Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

VIA ELECTRONIC MAIL

September 24, 2019

Stephen Diamond
Chairman of the Board of Directors
Waterfront Toronto

Dear Mr. Diamond:

Re: Sidewalk Labs' Proposal

I am writing to comment on the privacy and access to information issues that arise in Sidewalk Labs' draft Master Innovation and Development Plan (MIDP) for the Quayside project. The purpose of this letter is to help guide Waterfront Toronto's consideration of the MIDP's digital governance proposals. Note that a number of our recommendations are directed to the government of Ontario and directly implicate the interests of the City of Toronto. For that reason, I have copied the provincial government and the City. As there is limited detail on the proposed digital innovations, our comments will focus on the digital governance proposals.

As discussed in greater detail below, I have the following key concerns about the proposals in the MIDP:

- The City must have a clearer role in the project and a voice in identifying what is in the public interest. Cities are at the core of smart city innovations such as transit optimization, or enhancement of public spaces, and they have experience in the delivery of municipal services.

- When a city or other public sector organization contracts with a private sector organization to carry out municipal services, it is essential that any related collection, use or disclosure of personal information complies with MFIPPA.

- The provincial government must modernize our laws to ensure that privacy protective, transparent, accountable and ethical data practices are at the forefront of all smart city projects.

- The proposed Urban Data Trust is problematic for a number of reasons, including: a concerning overlap with the mandate of the Trust and that of existing privacy regulators; a lack of independent oversight of the Trust's decisions; and an expectation that public sector organizations seek approval from the Trust.

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél: (416) 326-3333
1 (800) 387-0073
Fax/Téléc: (416) 325-9195
TTY/ATS: (416) 325-7539
Web: www.ipc.on.ca

- If new public sector organizations are created as a result of Sidewalk Labs' proposals, the provincial government must ensure that Ontario's public sector privacy and access legislation applies to those bodies.

Our office oversees Ontario's *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* which apply to provincial and municipal institutions respectively (also referred to as "organizations"). FIPPA and MFIPPA establish the rules for collection, use and disclosure of personal information and provide a right of access to information held by public institutions. These laws help ensure that governments are open, accountable and transparent – central features of any democratic government. The privacy protections recognize the fundamental right of individuals to have control over their own personal information. An important part of my office's role is to comment on proposed government programs and to work with provincial and municipal government institutions to ensure compliance with the laws.

My office has been closely following the Quayside consultations carried out by Waterfront Toronto. I was pleased to see that Waterfront Toronto set up an advisory panel with participation from some of the leading privacy voices to provide independent guidance on these challenging issues. Earlier in the year, we also met with Sidewalk Labs and Waterfront Toronto and provided some preliminary comments on the possible application of MFIPPA to the collection, use and disclosure of personal information in some of the scenarios described in the MIDP. We have also had discussions with the City and provincial government staff about the project where we expressed our commitment to support a thorough review of the privacy implications of the proposals in the MIDP.

I believe that some smart city technologies and the data they generate have the potential to help cities better manage urban environments and deliver services in a more effective and efficient way. Privacy does not have to be a barrier to these technologies. However, the increasing reliance on data – in some cases personal information – requires more robust protections.

OVERVIEW OF PRIVACY LAWS IN THE MUNICIPAL CONTEXT

Before commenting on the digital governance proposal, it is important to consider how municipal institutions are currently expected to protect privacy when collecting personal information.

Under MFIPPA, municipalities are only permitted to collect personal information if it is:

- expressly authorized by statute,
- used for law enforcement, or
- necessary to the proper administration of a lawfully authorized activity.

In many cases, municipalities rely on the last condition – that is, they collect personal information because it is necessary to do so to deliver a service. This is an important principle as it builds in data minimization requirements, a foundation of privacy laws worldwide. MFIPPA also limits how

municipalities may use and disclose personal information, and includes requirements for retention, storage and destruction.

Government organizations are increasingly working with the private sector to help them deliver effective and cost efficient public services. This is reflected in many smart city initiatives where public-private partnerships are formed to deliver services. In Ontario, the *Personal Information Protection and Electronic Documents Act* – a federal law overseen by the Privacy Commissioner of Canada – applies to the private sector when engaged in commercial activity.

