose is the personal information being collected, used or disclosed; and (4) What are the risks of harm or other consequences that might come from any collection, use or disclosure of the information provided. Smart city technologies collect and use information from many sensors that interact with people and their personal devices as they go about their daily lives, in some instances without any positive action required or real opportunity to opt out. Smart city technologies may not always provide an opportunity for actual consent to the collection of personal information.

## Proposed Measures to Address Privacy Concerns

Sidewalk Labs has itself set out a draft digital governance framework for Quayside<sup>10</sup> that incorporates the following measures directed at quelling voiced privacy and data governance concerns:

1. “Responsible Data Use Guidelines” to be applied to Sidewalk Labs and all partners in Quayside that would foster innovation within a framework of giving priority to personal privacy and the public good.
2. “Responsible Data Use Assessment” which provide for publicly auditable assessments for all public and private digital services required before data is collected and used.
3. Sidewalk Labs will base its technology on open standards, allowing others to build and connect new services, offer competitive alternatives and drive innovations.

The effectiveness of these measures lies in their details to be laid out. An updated proposal is expected in June 2019 from Sidewalk Labs. The Office of the Privacy Commissioner of Canada, along with Ontario’s Information and Privacy Commission, have met (and intend to continue to meet) with Sidewalk Labs officials to learn more about how privacy concerns will be addressed.

Sidewalk Labs has also stated that the data generated from public sources will not be treated as its property and will not be sold or used for advertising purposes. Sidewalk Labs proposes to place the data in the hands of an independent trust, a Civic Data Trust, which would set the rules around data use, stripping identifying information, and making it publicly accessible on equal terms to all persons and entities. An open data concept, treating information generated from Quayside as a public resource, aligns with steps other cities have taken. For example, the City of Ottawa has recently launched an open data portal called Open Ottawa which gives residents and businesses easier access to the City’s open data library.<sup>11</sup>

Not everyone is satisfied that the proposed Civic Data Trust goes far enough. Some privacy professionals have commented that the proposed trust may escape being subject to existing privacy laws as neither a government authority nor a private enterprise collecting personal information for a commercial purpose.<sup>12</sup> Others have seen as a critical shortcoming Sidewalk Labs’ stated inability to ensure that all Quayside participants will comply with de-identifying all collected data, prompting the resignation of Ann Cavoukian, a former Ontario privacy commissioner, from the Digital Strategy Advisory Panel established by Waterfront Toronto to study the control and access the data gathered from Quayside.<sup>13</sup>

The Canadian Civil Liberties Association (“CCLA”) has also challenged leaving the decision around data governance for Quayside in the hands of Waterfront Toronto, a non-profit corporation created by the governments of Canada, Ontario and Toronto to revitalize the city’s disused waterfront lands. It notes that Waterfront Toronto’s mandate is real estate revitalization and not privacy and data governance, and that those matters cannot be delegated by government authorities to Waterfront Toronto. The CCLA has commenced a judicial review application to, among other things, have agreements between Waterfront Toronto and Sidewalk Labs declared of no force and effect and to enjoin Waterfront Toronto from entering into a master innovation development plan with Sidewalk Labs expected to address access and ownership of data from Quayside.<sup>14</sup> CCLA essentially submits that the Quayside project should be reset and only advance with new requests for proposals once all three levels of government have established digital data governance policies. The CCLA envisions those policies would follow a public consultation process, and cover the collection, ownership, use and residency of personal information and other data obtained by smart city sensors.<sup>15</sup>

## Moving Forward

In May 2019, the federal government announced a Digital Charter for Canada. The Charter outlines what Canadians can expect from the federal government in terms of a framework and approach to digital and data policy with the stated goal of engendering trust among Canadians in new digital technology initiatives like smart cities. Among the ten principles underlying the Digital Charter are: (i) “Control and Consent” (i.e. providing individuals control over what data they are sharing, who is using their personal data and for what purposes, as well as the knowledge that their privacy is protected), and (ii) “Strong Enforcement and Real Accountability” (i.e. clear, meaningful penalties for violations of the laws and regulations that support these principles).<sup>16</sup>

