

Sidewalk Labs – Public or Private Data?

The Google subsidiary, Sidewalk Labs, is proposing to create an “innovative urban district” on Toronto’s waterfront to be called Quayside.¹ The goal is to overlay the “physical layer” of urban environment (buildings, streets, vehicles) with a “digital layer” of *information* reflecting the dynamic activities and interactions within the physical layer. Essential to the creation of this digital information layer is the collection of data, both public and private, reflecting these activities and interactions. The ultimate objective is to obtain a greater understanding of the nature of dynamic activities within the community, and thereby achieve insights and enhance planning of the urban environment - including energy efficiencies, economic efficiencies, quality of life and sustainability.

Existing data stores – filling in the gaps

There exists already a significant store of digital and other data available from diverse sources reflecting not only activities but also conditions within an urban environment. Such data sources include mobile phones, connected devices, and utility usage databases. Other more public data stores include weather, air quality, municipal taxation and traffic. However, to achieve a comprehensive view of all activities within an urban environment, Sidewalk Labs proposes to create a new level of data collection in both private and public spaces – through more intensive analysis of activities by people and things as they interact, move about and live within that environment. Such an analysis could be characterized as filling in the gaps – so to speak – between the existing data stores.

It is this *filling in the gaps* data collection that has created challenges and concerns about the nature of personal information that may be obtained, and the required governance respecting such information once collected. Concerns about privacy are exacerbated by the proposed nature of the collection – through ubiquitous electronic “sensors” and in some instances video monitoring – as well as from transaction data (e.g. parking). To be clear, not all data collected would be personally identifiable; a significant element would encompass traffic patterns, vehicle travel, pedestrian travel, visits to buildings and other non-personal data.

In order to address the concerns regarding collection and use of identifiable personal data, it is instructive to characterize the data with a privacy lens. As part of such characterization, consideration must be given to not only the entities involved – such as Sidewalk Labs – but also any governance regime that would provide oversight.

¹ See [Project Vision](#), excerpt from Response to Waterfront Toronto Quayside RFP, October 17, 2017

Private space data

As noted, a significant amount of personal data that may contribute to planning a digital urban community is clearly “private space” data, collected by both private and public entities from sources including home environment controls, mobile phones (not only their locations but also app-generated information), and connected (and potentially self-driving) cars. Other personally-identifiable data is generated by home and business security and monitoring systems as well as through video surveillance data both within and surrounding private and public buildings. Utility usage information, including electricity, gas and water, is another important data source.

To achieve the envisioned “digital layer” of information for its innovative urban community, Sidewalk Labs will create additional private space data stores and likely will access at least some of the existing private space data to combine it with data collected in the “public space” environments.

All of this personal information, if collected by a private sector organization for commercial purposes, must have the consent, either express or implied, of the individual to whom it relates. Furthermore, such data will be subject to the full privacy compliance rules dictated by the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA), the national private sector privacy law. If collected by a public sector organization, consent is *not required* but there must be statutory authorization. Rules regarding such collection are found in the public sector privacy laws such as the [Freedom of Information and Protection of Privacy Act](#) (Ontario).²

Public space data

How to characterize and treat the personally-identifiable data collected in public spaces? Should this data be considered publicly available and therefore accessible to any person who wishes to collect it? Or is it personal information that should be governed by the full rigour of applicable privacy laws? If the data is personal information, what privacy laws would, or should, apply?³

Sidewalk Labs currently is proposing that it would collect the data and in certain instances de-identify it. However a significant amount of data would remain personally-identifiable as collected in the first instance at least, by Sidewalk Labs. Our privacy laws extend protection to personally-identifiable data wherever it is collected, whether in public or private spaces. PIPEDA applies to collection of personal information for commercial purposes and its rules would apply to any such data collection by Sidewalk Labs, assuming that

² Applicable to provincial government organizations; municipal government organizations are subject to the [Municipal Freedom of Information and Protection of Privacy Act](#) (MFIPPA).

³ An argument also may be made that the data is a community asset that should be owned or controlled by the community at large. See [Not for Sale – The case for Non-Profit Ownership and Operation of Critical Community Infrastructure](#), Ontario Nonprofit Network (November 2018).

some of the intended purposes are commercial in nature. Under PIPEDA, consent of all individuals whose data is collected would be required.⁴

Any such collection by Sidewalk Labs would also require authorization of the governmental authorities having jurisdiction over the public spaces where collection would occur. Without delving into the details of the relationships among the three governments involved (federal, provincial, municipal) and Waterfront Toronto, the vehicle through which the governments are interacting with Sidewalk Labs, it is clear that Quayside will involve at least municipal jurisdiction (e.g. over streets, etc.) as well as land ownership by one or more public sector entities. Consequently, it is reasonable to assume that authority to collect data within Quayside's public spaces must be granted (or at least not prohibited) by some or all of the public sector entities involved. Does this mean that the data would be subject to public sector privacy laws as well as any application of PIPEDA?