The complex nature of smart city partnerships can make it challenging to determine the applicable privacy laws. Depending on the circumstances of the public-private partnership, it is possible that the collection, use or disclosure of personal information would be governed by MFIPPA, PIPEDA, or both. In our view, municipalities should be leading smart city initiatives involving the collection of data within public spaces, to solve urban challenges and improve the delivery of municipal services. When municipalities contract with private sector organizations to carry out activities that involve the collection, use or disclosure of personal information, compliance with MFIPPA is of the utmost importance. Unlike PIPEDA, MFIPPA does not allow the collection of personal information on the basis of consent. This has been an ongoing point of confusion in the Quayside discussion.

COMMENTS ON THE MIDP PROPOSAL

Proposal to create new organizations

Sidewalk Labs proposes the establishment of a number of organizations, including:

- Public Administrator – a public entity serving as revitalization lead in the project area.

- Waterfront Transportation Management Association (WTMA) – a unit of the Public Administrator that would oversee the mobility infrastructure and systems, such as the streets, sidewalks and transportation services within the project area.

Sidewalk Labs envisions the role of the Public Administrator to include overseeing the innovation, real estate, infrastructure and technology in the geographic area covered by the MIDP. Notably, Sidewalk Labs proposes that the Public Administrator would work closely with the City and others to lead planning efforts, and supplement the City's existing public approval process.

If any new public sector organizations are created as a result of Sidewalk Labs' proposals, the provincial government must ensure that Ontario's public sector privacy and access legislation applies to those bodies. It appears that the new organizations described above may deliver some key services that are within the legislative mandate of the City (as set out in the *City of Toronto Act, 2006*), and the TTC. If carried out in the more traditional manner by these institutions, these activities would clearly be governed by MFIPPA. However, the new public sector organizations would not necessarily fall under Ontario's public sector privacy and access legislation, unless they are designated as institutions. Clear statutory rights of access and privacy are key components to

democratic and accountable government.

Digital governance proposals

Sidewalk Labs' main digital governance proposals are:

- Urban Data – includes personal, non-personal, aggregate or de-identified data collected in a physical space in the City, where it is difficult to get meaningful consent prior to collection and use. Sidewalk Labs has proposed new rules and processes for the collection and use of Urban Data, intended to supplement existing rules set out in Ontario's public sector privacy laws and PIPEDA.

- Transactional Data – information that individuals provide through direct interaction with commercial or government-operated services, such as apps, websites, and product or service delivery. In contrast to Urban Data, Sidewalk Labs has not proposed any new rules or processes for the collection or use of Transactional Data; it is excluded from the Trust's oversight.

- Urban Data Trust (the Trust) – a data steward that oversees both public and private sector organizations collecting and using Urban Data in the project area. The Trust would have the authority to approve or reject any proposed collection or use of Urban Data.

- Responsible Data Use Assessment (RDUA) – organizations would be required to submit an RDUA to the Trust that evaluates the purpose of the proposal, the type of data it would collect, its potential impact on the community, and its risks and benefits.

Sidewalk Labs proposes a two-staged implementation of the Trust:

- Phase 1 – establish a non-profit organization overseen by a five-member board comprised of a data governance, privacy, or intellectual property expert; a community representative; a public-sector representative; an academic representative; and a Canadian business representative.

- Phase 2 – the Trust becomes a public-sector agency or quasi-public agency requiring enabling legislation.

Sidewalk Labs acknowledges that the Trust is just one digital governance model. I echo that statement. While there is value in open engagement with a diverse range of parties, ultimately the provincial and municipal governments, led by democratically elected officials, are best-placed to define the digital governance framework for this project and all other smart city initiatives in the province. We encourage the relevant governments to consult with our office to design an appropriate framework to ensure that privacy, accountability and ethical practices are at the forefront of these types of complex personal information practices.

With that in mind, the following comments should not be interpreted as implicit support of the digital governance proposals outlined in the MIDP. At this time, I remain unconvinced that the

proposal to create an Urban Data Trust as outlined in the MIDP is the most effective way to protect privacy rights. However, I am providing feedback on the digital governance proposals so they can be improved upon in the event that they are approved.

i. Urban and Transactional Data

Urban Data reflects a marked departure from the scope of current federal and provincial privacy legislation, which applies to *personal information*. If Waterfront Toronto supports the creation of a digital governance model that is based on Urban Data, it will be important not to lose sight of the need to comply with existing access and privacy laws that apply to *personal information* collected, used and disclosed by public and private sector organizations.