How the Digital Charter's principles will be achieved legislatively is still not entirely known, however, the announcement did propose reforms to the *Personal Information Protection and Electronic Documents Act (PIPEDA)* that will require further discussion and consultation.<sup>17</sup> Among the proposed reforms are measures around: (i) enhancing individuals' control; (ii) enabling responsible innovation; (iii) enhancing enforcement and oversight; and (iv) areas of ongoing assessment.<sup>18</sup>

The Digital Charter announcement also proposed the establishment of a Canadian Data Governance Standardization Collaborative to help coordinate the development and compatibility of data governance standards across Canada. The ideal of a coordinated development of data governance standards aligns with the invitation made by the Ontario Government to its federal and municipal counterparts to help develop a framework that can act as a standard for smart city development. This invitation formed part of the Ontario Government's announcement on May 30, 2019 of five framework principles for smart cities.<sup>19</sup>

The consultation processes around Quayside through the Digital Strategy Advisory Panel, the Ontario Government's Digital and Data Task Force, and around proposed amendments to *PIPEDA* all offer a welcome opportunity for civic engagement on how to balance the use of data technologies to achieve laudable social goals while engendering trust around privacy protection. It presents an opportunity for fresh ideas (or even borrowed ideas) around transparency and accountability which are the bedrock to rebuilding trust.

As Daniel Therrien, Privacy Commissioner of Canada, noted in his remarks at recent privacy symposium, "Canada's largely reactive, complaints-based model for privacy protection seldom affords us the opportunity to examine new technologies, complex data flows and opaque business models. People are unlikely to file a complaint when they do not know what is happening to their personal information."<sup>20</sup> It may be time to re-examine other models around accountability applied in other business contexts that depend on trust in considering big data initiatives. For example, the regulatory regime around public disclosure and financial reporting by public companies mandates particular public disclosures based on stated standards, with officer certifications and third-party audits backed with civil and regulatory enforcement. Mandated disclosures around big data collection and usage, backed by periodic certifications with third party audits, with meaningful consequences for false disclosures, may enhance the transparency and trust necessary for smart city initiatives.

Regardless, smart cities like Quayside provide us an opportunity for engagement on privacy that should be fully exploited with forward looking ideas around data governance.

*\* This article was originally published on June 14, 2019 by the Ontario Bar Association's Privacy & Access to Information Law Section.*

<sup>1</sup> "Sidewalk Toronto", online: *Side Walk Labs* <[sidewalktoronto.ca/wp-content/uploads/2019/02/FEB14-SWTO-Business-Case-Overview.pdf](http://sidewalktoronto.ca/wp-content/uploads/2019/02/FEB14-SWTO-Business-Case-Overview.pdf)>.

<sup>1</sup> "Sidewalk Toronto", online: *Side Walk Labs* <[sidewalktoronto.ca/documents/](http://sidewalktoronto.ca/documents/)>.

<sup>2</sup> "List of Smart City Projects", online: *Nominet* <[www.nominet.uk/list-smart-city-projects/](http://www.nominet.uk/list-smart-city-projects/)>.

<sup>3</sup> "Cities and Innovation Economy: Perceptions of Local Leaders", online: *National League of Cities* <[www.nlc.org/resource/cities-and-innovation-economy-perceptions-of-local-leaders](http://www.nlc.org/resource/cities-and-innovation-economy-perceptions-of-local-leaders)>.

<sup>4</sup> "Joint letter to the Minister of Infrastructure and Communities on Smart Cities Challenge" (last modified 24 April 2018), online: *Office of the Privacy Commissioner of Canada* <[www.priv.gc.ca/en/opc-news/news-and-announcements/2018/let\\_sc\\_180424/](http://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/let_sc_180424/)>.

<sup>5</sup> Laura Adler, "How Smart City Barcelona Brought the Internet of Things to Life", online: *Data Smart City Solutions* <[datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789](http://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789)>.

<sup>6</sup> “Smart Site Challenge”, online: *Infrastructure Canada* <[www.infrastructure.gc.ca/cities-villes/index-eng.html](http://www.infrastructure.gc.ca/cities-villes/index-eng.html)>.