Personal information collected in public spaces is only subject to public sector protection if it is collected by an "institution" designated under the public sector privacy laws. Therefore, if the governments involved, including Waterfront Toronto, simply authorize that collection by a private sector entity such as Sidewalk Labs, there is no public sector privacy oversight. However, if a public sector entity designated as an "institution" authorizes the private sector entity to collect the information on its behalf, then the public sector privacy law will apply. PIPEDA would have more limited application – essentially only with respect to any data independently collected by private sector organizations for their own purposes.

Public sector privacy oversight

Does it make sense from an accountability perspective to grant rights to a private entity for what will be pervasive data collection in public spaces without any public sector privacy oversight? Clearly, public sector entities are integral to authorizing this data collection. However, as currently proposed, they will not just be delegating the collection to Sidewalk Labs, they will be transferring usage rights to that data to Sidewalk.⁵

The public sector privacy laws are intended not only to establish privacy protections for personal information collected by public sector organizations, but also to provide for rights of access to *all information* held by such organizations. Waterfront Toronto currently is not designated an institution under these laws. This circumstance could result in there being no public sector access to information or privacy law protection with respect to any data collected by Sidewalk Labs.

Sidewalk Labs and others have advanced proposals to respond to this perceived gap in privacy protection. Sidewalk has proposed that all data will be held in a "[Civic Data Trust](#)" managed by a cross-section of community representatives. This entity potentially could be designated as an institution. However, the proposal appears to contemplate that Sidewalk would be the collector in the first instance with the possible result that its internal

⁴ How consent would be obtained has not been addressed. Would it involve some form of notice sufficiently posted to come to the attention of all persons entering the neighborhood, or would a form of express, opt-in consent be required?

⁵ [Project Vision](#), excerpt from Response to Waterfront Toronto Quayside RFP, October 17, 2017.

procedures would not be subject to public sector privacy scrutiny. However, if data collection were structured as undertaken *on behalf of* the data trust - having institution status - the public sector rules would apply.

Another [proposal](#) (by the Toronto Region Board of Trade) is for all data to be housed in a “Data Hub” within the Toronto Public Library, and rules for collection and use articulated by the Library or an advisory group within it.⁶ The Library, as a municipal entity within the City of Toronto, would be subject to MFIPPA. The Board’s proposal appears to envisage that all data collection would be overseen by the Library. It is not clear whether Sidewalk Labs would continue to be the collector of first instance, or be collecting on behalf of the Library.

An alternative would be to designate Waterfront Toronto as an institution under either FIPPA or MFIPPA and for it then to make clear that any data collection in Quayside will be conducted on its behalf. This does not necessarily mean that Waterfront Toronto would be required to develop internal functionalities to manage and utilize the data. It can pursue its relationship with Sidewalk Labs, and potentially other organizations, such as the Toronto Library, to build out functionalities for the Quayside digital community, ensuring that procedures and controls will be in place to address and frame the vast potential data usage that can be achieved.

Summary

Sidewalk Labs’ proposal to establish a digitally-enabled neighborhood in the Quayside district of the Toronto Waterfront involves not only the utilization of significant “private space” data stores obtained through existing technologies such as connected devices but also significant new data collection reflecting the dynamic interactions of people and things within the neighborhood. This new data collection would be achieved through electronic “sensor” measurements including video monitoring as well as from records of transactional interactions (such as parking fees). The new data would to a great extent be collected from “public spaces”, not within the scope of private space data stores, and would serve to fill in many of the gaps within the existing “physical layer” of the neighborhood, with dynamic digital data.

Sidewalk Labs’ current proposal is for this new data collection to be conducted by it, with a “Civic Data Trust” regime to provide rules guidance and to manage the data. However this proposal does not recognize or provide for any public sector privacy oversight. Such oversight can be achieved if the Data Trust or Waterfront Toronto were brought under FIPPA or MFIPPA by designation as a governmental “institution”, or another public sector entity such as the Toronto Public Library were designated as the vehicle for collection and use management of the data.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.

© David Young Law 2019

⁶ [BiblioTech - Beyond Quayside: A City-Building Proposal for the Toronto Public Library to Establish a Civic Data Hub](#), January 2019.