If pursued, there is also a need for clarity regarding the scope of Urban Data versus Transactional Data. In my view, it is difficult to determine whether some of the data activities described in the MIDP would be considered Urban Data, and therefore subject to the oversight of the Trust, or Transactional Data, which is not.

It is important to consider whether Urban Data and Transactional Data are meaningful distinctions – both types of data raise privacy concerns. For instance, consider a mobility app proposed in the MIDP that provides information about public and private sector transit options and allows users to pay using the same app. If the data collected via this app were to be classified as Transactional Data (which seems likely given that Transactional Data includes information individuals provide for service delivery through a direct interaction, such as apps) it would be considered outside of the scope of the Trust's review. This is concerning given that such an app, while beneficial for users, could enable a complete portrait of a user's movements in the area.

If one of the key purposes of the Trust is to add an extra layer of protection where there are increased privacy risks, such as surveillance, the omission of Transactional Data from the Trust's mandate is troubling. The privacy risks associated with Transactional Data are further amplified in the event that one organization, such as Sidewalk Labs, is engaged to support the delivery of multiple services in Quayside (such as offering mobile apps or delivering freight management and storage as suggested in the MIDP). If Sidewalk Labs (or another organization) provides multiple services, it could amass a great deal of information on individuals that could be linked to create detailed profiles of individuals' lives. Where an organization is providing multiple services to an individual who lives and/or works in Quayside (such as transit, mail delivery and hydro), consent may not offer strong privacy protection, as the individual may not have a viable alternative for those services.

For the reasons described above, it is important to consider whether both Urban Data and Transactional Data are deserving of an extra layer of review and protection, whether it be through a Trust or other legislative protections. I am pleased that Sidewalk Labs has committed to applying the Responsible Data Use Guidelines to any of its own commercially launched products and services that involve Transactional Data. I see this as an important role for Sidewalk Labs – that is, if they want to see a more robust framework in place for transparent, privacy-enhancing and ethical information practices, they should lead by example.

ii. The Urban Data Trust

One of the purposes of the Trust is to provide enhanced privacy and ethical protections that surpass the current privacy laws. Sidewalk Labs states that it wants the Trust to build a robust process that stakeholders can trust, can help advance the priority outcomes for the project, provides additional protections for individual privacy and groups, and makes publicly accessible the data that could reasonably be considered a public asset.

Sidewalk Labs' Trust proposal establishes a common approach for information handling and encourages best practices that go beyond the current legislative requirements. I believe that this is a laudable objective. For instance, the establishment of guiding principles around responsible artificial intelligence, or de-identification by default would enhance privacy protection for individuals whose information is collected, used and disclosed in a smart city initiative. While guidelines and best practices can be useful tools, in my view they are not adequate to ensure that these goals are met. The government needs to put in place a legislative framework to ensure that the highest protections are upheld and enforceable by an independent oversight agency. Below are further comments on the proposed Trust.

Overlap with existing privacy and access regulators

There is a distinct overlap between the roles of the Trust and the roles of my office and the federal Privacy Commissioner. For instance, it is possible that the Trust could approve a project, the parties would reasonably assume the project is legally sound, and my office could later find that the project violated MFIPPA. In other areas, such as auditing and enforcement, the Trust's authority may even reach beyond that of my office. This problem of overlapping jurisdictions and oversight is further complicated in public-private partnerships where it may be unclear whether public or private sector privacy laws apply. As I expand on below, the notion of a non-profit Trust having the ability to govern the information practices of public institutions that are already governed by privacy legislation and other statutes is problematic.

Composition of the board

As previously noted, Sidewalk Labs has suggested that the composition of the board could include a data governance, privacy, or intellectual property expert; a community representative; a public-sector representative; an academic representative; and a Canadian business representative. As well, they have recommended best practices to ensure the independence of the board. The representation of a diverse range of experience and interests is very important to the extent that the board will make decisions about all information practices in the scope of this project. While I understand why a sectoral approach was proposed, it may be beneficial to instead focus on the areas of expertise required to make such decisions; for example, ethics, risks to marginalized populations, data science and effective de-identification. Also, measures will need to be put in place to ensure that the board is independent, including defining processes for the selection of board members.