<sup>7</sup> “Smart Cities Initiative”, online: *Toronto* <[www.toronto.ca/city-government/council/2018-council-issue-notes/torontos-finances-and-government/smart-cities-initiatives/](http://www.toronto.ca/city-government/council/2018-council-issue-notes/torontos-finances-and-government/smart-cities-initiatives/)>.

<sup>8</sup> Kate Conger, Richard Fausset and Serge F. Kovalski, “San Francisco Bans Facial Recognition Technology” (14 May 2019), online: *The New York Times* <[www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html](http://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html)>.

<sup>9</sup> “Joint letter to the Minister of Infrastructure and Communities on Smart Cities Challenge” (last modified 24 April 2018), online: *Office of the Privacy Commissioner of Canada* <[www.priv.gc.ca/en/opc-news/news-and-announcements/2018/let\\_sc\\_180424/](http://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/let_sc_180424/)>.

<sup>10</sup> “Digital Governance Proposals for DSAP Consultation” (last modified October 2018), online: *Sidewalk Labs* <[waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15\\_SWT\\_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES](http://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES)>.

<sup>11</sup> Online: *Open Ottawa* <[open.ottawa.ca/](http://open.ottawa.ca/)>.

<sup>12</sup> Timothy Banks, “Three questions that Waterfront Toronto should ask Sidewalk Labs” (19 November 2018), <[timothy-banks.com/2018/11/19/three-questions-that-waterfront-toronto-should-ask-sidewalk-labs/](http://timothy-banks.com/2018/11/19/three-questions-that-waterfront-toronto-should-ask-sidewalk-labs/)>.

<sup>13</sup> “‘Not good enough’: Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns (last modified 21 October 2019), online: *CBC News* <[www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223](http://www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223)>.

<sup>14</sup> “CCLA Commences Proceedings Against Waterfront Toronto” (16 April 2019), online: *Canadian Civil Liberties Association* <[ccla.org/ccla-commences-proceedings-waterfront-toronto/](http://ccla.org/ccla-commences-proceedings-waterfront-toronto/)>.

<sup>15</sup> “Open Letter From CCLA: Calling for a Reset on Waterfront Toronto” (3 March 2019), online: *Canadian Civil Liberties Association* <[ccla.org/open-letter-ccla-calling-reset-waterfront-toronto/](http://ccla.org/open-letter-ccla-calling-reset-waterfront-toronto/)>

<sup>16</sup> Innovation, Science and Economic Development Canada, “Canada’s Digital Charter: Trust in a Digital World” (last modified 5 May 2019), online: *Government of Canada* <[www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00108.html](http://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html)>.

<sup>17</sup> Innovation, Science and Economic Development Canada, “Canada’s Digital Charter in Action: A Plan by Canadians, for Canadians” (last modified 21 May 2019), online: *Government of Canada* <[www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00109.html](http://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html)>.

<sup>18</sup> Innovation, Science and Economic Development Canada, “Proposals to Modernize the *Personal Information Protection and Electronic Documents Act*” (last modified 21 May 2019), online: *Strengthening Privacy for the Digital Age* <[www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00107.html](http://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html)>.

<sup>19</sup> “Ontario Takes Action to Protect Privacy and Personal Data” (30 May 2019), online: *Ontario* <[news.ontario.ca/mgs/en/2019/05/ontario-takes-action-to-protect-privacy-and-personal-data.html](http://news.ontario.ca/mgs/en/2019/05/ontario-takes-action-to-protect-privacy-and-personal-data.html)>.

<sup>20</sup> Daniel Therrien, “Shifting for Results for Canadians - Remarks at the IAPP Canada Privacy Symposium 2018” (last modified 13 June 2018), online: *Office of the Privacy Commissioner of Canada* <[www.priv.gc.ca/en/opc-news/speeches/2018/sp-d\\_20180524/](http://www.priv.gc.ca/en/opc-news/speeches/2018/sp-d_20180524/)>.

## Author



**Steve J. Tenai**  
Partner  
T 416.865.4620  
[stenai@airdberlis.com](mailto:stenai@airdberlis.com)

This communication offers general comments on legal developments of concern to business organizations and individuals and is not intended to provide legal advice. Readers should seek professional legal advice on the particular issues that concern them.