Limited oversight and redress

As described above, Sidewalk Labs proposes that the Trust be established as a non-profit with a chief data officer tasked with setting the guidelines and governance for digital practices in Quayside. If the Trust is established as proposed, our office would continue to have oversight over privacy and access laws applicable to Ontario's public institutions operating in the project area. However, under the MIDP proposal, in phase one there would be no independent oversight of the decisions made by the Trust. Nor would it be subject to Ontario's access and privacy laws. It appears that the only remedy for parties subject to the Trust would be to seek redress before the courts – a costly and time consuming process. It is also not clear that the public, particularly individuals affected by the Trust's decision to approve or disallow projects, would have any recourse during phase one, given that they would not be a party to the contractual agreements between the Trust and the organizations seeking approval of their collection practices.

For the above reasons, I do not recommend that Waterfront Toronto approve a two-phase approach to implementation of the Trust. Absent a legislative framework to protect privacy and access rights, ensure best practices and provide independent oversight, the Trust model is not adequate. Instead, I recommend that the provincial government conduct an open review of the Trust model and determine whether it or some other legislative scheme should be enacted to govern privacy in all smart city projects. If the government decides to pursue this Trust model, it must be supported by a clear regulatory framework that sets out the Trust's authority, mandate, criteria for evaluating the full lifecycle of data (not just collection and use), as well as a mechanism for independent oversight. Ontario has a number of good examples of entities that are entrusted with the management of large amounts of personal information, such as the prescribed entities model under Ontario's health privacy law.

Public interest must be clearly defined

Sidewalk Labs proposes that the mandate of the Trust include balancing the public interest and the need for innovation. There are many interests that will need to be considered in such an evaluation, such as privacy, human rights, security, intellectual property, potential benefits to future society, data monopolies and many others. It is not clear how the Trust would balance these diverse interests unless the public interest is clearly defined. The government should ensure that public interest objectives are defined in legislation.

Clearer role for the City

It is unclear from our review what role the City will play in the implementation of the proposal as a whole. This is unfortunate, as the City is at the core of smart city innovations such as transit optimization, or enhancement of public spaces, and it has obvious experience in the delivery of municipal services. The City also has broad legislative authority to pass bylaws regulating the economic, social and environmental well-being of the City, as well as the health, safety and well-being of persons within the City. As a democratically elected government, the City must have a clearer role in the project and ultimately a voice in identifying what is in the public interest. If the provincial government pursues the Trust model proposed, there must an integral role for cities clearly articulated in the legislative framework.

Public sector reporting to the Trust

As noted above, I also find it problematic that, as proposed, the City and other public sector organizations would be expected to apply to the Trust in order to collect or use any Urban Data in the geographical area of the project. The City has statutory authority to carry out various activities that will require the collection, use and disclosure of personal information in order to properly administer its lawfully authorized activities. In some cases, the City may be statutorily required to collect, use or disclose personal information. The City also has extensive experience in determining what is in the public interest, a democratic mandate, and has also developed a framework for the protection of privacy. To then expect the City to apply to a non-profit Trust, go through the evaluation process, and commit to contractual undertakings would be inappropriate given the experience, mandate and statutory authority of the City.

Need for law reform

As described above, part of the aim of the Trust is to build upon the foundation of privacy laws and create a higher standard of protection. We encourage organizations to surpass the bare minimums set out in legislation, and recognize Sidewalk Labs' effort to improve upon an imperfect legislative framework in the Trust proposal. Our privacy and access laws are out-dated and the IPC has long called for a comprehensive review and modernization of our public sector privacy laws.

Rather than relying on Sidewalk Labs to develop an appropriate solution, this is an opportunity for the provincial government to take the lead and modernize the laws to address the legislative shortcomings. Amendments could include mandatory requirements for data minimization, additional protections for individual and group privacy, ethical safeguards, and greater enforcement tools for my office, including additional investigation, order making and audit powers.

With regard to private sector privacy laws, reports of the federal Privacy Commissioner and the Standing Committee on Access to Information, Privacy and Ethics, among others, demonstrate that PIPEDA is inadequate. As the process unfolding at the federal level to bring PIPEDA up to date is proceeding slowly, this may also be the time for the government to consider advancing made-in-Ontario private sector privacy legislation. An Ontario private sector privacy law would help ensure public and private sector laws are cohesive, and help to minimize the risks of regulatory uncertainty. Simplifying oversight would lead to efficiencies, particularly in the context of smart city initiatives that involve partnerships between the private and public sectors.

An alternative option for the government to consider is stand alone smart city legislation. Legislative reform could ensure that there are clearly defined and consistent rules in Ontario to address the unique risks arising from public-private sector partnerships in all urban settings, not just Quayside. This includes a need for clarity on which law applies to these types of complex information practices within our cities.

iii. Responsible Data Use Assessment and Guidelines

Sidewalk Labs sets out its views on what should be included in the Responsible Data Use Guidelines, though ultimately they suggest that the Trust should establish the Guidelines. The principles included in the Guidelines (including transparency, de-identification by default, data minimization and making data publicly accessible) are important principles and I agree that all of these factors should be considered when carrying out data activities.

Full lifecycle

The MIDP proposes the Trust be tasked with "implementing and managing a four-step process for approving the responsible collection and use of Urban Data." Disclosure is a notable absence in this mandate. Some references in the MIDP suggest that the full lifecycle of information will be considered – however, most seem to only consider collection and use. Whatever the approach, the full lifecycle of information handling must be considered.

PIAs

The RDUA is a tool developed by Sidewalk Labs to evaluate any proposed activities involving Urban Data. While the proposed RDUA process clearly incorporates some elements of a Privacy Impact Assessment (PIA), it is unclear if the completion of an RDUA would satisfy all of the components typically considered in a PIA (such as identifying the data flows, confirming legal authority for each data activity, and considering the full information lifecycle from collection/creation to destruction/return). PIAs are widely recognized as important tools to help ensure that privacy risks are identified and adequately addressed in the design of new technologies and programs. The City completes PIAs regularly when considering new technologies or programs. In this project, there must be a requirement for all organizations processing personal information to conduct a full PIA, or to include PIA requirements in the RDUA.

Net impact

The RDUA developed by Sidewalk Labs proposes that the Trust base decisions on a net impact of an initiative, balancing benefit and risk. This may be problematic. For instance, an initiative that is high risk yet yields a higher benefit would arguably be allowed to proceed with this approach. Some privacy risks will not be acceptable, no matter how beneficial the outcome may be.

CONCLUSION

I appreciate the valuable public discussion encouraged by Waterfront Toronto and Sidewalk Labs and furthered by governments, academics, civil society actors and special interest groups around new digital governance models. I also want to commend Waterfront Toronto and Sidewalk Labs for the number of open consultations that have taken place over the last year.

The digital governance proposals set out in the MIDP raise several concerns, including: a lack of independent public oversight, a cumbersome mandate that overlaps with that of my office and the federal Privacy Commissioner, and an insufficient role for the City given its experience delivering

municipal services in the public interest. If Waterfront Toronto decides to pursue the Trust proposal advanced by Sidewalk Labs, it must be supported by the provincial government with a clear regulatory framework that sets out the mandate, criteria for evaluating the full lifecycle of data, as well as a mechanism for independent oversight. In addition, if new public organizations are created, such as the proposed Public Administrator, they must be designated as institutions under MFIPPA or FIPPA.

Most importantly, the digital governance proposals proposed by Sidewalk Labs highlight the legislative shortcomings in our privacy laws. I appreciate the efforts of Waterfront Toronto and Sidewalk Labs to explore interim measures to address these deficiencies; however, the provincial government needs to modernize our laws to ensure that privacy protective, transparent, accountable and ethical data practices are at the forefront of all of these complex data projects. My office is available to consult with the government on the design of a legislative framework that meets these requirements.

Sincerely,

Brian Beamish
Commissioner

cc: Hillary Hartley
Chief Digital and Data Officer, Deputy Minister
Cabinet Office

John Roberts
Chief Privacy Officer and Archivist of Ontario
Ministry of Government and Consumer Services

John Tory
Mayor
City of Toronto

Honorable Laurie Scott
Ontario Infrastructure Minister
Ministry of Infrastructure